opentext™

OpenText™ Dynamic Application Security Testing (Fortify WebInspect)

ソフトウェアバージョン: 25.2.0
Windows® OS

ユーザガイド

ドキュメントリリース日 : 2025年5月
ソフトウェアリリース日 : 2025年5月

法的通知

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

著作権表示

商標表示

ドキュメントの更新情報

このドキュメントのタイトルページには、次の識別情報が記載されています。

- ソフトウェアバージョン番号
- ドキュメントリリース日。ドキュメントが更新されるたびに変更されます
- ソフトウェアリリース日。ソフトウェアのこのバージョンのリリース日付を示します

このドキュメントは、OpenText™ Dynamic Application Security Testing CE 25.2向けに7月 29, 2025に作成されました。

オンラインヘルプのこのPDF版について

このドキュメントは、オンラインヘルプのPDF版です。このPDFファイルの提供によって、ヘルプ情報から複数のトピックを簡単に印刷したり、オンラインヘルプをPDF形式で閲覧したりできます。このコンテンツは、もともとWebブラウザで表示するオンラインヘルプとして作成されたため、一部のトピックが適切な形式で表示されない可能性があります。このPDF版では、一部の対話型トピックを表示できない場合があります。それらのトピックは、オンラインヘルプから正常に印刷できます。

目次

序文

カスタマサポートへのお問い合わせ

カスタマサポートWebサイトにアクセスして、次の作業を実行できます。

- ライセンスとエンタイトルメントの管理
- 技術サポートリクエストの作成と管理
- ドキュメントやナレッジ記事の閲覧
- ソフトウェアのダウンロード
- コミュニティの探索

詳細情報

OpenText Application Security Testing製品の詳細については、「OpenText Application Security」を参照してください。

製品の機能紹介ビデオ

YouTube™のFortify Unpluggedチャネルで、OpenText Application Security Softwareの製品と機能を紹介するビデオをご覧いただけます。

変更ログ

次の表に、このドキュメントで行われた変更を示します。このドキュメントの改訂版は、変更が製品の機能に影響を与える場合にのみ、ソフトウェアリリース間で発行されます。

ソフトウェアリリース/ドキュメントバージョン	変更点
25.2.0	更新: • 製品名の変更を反映するため、Fortify WebInspectの記載をOpenText DASTに変更。 • 複数ポリシー選択に関するスキャンウィザード、wi.exe、およびスキャン設定のコンテンツ。次のトピックを参照してください。 • "ダッシュボード" ページ76 • "基本スキャンの実行(Webサイトスキャン)" ページ199 • "API監査範囲と徹底性の設定" ページ183 (新規トピック) • "wi.exeの使用" ページ329 • "スキャン設定: ポリシー" ページ450 • 新しいユーザエージェントを使用したデフォルトのスキャン設定。「"スキャン設定: ユーザエージェント" ページ452」を参照してください。 • 新しい複合設定オプションを含むアプリケーション設定。「"アプリケーション設定: 全般" ページ480」を参照してください。 • 複合スキャン設定での証明書の更新に関する詳細。次のトピックを参照してください。 • "基本スキャンの実行(Webサイトスキャン)" ページ199 • "APIスキャンの認証とコネクティビティの設定" ページ170 • "スキャン設定: 認証" ページ440
24.4.0 / 2024年11月	追加: • Fortify WebInspect Enterpriseのサービス終了に関するコンテンツ。「"Fortify WebInspect Enterpriseについて" ページ33」を参照してください。

ソフトウェアリリース/ドキュメントバージョン	変更点
24.4.0	更新: • ユーザエージェントをFirefox 110.0に変更。「"スキャン設定: ユーザエージェント" ページ452」を参照してください。 • バージョン番号とリリース日。
24.2.0	追加: • スキャン設定でOAuth 2.0 Bearer資格情報を使用するためのコンテンツ。「"OAuth 2.0のBearer資格情報の設定" ページ447」を参照してください。 更新: • OAuth 2.0 Bearer資格情報に関する情報を含むスキャンウィザードおよびスキャン設定のコンテンツ。次のトピックを参照してください。 • "事前定義テンプレートの使用" ページ113 • "モバイルスキャンテンプレートの使用" ページ130 • "ネイティブスキャンテンプレートの使用" ページ147 • "APIスキャンの認証とコネクティビティの設定" ページ170 • "基本スキャンの実行(Webサイトスキャン)" ページ199 • "スキャン設定: 認証" ページ440 • スキャン詳細をエクスポートするためのコンテンツ(CycloneDXファイルをFortify Software Security Centerにインポートするための回避策を含む)。「"スキャン詳細のエクスポート" ページ254」を参照してください。 • OWASP API Top 10 <年>ポリシーおよび非推奨のAggressiveLog4Shellポリシー関連のコンテンツ。「"wi.exeの使用" ページ329」および「"OpenText DAST ポリシー" ページ509」を参照してください。
23.2.0	更新: • IMAPをサポートする2要素認証コンテンツと、Gmailアカウントに関する考慮事項。「"2要素認証の使用" ページ222」を参照してください。

ソフトウェアリリース/ドキュメントバージョン	変更点
	• ポリシーのコンテンツに、OAST関連チェックに関する情報を追加。「"OpenText DAST ポリシー" ページ509」を参照してください。 • JavaScriptの設定についてのコンテンツに、新しいWebSocketイベントのキャプチャに関する設定を追加。「"スキャン設定: JavaScript" ページ412」を参照してください。 削除: • Site Explorerへの参照。

第1章:はじめに

OpenText™ Dynamic Application Security Testing (DAST) 25.2.0は、自動化されたWebアプリケーション、API、およびWebサービスの脆弱性スキャンツールです。OpenText DASTは、スキャン技術の最新の進化形として、あらゆるエンタープライズ環境に適応するWebアプリケーションセキュリティ製品を提供します。スキャンを開始すると、OpenText DASTはWebアプリケーションのすべてのエリアをダイナミックにカタログするエージェントを割り当てます。これらのエージェントは、検出事項を分析する主要なセキュリティエンジンに結果を報告します。その後、OpenText DASTは「脅威エージェント」を起動して、収集された情報を評価し、攻撃アルゴリズムを適用して潜在的な脆弱性の存在と相対的な重大度を判断します。このスマートなアプローチにより、OpenText DASTは特定のアプリケーション環境に適応する適切なスキャンリソースを継続的に適用します。

検出事項について

OpenText DASTの検出事項は、実際の脆弱性ではなく潜在的な脆弱性と見なす必要があります。アプリケーションはどれも固有であり、どの機能も特有のコンテキスト内で実行されます。そのコンテキストを最もよく理解できるのは開発チームです。開発者に直接確認することなく、疑わしい動作が脆弱性と見なされるかどうかを完全に判断できる技術はありません。

参照情報

"OpenText DASTの概要" 下

OpenText DASTの概要

OpenText DASTで実行できる操作、および組織が得られるメリットについて、次に簡単に説明します。

Web探索および監査

OpenText DASTでは、セキュリティ上の弱点を明らかにするために、2つの基本モードを使用します。

- Web探索とは、OpenText DASTでターゲットWebサイトの構造を識別するプロセスです。基本的に、Web探索はURL上にアクセスできるリンクがなくなるまで実行されます。
- 監査とは、実際の脆弱性スキャンです。クロールと監査を1つの機能としてまとめたものをスキャンと呼びます。

レポーティング

OpenText DASTレポートを使用して、整理された有益なアプリケーション情報を取得します。レポートの詳細をカスタマイズしたり、各レポートに含める情報のレベルを決定したり、特定の対象ユーザ向けにレポートを作成したりすることができます。カスタマイズしたレポートはテンプレートとして保存することもできます。これにより、同じレポート基準を使用して、更新情報を反映したレポートを生成することが可能になります。レポートは、PDF、HTML、Excel、Raw、RTF、またはテキスト形式で保存できます。また、脆弱性データのグラフィックサマリを含めることもできます。

手動ハッキング制御

OpenText DASTでは、サイトで実際に何が起こっているかを確認し、真の攻撃環境をシミュレートできます。OpenText DAST機能を使用すると、脆弱性のあるページのコードを表示し、サーバ要求を変更して直ちに再送信することができます。

概要と修復

情報ペインには、ナビゲーションペインまたはサマリペインのいずれかで選択した脆弱性に関するすべての概要と修復情報が表示されます。詳細については、「"ナビゲーションペイン" ページ61」および「"サマリペイン" ページ104」を参照してください。

また、参照資料が提示され、パッチへのリンク、将来の問題を防止するための指示、および脆弱性ソリューションも示されています。新しい攻撃やエクスプロイトコードは毎日作成されるため、OpenTextによって概要と修復情報のデータベースが頻繁に更新されます。OpenText DASTツールバーの [スマートアップデート(Smart Update)] でデータベースを更新して最新の脆弱性解決情報を反映させることも、起動時に自動的に更新を確認することもできます。詳細については、「"SmartUpdate" ページ324」および「"アプリケーション設定:スマートアップデート" ページ505」を参照してください。

スキャンポリシー

組織のニーズに合わせてスキャンポリシーを編集およびカスタマイズして、OpenText DASTのスキャン所要時間を短縮できます。OpenText DASTポリシーの設定方法に関する詳細については、Policy Managerのヘルプまたは『*OpenText™ Dynamic Application Security Testing ツールガイド*』を参照してください。

ソートとカスタマイズが可能なビュー

スキャンを実行または表示する場合、OpenText DASTウィンドウの左のナビゲーションペインには、**サイト(Site)**]、**シーケンス(Sequence)**]、**検索(Search)**]、および**ステップモード(Step Mode)**]の各ボタンがあり、このボタンでナビゲーションペインに表示されるコンテンツ(または「ビュー」)を決定できます。

- サイト(Site)]ビューには、OpenText DASTによって決定された、スキャン対象サイトの階層ファイル構造が表示されます。また、リソースごとに、サーバから返されたHTTPステータスコードと検出された脆弱性の数も表示されます。
- シーケンス(Sequence)]ビューには、OpenText DASTによって自動スキャンまたは手動Web探索(ステップモード)中に検出された順序でサーバリソースが表示されます。
- 検索ビューでは、指定した基準に一致するセッションを検索できます。詳細については、「"検索(Search)]ビュー" ページ289」を参照してください。
- ステップモードは、サイト(Site)]ビューまたはシーケンス(Sequence)]ビューのいずれかから選択したセッションを起点にして、サイト内を手動で移動するために使用されます。詳細については、「"手動スキャンの実行" ページ231」を参照してください。

企業全体における利用状況の機能

統合スキャンでは、企業全体の観点からWebプレゼンスの包括的な概要が提供され、ネットワーク上のすべてのWeb対応アプリケーションのアプリケーションスキャンを実行できます。

Webサービススキャン機能

Webサービスの脆弱性を包括的にスキャンします。Webサービス/SOAPオブジェクトが含まれているアプリケーションを評価できます。

エクスポートウィザード

OpenText DASTの堅牢で設定可能なXMLエクスポートツールを使用すると、ユーザはスキャン中に検出されたあらゆる情報を(標準化されたXML形式で)エクスポートできます。これには、コメント、非表示フィールド、JavaScript、クッキー、Webフォーム、URL、要求、およびセッションが含まれます。ユーザは、エクスポートする情報のタイプを指定できます。

Webサービステストデザイナ

Web Service Test Designerでは、Webサービススキャンの実行時にOpenText DASTから送信される値が入ったWebサービステスト設計ファイル(*<ファイル名>*.wsd)を作成できます。

[APIスキャン(API Scan)]

OpenText DASTでは、REST APIアプリケーションのスキャンは次のようにサポートされます:

- APIスキャンウィザードを使用して、ユーザインタフェースでAPIスキャンを設定します。詳細については、「"APIスキャンウィザードの使用" ページ165」を参照してください。
- OpenText DAST REST APIを使用して、REST API定義をスキャンします。詳細については、「"OpenText DAST REST API" ページ357」を参照してください。
- API要求のPostmanコレクションを使用して、スキャンを開始します。詳細については、「"Postmanコレクションによるスキャン" ページ364」を参照してください。

API検出

API検出では、スキャン中に検出されたSwaggerスキーマまたはOpenAPIスキーマのエンドポイントが既存のスキャンに追加され、自動状態検出を使用してエンドポイントに認証が適用されます。また、一般的なAPIフレームワークのデフォルトの場所にプローブが送信され、スキーマが検出されます。

統合機能

OpenText DASTは、最も広く使用されているアプリケーションセキュリティ開発およびテストツールと統合できます。これには以下のものが含まれます。

- Burp (詳細については、「"Burp API拡張機能について" ページ384」を参照してください。)
- Postman (詳細については、「"Postmanコレクションによるスキャン" ページ364」を参照してください。)
- Selenium WebDriver (詳細については、「"Selenium WebDriverとの統合" ページ373」を参照してください。)
- HTTPアーカイブ(HAR)ファイルワークフローマクロ(詳細については、「"ワークフローマクロの選択" ページ281」を参照してください)。

強化されたサードパーティの商用アプリケーション脅威エージェント

OpenText DASTを使用すれば、ユーザは業界をリードするアプリケーションプラットフォームを含むあらゆるWebアプリケーションのセキュリティスキャンを実行できます。OpenText DASTを使用する標準的な商用アプリケーション脅威エージェントには、次のようなものがあります:

- Adobe ColdFusion
- Adobe JRun
- Apache Tomcat
- IBM Domino

- IBM WebSphere
- Microsoft.NET
- Oracle Application Server
- Oracle WebLogic

ハッカーレベルのインサイト

OpenText DASTでは、スキャン中にアプリケーションで検出されたライブラリにフラグが設定されます。この情報により、開発者やセキュリティ専門家はアプリケーションの全体的なセキュリティ状態に関連するコンテキストを把握できます。これらの検出事項が必ずしもセキュリティの脆弱性を示しているとは限りませんが、通常、攻撃者は既知の弱点やパターンを特定しようとする際にターゲットの偵察を実行するということに注意することが重要です。詳細については、「"クライアント側ライブラリ分析" ページ287」を参照してください。

Fortify WebInspect Enterpriseについて

OpenText™ Fortify WebInspect Enterpriseは、一元管理されたデータベースを持つシステムマネージャによって制御されるOpenText DASTセンサの分散ネットワークを採用しています。必要に応じて、Fortify WebInspect EnterpriseをOpenText™ Fortify Software Security Centerと統合し、WebサイトとWebサービスのダイナミックスキャンを通して検出された情報をFortify Software Security Centerに提供できます。

注記: Fortify WebInspect Enterpriseはサポートされなくなりました。製品の最終リリースバージョンは、バージョン23.2.0です。OpenTextでは、動的スキャンを実現するため、OpenText™ ScanCentral DASTへの移行をお勧めしています。

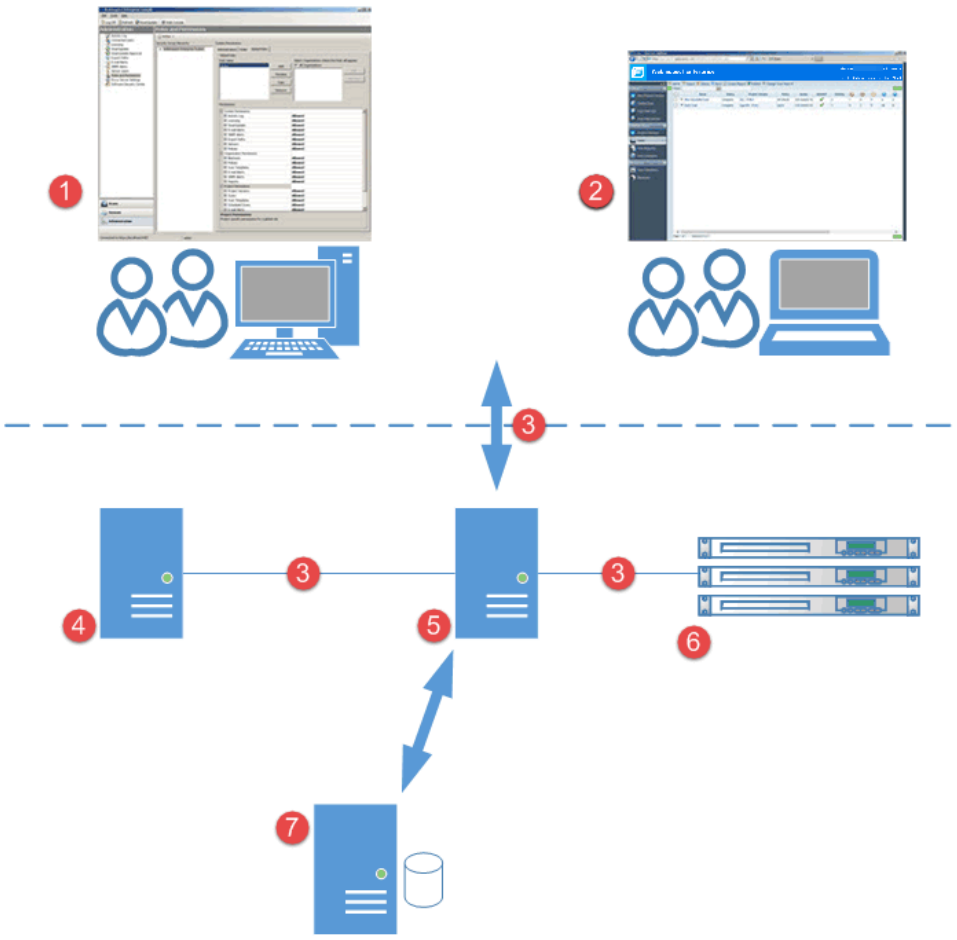
この革新的なアーキテクチャにより、次の操作を実行できます。

- 任意の数のOpenText DASTセンサを使用して多数の自動化セキュリティスキャンを実行し、WebアプリケーションとSOAPサービスをスキャンします。
- 組織全体にわたる大規模または小規模なOpenText DAST展開を管理し、製品のアップデート、スキャンポリシー、スキャン許可、ツールの使用状況、およびスキャン結果のすべてをFortify WebInspect Enterpriseコンソールから一元的に管理します。
- 新しいWebアプリケーションと既存のWebアプリケーションを追跡、管理、および検出し、それらに関連付けられたすべてのアクティビティを監視します。
- 必要に応じて、スキャンデータをFortify Software Security Centerにアップロードします。
- OpenText DASTまたはFortify WebInspect Enterpriseコンソールを使用して、スキャンとブラックアウト期間を個別にスケジュールしたり、スキャンを手動で起動したり、リポジトリ情報を更新したりします。詳細については、「"ブラックアウト期間" ページ398」を参照してください。
- ユーザ用に一元的に定義された役割を使用することによって、社外秘扱いのコンポーネントやデータの表示を制限します。

- スキャン結果、レポーティング、および傾向分析の一元管理されたデータベースを通して、組織のリスクとポリシーコンプライアンスの正確な全体像を把握します。
- サードパーティ製品との統合と、カスタマイズされたWebベースのフロントエンドの展開を、Webサービスアプリケーションプログラムインタフェース(API)を使用して促進します。

Fortify WebInspect Enterpriseのコンポーネント

次の図は、Fortify WebInspect Enterpriseシステムの主要なコンポーネントを示しています。これには、Fortify WebInspect Enterpriseアプリケーション、データベース、センサ、およびユーザが含まれます。



コンポーネントの説明

次の表に、Fortify WebInspect Enterpriseのユーザインタフェースとアーキテクチャの説明を示します。

項目	コンポーネント	説明
1	Windowsコンソールのユーザインタフェース	このコンソールは、管理機能、ポリシー編集、およびツールキットを提供するシンクライアントアプリケーションです。
2	Webコンソールのユーザインタフェース	このコンソールは、ユーザ機能を提供するブラウザベースのアプリケーションです。これは、管理機能、ポリシー編集、またはツールキットを備えていません。
3	HTTPまたはHTTPS	Fortify WebInspect Enterpriseコンポーネントでは、これらの通信プロトコルが使用されます。
4	Fortify Software Security Center(オプション)	Fortify Software Security Centerと統合すると、すべてのスタティックスキャンとダイナミックスキャンの中央リポジトリにスキャンを発行できます。これにより、ある程度一元管理されたアカウント(ただし、許可は依然として独立して管理される)、スキャン要求を送信する機能、およびスタンドアロンインストールに比べてより広範囲のレポーティングが提供されます。
5	Fortify WebInspect Enterpriseマネージャ	これは、IISアプリケーションプラットフォームを使用したMicrosoft Windowsサーバです。ユーザ認証と権限付与、データリポジトリ、およびリモートスキャンスケジューリングを主な機能とするWebサービスです。
6	センサ	これらのOpenText DASTセンサは、Microsoft WindowsまたはWindows Serverオペレーティングシステムにインストールされます。センサは、GUIがなく、Webコンソールで設定されたリモートスキャンを実行します。Webコンソールを使用して、スキャン設定、結果、レポート、および更新のすべてを制御します。
7	Microsoft SQL Server	このMicrosoft Windowsサーバは、すべてのユーザ、許可、および管理設定を格納するSQLデータベースを備えています。このデータベースには、すべてのスキャンデータとレポーティングも保存されます。

OpenText DAST製品のFIPSの準拠について

OpenText DASTプログラムは連邦情報処理標準(FIPS)に準拠するために必要な暗号化規格を満たします。アメリカ国立標準技術研究所(NIST)によって確立されたAESアルゴリズムを使用してデータが暗号化されます。これには、OpenText DASTとのデータの送受信や、保存されたスキャンデータが含まれます。

製品名の変更

OpenTextでは、次の製品名を変更中です。

前の名前	新しい名前
Fortify Static Code Analyzer	OpenText™ Static Application Security Testing (OpenText SAST)
Fortify Software Security Center	OpenText™ Application Security
Fortify WebInspect	OpenText™ Dynamic Application Security Testing (OpenText DAST)
Fortify on Demand	OpenText™ Core Application Security
Debricked	OpenText™ Core Software Composition Analysis (OpenText Core SCA)
Fortifyアプリケーションとツール	OpenText™ Application Security Tools

これらの製品名は、製品のスプラッシュページ、マストヘッド、ログインページ、および製品が識別されるその他の場所で変更されました。名前の変更は、製品の機能を明確にし、Fortify Software製品とOpenText製品をより適切に適合させることを目的としています。ドキュメントのタイトルページなど、場合によっては、古い名前が一時的に括弧に含まれる場合があります。今後の製品リリースで、さらに多くの変更を予定しています。

関連ドキュメント

このトピックでは、OpenText Application Security Software製品に関する情報を提供するドキュメントについて説明します。

注記: ほとんどのガイドは、PDF形式とHTML形式の両方で提供されています。製品ヘルプは、OpenText DAST製品内で利用できます。

すべての製品

以下のドキュメントには、すべての製品に関する一般情報が記載されています。特に明記されている場合を除き、これらのドキュメントは各製品の製品マニュアルのWebサイトで利用できます。

ドキュメント/ファイル名	説明
OpenText Application Security Softwareについて appsec-docs-n-*<version>*.pdf	この文書では、OpenText Application Security Software製品のドキュメントにアクセスする方法について説明します。 **注記:** このドキュメントは、製品のダウンロードにのみ含まれています。
OpenText Application Security Softwareソフトウェア<version>の新機能 appsec-wn-*<version>*.pdf	このドキュメントでは、OpenText Application Security Software製品の新機能について説明します。
OpenText Application Security Softwareリリースノート appsec-rn-*<version>*.pdf	このドキュメントでは、OpenText Application Security Softwareのこのリリースで行われた変更の概要と、他の製品ドキュメントには記載されていない重要な情報について説明します。

OpenText DAST

次のドキュメントでは、OpenText DAST (Fortify WebInspect)の情報について説明します。これらのドキュメントは製品マニュアルのWebサイト (https://www.microfocus.com/documentation/fortify-webinspect)で利用できます。

ドキュメント/ファイル名	説明
OpenText™ Dynamic Application Security Testingインストールガイド dast-igd-*<version>*.pdf	このドキュメントでは、OpenText DASTの概要、インストール方法、製品ライセンスの有効化手順について説明します。
OpenText™ Dynamic Application Security Testingユーザガイド dast-ugd-*<version>*.pdf	このドキュメントでは、OpenText DASTを設定および使用して、WebアプリケーションやWebサービスをスキャンして分析する方法について説明します。

ドキュメント/ファイル名	説明
	注記: このドキュメントは、OpenText DASTヘルプのPDF版です。このPDFファイルは、ヘルプ情報から簡単に複数のトピックを印刷したり、ヘルプをPDF形式で閲覧したりできるようにするために用意されています。このコンテンツは、もともとWebブラウザで表示するヘルプとして作成されたため、一部のトピックが適切な形式で表示されない可能性があります。また、このPDF版では一部の対話型トピックやリンクされたコンテンツを表示できない場合があります。
OpenText™ Dynamic Application Security TestingおよびOAST on Dockerユーザガイド dast-docker-ugd-*<version>*.pdf	このドキュメントでは、Dockerプラットフォーム上のコンテナイメージとして利用可能なOpenText DASTおよびFortify OASTをダウンロード、設定、使用する方法について説明します。OpenText DASTイメージの目的は、コマンドラインインタフェース(CLI)またはアプリケーションプログラミングインタフェース(API)を経由して設定されたヘッドレスセンサとして自動化プロセスで使用することです。OpenText ScanCentral DASTのセンサとして実行し、Fortify Software Security Centerと組み合わせて使用することもできます。Fortify OASTは、帯域外のアプリケーションセキュリティテスト(OAST)サーバであり、OAST脆弱性の検出のために、DNSサービスを提供します。
OpenText™ Fortify License and Infrastructure Managerインストールおよび使用ガイド lim-ugd-*<version>*.pdf	このドキュメントでは、Fortify License and Infrastructure Manager (LIM)をインストール、設定、使用する方法について説明します。LIMは、ローカルWindowsサーバにインストールして、Dockerプラットフォーム上のコンテナイメージとして使用できます。
OpenText™ Dynamic Application Security Testingツールガイド dast-tgd-*<version>*.pdf	このドキュメントでは、OpenText DASTおよびFortify WebInspect Enterpriseにパッケージ化されたOpenText DASTの診断および侵入テストツールと設定ユーティリティの使用方法について説明します。
OpenText™ Dynamic Application Security Testing Agentインストール	このドキュメントでは、OpenText DAST Agentのインストール方法と、OpenText DAST Agentルールパッ

ドキュメント/ファイル名	説明
およびルールパックガイド dast-agent-igd-<*version*>.pdf	クキットの検出機能について説明します。OpenText DAST Agentルールパックキットは OpenText DAST Agentの上で実行され、実行時にコードを監視してソフトウェアのセキュリティ脆弱性を検出できるようにします。OpenText DAST Agentルールパックキットは、動的な結果を静的な結果に関連付けるのに役立つランタイムテクノロジを提供します。

Fortify WebInspect Enterprise

次のドキュメントでは、Fortify WebInspect Enterpriseの情報について説明します。特に明記されている場合を除き、これらのドキュメントは製品マニュアルのWebサイト (https://www.microfocus.com/documentation/fortify-webinspect-enterprise)で利用できます。

ドキュメント/ファイル名	説明
OpenText™ Fortify WebInspect Enterpriseインストールおよび実装ガイド WIE_Install_<*version*>.pdf	このドキュメントでは、Fortify WebInspect Enterpriseの概要、Fortify WebInspect Enterpriseのインストール手順、Fortify Software Security CenterやOpenText DASTとの統合、およびインストールのトラブルシューティングについて説明します。また、Fortify WebInspect Enterpriseシステムのコンポーネントの設定方法についても説明します。これには、Fortify WebInspect Enterpriseのアプリケーション、データベース、センサ、およびユーザが含まれています。
OpenText™ Fortify WebInspect Enterpriseユーザガイド WIE_Guide_<*version*>.pdf	このドキュメントでは、Fortify WebInspect Enterpriseを使用してOpenText DASTセンサの分散ネットワークを管理し、WebアプリケーションとWebサービスをスキャンして分析する方法について説明します。 **注記:** このドキュメントは、Fortify WebInspect EnterpriseヘルプのPDF版です。このPDFファイルは、ヘルプ情報から簡単に複数のトピックを印刷したり、ヘルプをPDF形式で閲覧したりできるようにするために用意されています。このコンテンツは、もともとWebブラウザで表示するヘルプとして作成されたため、一部のトピックが適切な形式で表示されない可能性があります。また、このPDF版では一部の対

ドキュメント/ファイル名	説明
	話型トピックやリンクされたコンテンツを表示できない場合があります。
OpenText™ Dynamic Application Security Testing ツールガイド dast-tgd-<*version*>.pdf	このドキュメントでは、OpenText DASTおよびFortify WebInspect Enterpriseにパッケージ化されたOpenText DASTの診断および侵入テストツールと設定ユーティリティの使用方法について説明します。

第2章:はじめに

この章では、OpenText DASTをすぐに使い始めることができるように、お使いのシステムを監査用に準備し、SecureBaseを更新して、スキャンを開始する方法について説明します。

システムの監査準備

OpenText DASTは、実際のおよび潜在的なセキュリティの脆弱性がないかWebサイト全体を厳正に調査する、積極的なWebアプリケーションアナライザです。程度の差こそあれ、この手順は侵入型です。適用するOpenText DASTポリシーと選択するオプションによっては、サーバとアプリケーションのスループットと効率に影響する場合があります。最も積極的なポリシーを使用する場合、OpenTextはサーバを監視しながら制御された環境でこの分析を実行することをお勧めします。

機密データ

OpenText DASTでは、アプリケーションとサーバ間で送信されたアプリケーションデータがすべてキャプチャおよび表示されます。使用しているアプリケーション内で自分が認識していない機密データが検出されることさえあるかもしれません。OpenTextでは、機密データに関する次のいずれかのベストプラクティスに従うことをお勧めします。

- OpenText DASTでのテスト中は、実際のユーザ名やパスワードなどの潜在的な機密データを使用しない。
- 潜在的な機密データへのアクセスを許可されていないユーザがOpenText DASTスキャン、関連するアーティファクト、およびデータストアにアクセスできないようにする。

ネットワーク認証資格情報はOpenText DASTに表示されず、設定に保存される際に暗号化されます。

ファイアウォール、ウィルス対策ソフトウェア、および侵入検知システム

OpenText DASTでは、攻撃をサーバに送信し、結果を分析して保存します。このようなアクティビティを防止するために、Webアプリケーションファイアウォール(WAF)、ウィルス対策ソフトウェア、ファイアウォール、および侵入検知/防止システム(IDS/IPS)が用意されています。そのため、脆弱性のスキャンを実行する際に、これらのツールが問題になることがあります。

まず、これらのツールは、OpenText DASTによるサーバのスキャンに干渉する可能性があります。OpenText DASTからサーバに送信される攻撃が傍受されて、サーバへの要求が失敗する可能性があります。サーバがその攻撃に対して脆弱な場合は、検出漏れが発生する可能性があります。

第二に、結果や攻撃がOpenText DAST製品内にある場合、ディスク上にローカルにキャッシュされている場合、またはデータベース内にある場合、これらのツールによって特定されて検疫されることがあります。OpenText DASTで使用される作業ファイルまたはデータベース内のデータが検疫されると、OpenText DASTでの結果に矛盾が生じる可能性があります。また、このような検疫済みのファイルとデータによって、予期しない動作が発生する可能性もあります。

この種の問題は環境に固有のものですが、McAfee IPSは両方の種類の問題の原因となることが知られており、WAFはどれも最初の問題の原因となります。OpenTextでは、これらのツールに関連する他の問題も確認されています。

スキャンの実行中にこのような問題が発生した場合、OpenTextでは、スキャン中はWAF、ウィルス対策ソフトウェア、ファイアウォール、およびIDS/IPSツールを無効にすることをお勧めします。この方法が信頼できるスキャン結果を確実に取得できる唯一の方法です。

考慮すべき影響

どの種類の監査でも、OpenText DASTによって多数のHTTP要求が送信されますが、その多くには「無効」パラメータが含まれています。処理速度の遅いシステムでは、要求の量のせいで他のユーザからのアクセス速度が低下したり、アクセスが拒否されたりすることがあります。また、侵入検知システムを使用している場合は、多数の不正アクセス試行が識別されることになります。

徹底スキャンを実行するため、OpenText DASTでは、アプリケーション内にあるすべてのページ、フォーム、ファイル、およびフォルダの識別が試みられます。サイトのWeb探索中にフォームを送信するオプションを選択すると、OpenText DASTによって、検出されたすべてのフォームが入力されて送信されます。これにより、アプリケーション内でOpenText DASTのシームレスな移動が可能になりますが、次のような結果が生じる場合があります。

- 通常、ユーザがフォームを送信すると、アプリケーションで電子メールや電子掲示板の投稿が作成されて、(製品サポートまたは販売グループ宛などに)送信されるようになっている場合、OpenText DASTでもプローブの一環としてこれらのメッセージが生成されます。
- 通常のフォーム送信によってデータベースにレコードが追加されるようになっている場合、OpenText DASTから送信されるフォームによって擬似的なレコードが作成されます。

スキャンの監査段階で、OpenText DASTは、アプリケーションの問題を特定するため、考えられるあらゆるパラメータを操作して、何度もフォームを再送信します。これにより、作成されるメッセージとデータベースレコードの数が大幅に増加します。

役に立つヒント

- クライアントから送信されたフォームに基づいてバックエンドサーバ(データベース、LDAPなど)にレコードを書き込むシステムの場合、運用システムを監査する前にデータベースをバックアップして、監査の完了後に復元するOpenText DASTユーザもいます。これを実施できない場合は、監査後にサーバにクエリを実行して、OpenText DASTから送信された1つ以上のフォーム値を含むレコードを検索して削除できます。これらの値は、Web Form Editorツールを開くことで特定できます。詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Web Form Editor」の章を参照してください。

- ユーザが送信したフォームに応答して電子メールメッセージが生成される場合は、電子メールサーバを無効にすることを検討してください。または、すべての電子メールをキューにリダイレクトしてから、監査後に、OpenText DASTから送信されたフォームに応答して生成されたこれらの電子メールを手動で確認して削除することもできます。
- OpenText DASTは、最大75の同時HTTP要求を送信してから、最初の要求に対するHTTP応答を待機するように設定できます。デフォルトのスレッド数設定は、Web探索では5、監査では10です(別々のリクエスタを使用する場合)。環境によっては、アプリケーションまたはサーバに障害が発生しないように、より小さい値を指定する必要があります。詳細については、「"スキャン設定:リクエスタ" ページ414」を参照してください。
- 何らかの理由で、OpenText DASTで特定のディレクトリに対してWeb探索と攻撃をしない場合は、OpenText DAST設定の除外URL機能を使用して、これらのディレクトリを指定する必要があります("スキャン設定:セッション除外" ページ418を参照)。また、特定のファイルタイプとMIMEタイプを除外することもできます。
- デフォルトでは、OpenText DASTは、Webアプリケーションで一般的に見られる多くのバイナリファイル(イメージやドキュメントなど)を無視するように設定されています。これらのドキュメントは、Web探索や攻撃ができないため、監査する価値はありません。これらのドキュメントをバイパスすることにより、監査速度が大幅に向上します。専有ドキュメントが使用中である場合は、ドキュメントのファイル拡張子を決定し、OpenText DASTのデフォルト設定内で除外します。Web探索中にOpenText DASTの動作が極端に遅くなったり、停止したりした場合は、バイナリドキュメントをダウンロードしようとしたことが原因である可能性があります。
- フォーム送信の場合、事前にパッケージ化されたファイルから抽出されたデータがOpenText DASTによって送信されます。特定の値(ユーザ名やパスワードなど)が必要な場合は、Web Form Editorツールでファイルを作成し、そのファイルをOpenText DASTで識別する必要があります。詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Web Form Editor」の章を参照してください。
- 対話型のスキャンを実行する場合を除き、CAPTCHAソフトウェアはオフにしてください。CAPTCHAはWebアプリケーションでの自動化を防止するように設計されているため、Webアプリケーションの自動スキャンに干渉する可能性があります。
- OpenText DASTでは、サーバへのファイルのアップロードを試行することで、特定の脆弱性がテストされます。これがサーバで許可された場合、この脆弱性はOpenText DASTによってスキャンレポートに記録され、このファイルの削除が試みられます。ただし、サーバ側でファイルの削除が阻止されることがあります。このため、スキャン後の保守では、「CreatedByHP」で始まる名前のファイルを検索して削除することを日常業務の一環としてください。

参照情報

"OpenText DASTの概要" ページ29

"クイックスタート" 下

クイックスタート

このトピックでは、OpenText DASTを使い始める際に役立つ情報を提供します。さらに詳しい情報へのリンクも含まれています。

SecureBaseの更新

OpenText DASTの脆弱性のカタログに関する最新の情報を確実に取得するには、次の手順に従って脆弱性データベースを更新します。

1. OpenText DASTを起動します。

   注記: OpenText DASTが、Fortify WebInspect Enterpriseの対話型コンポーネントとしてインストールされている場合、およびエンタープライズサーバが現在このOpenText DASTモジュールを使用してスキャンを実行している場合は、OpenText DASTを起動できません。次のメッセージが表示されます:「WebInspectを起動できません。許可が拒否されました。(Unable to start WebInspect. Permission denied.)」

2. **[開始ページ(Start Page)]**で、**[スマートアップデートの開始(Start Smart Update)]**をクリックします。

   [スマートアップデート(Smart Update)]ウィンドウが開き、使用可能な更新が一覧表示されます。

3. **[更新(Update)]**をクリックします。

注記: 製品を使用するたびに更新を行います。プログラムを起動するたびにスマートアップデートを実行するアプリケーション設定を選択できます。詳細については、「"アプリケーション設定:スマートアップデート" ページ505」を参照してください。

オフラインのOpenText DASTの更新手順を含む詳細については、"SmartUpdate" ページ324を参照してください。

システムを監査用に準備する

監査を実行する前に、Webサイトに与える潜在的な影響、および正常な監査のための準備作業に注意してください。詳細については、「"システムの監査準備" ページ41」を参照してください。

スキャンを開始する

データベースを更新すると、Webアプリケーションのセキュリティ脆弱性を判断する準備が整います。

OpenText DASTの**[開始ページ(Start Page)]**で、次のいずれかの選択肢をクリックします。

- **ガイド付きスキャンの開始**("ガイド付きスキャンの概要" ページ111を参照)
- **基本スキャンの開始**("基本スキャンの実行(Webサイトスキャン)" ページ199を参照)
- **APIスキャンの開始**("APIスキャンウィザードの使用" ページ165を参照)
- **エンタープライズスキャンの開始**("エンタープライズスキャンの実行" ページ227を参照)

参照情報

"システムの監査準備" ページ41

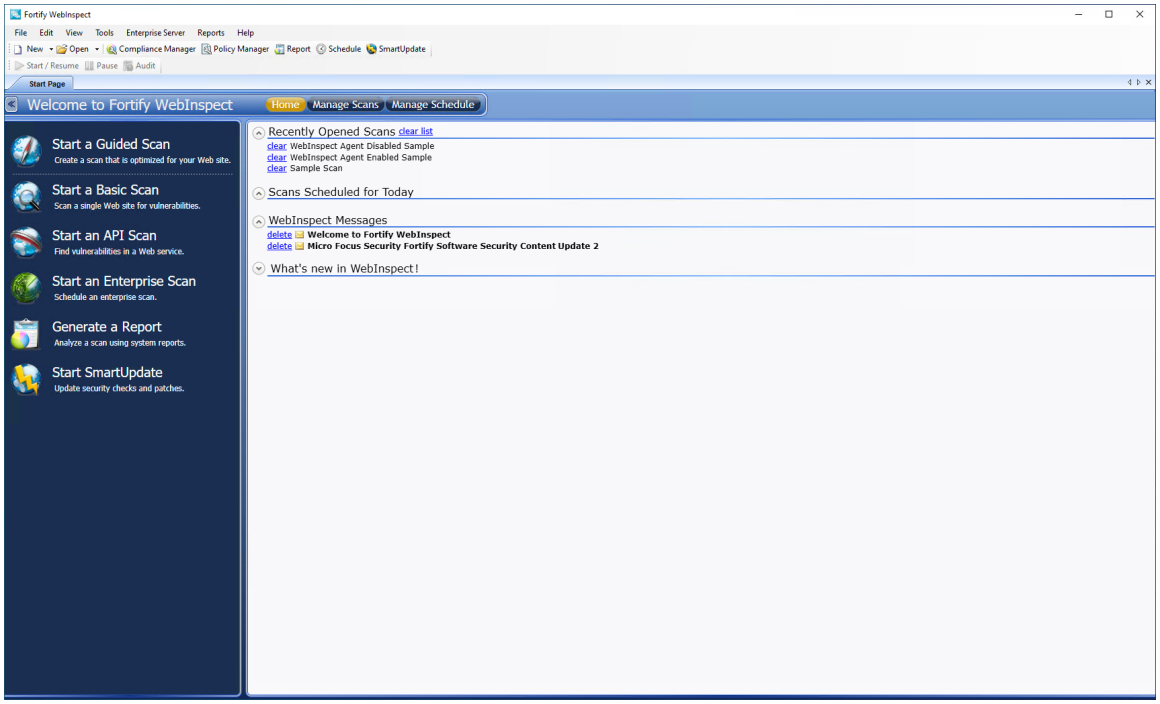
"OpenText DASTユーザインタフェース" ページ46

第3章:OpenText DASTユーザインタフェース

OpenText DASTを初めて開始するときには、以下に示すように、アプリケーションで **[開始ページ(Start Page)]** が表示されます。

[開始ページ(Start Page)] のイメージ

注記: OpenText DASTがエンタープライズサーバに接続されている場合は、[SmartUpdate] ボタンの右側に「WebInspect Enterprise WebConsole」というラベルのボタンがあります。このボタンによってWebコンソールが起動します。



アクティビティパネル

左側のペイン(アクティビティパネル)には、以下の主要な機能へのハイパーリンクが表示されます。

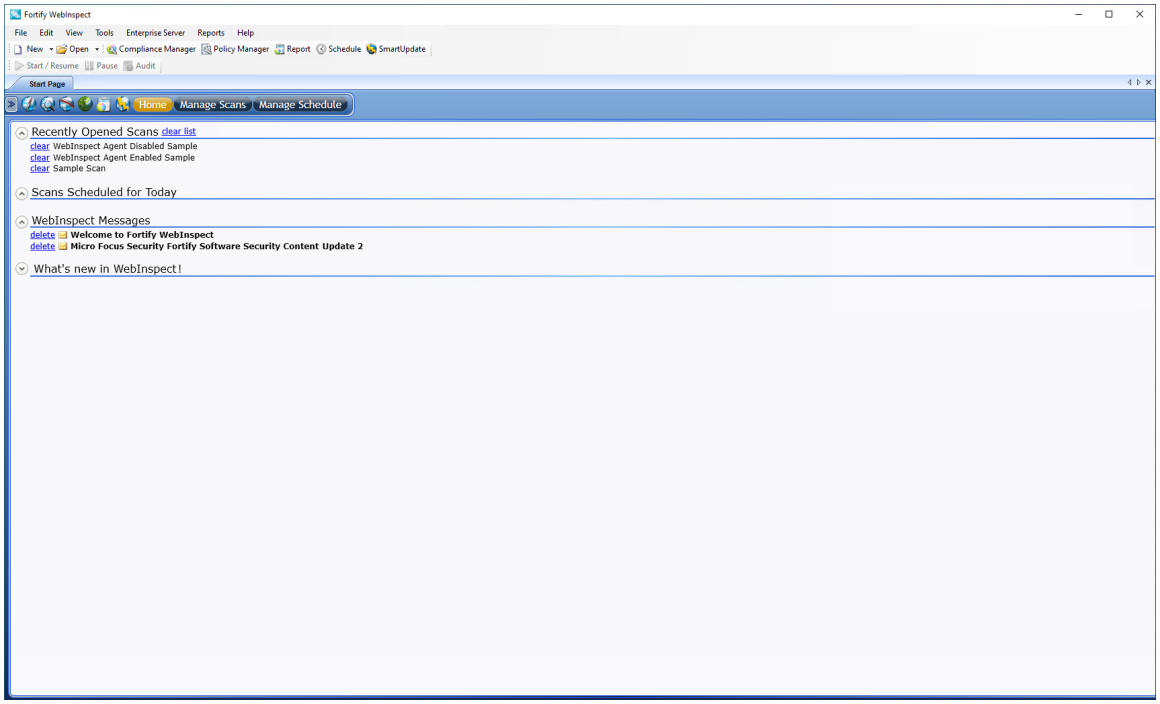
- ガイド付きスキャンの開始("ガイド付きスキャンの概要" ページ111を参照)
- 基本スキャンの開始("基本スキャンの実行(Webサイトスキャン)" ページ199を参照)
- APIスキャンの開始("APIスキャンウィザードの使用" ページ165を参照)
- エンタープライズスキャンの開始("エンタープライズスキャンの実行" ページ227を参照)

- レポートの生成("レポートの生成" ページ306を参照)
- SmartUpdateの開始("SmartUpdate" ページ324を参照)

アクティビティパネルを閉じる

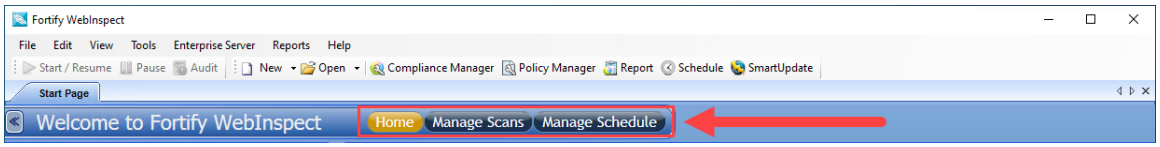
ペインの上のバーの左矢印をクリックすると、アクティビティパネルを閉じることができます。

アクティビティパネルがない[開始ページ(Start Page)]のイメージ



ボタンバー

右側のペインの内容は、次のイメージで示されているボタンバーで選択したボタンによって決まります。



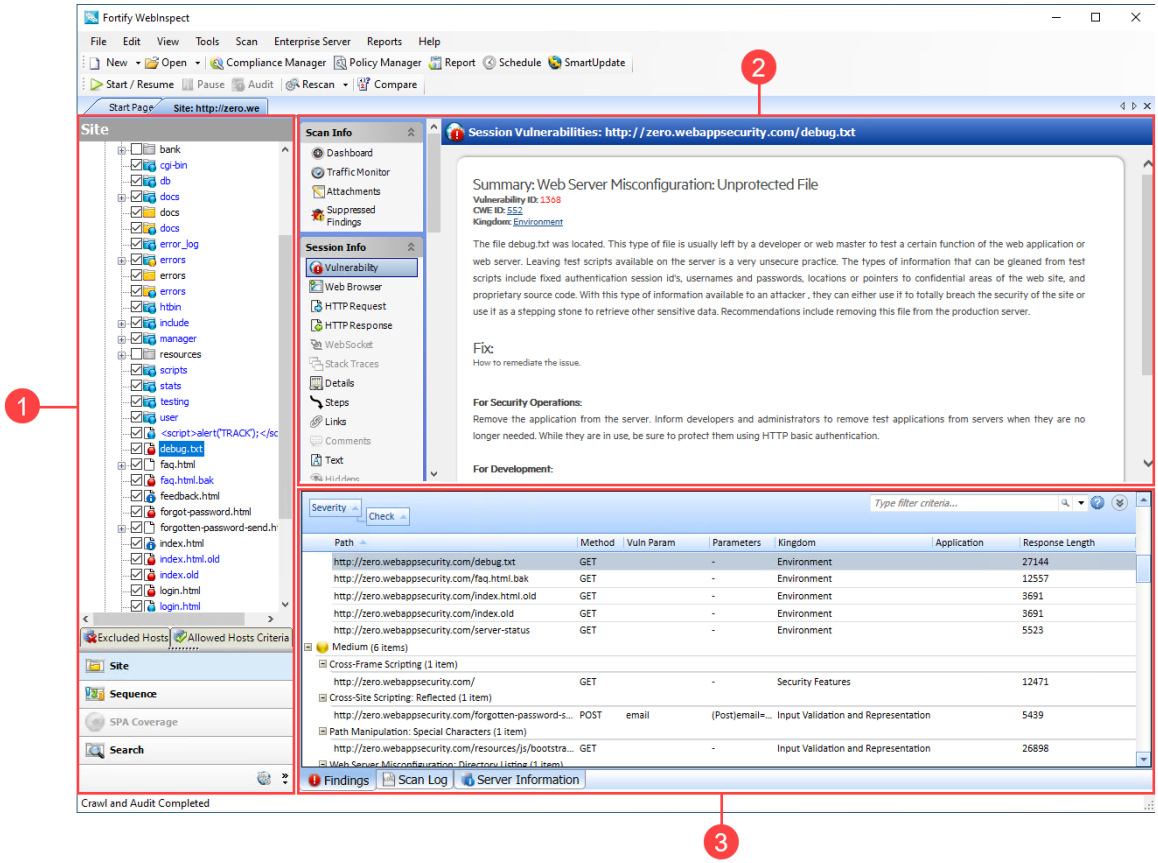
次の表で、選択肢について説明します。

ボタン	表示されるリスト
ホーム	最近開いたスキャンのリストと、今日実行予定のスキャン、最近生成さ

ボタン	表示されるリスト
	れたレポート、およびOpenTextサーバからダウンロードされたメッセージが表示されます。 ポインタをスキャン名の上に置くと、OpenText DASTにスキャンに関する概要情報が表示されます。スキャン名をクリックすると、OpenText DASTの別のタブでスキャンが開かれます。
スキャンの管理	以前に実行したスキャンのリストが表示されます。スキャンを開いたり、名前変更したり、削除したりできます。 **接続(Connections)**]をクリックして、ローカル(自分のマシン上のSQL Server Express Editionデータベースに保存されているスキャン)またはリモート(自分のマシン上またはネットワーク上の別の場所に設定されたSQL Server Standard Editionデータベースに保存されているスキャン)、またはその両方のデータベースを選択します。詳細については、「"スキャンの管理" ページ244」を参照してください。
スケジュールの管理(Manage Schedule)	実行予定のスキャンのリストを表示します。スキャンをスケジュールに追加したり、スケジュールされたスキャンを編集または削除したり、手動でスキャンを開始したりできます。詳細については、「"スケジュールされたスキャンの管理" ページ248」を参照してください。

スキャンに関連付けられたペイン

スキャンを開くか実行するたびに、OpenText DASTは、ターゲットサイトの名前または説明のラベルが付いたタブを開きます。この作業エリアは、次の図に示されている3つの領域に分かれています。



項目	説明
1	ナビゲーションペイン
2	情報ペイン
3	サマリペイン

同時に多数のスキャンを開いていて、すべてのタブを表示するスペースがない場合は、タブバーの最右端にある矢印をクリックしてタブをスクロールできます。選択したタブを閉じるには、Xをクリックします。

参照情報

"メニューバーについて" ページ51

"ツールバー" ページ57

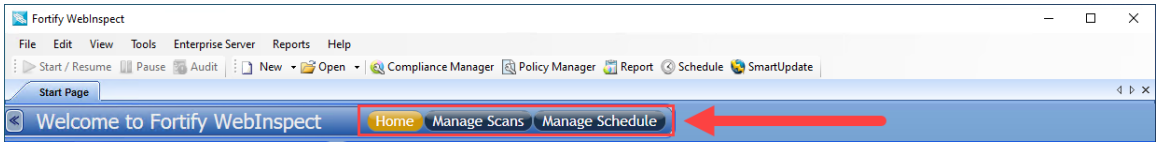
"開始ページ(Start Page)" 下
"ナビゲーションペイン" ページ61
"サマリペイン" ページ104
"情報ペイン" ページ72

開始ページ(Start Page)

[**開始ページ(Start Page)**]の左側のペインには、Webサイト、API、またはWebサービスの脆弱性スキャンに関連するアクティビティのリストが表示されます。

- ガイド付きスキャンの開始("ガイド付きスキャンの概要" ページ111を参照)
- 基本スキャンの開始("基本スキャンの実行(Webサイトスキャン)" ページ199を参照)
- APIスキャンの開始("APIスキャンウィザードの使用" ページ165を参照)
- エンタープライズスキャンの開始("エンタープライズスキャンの実行" ページ227を参照)
- レポートの生成("レポートの生成" ページ306を参照)
- SmartUpdateの開始("SmartUpdate" ページ324を参照)

右側のペインの内容は、ボタンバーのボタンによって制御されます。



ホーム

[**ホーム(Home)**]が選択されている場合(デフォルト)、OpenText DASTに以下のリストが表示されます。

- 最近開かれたスキャン。
  ポインタをスキャン名の上に置くと、OpenText DASTにスキャンに関する概要情報が表示されます。スキャン名をクリックすると、OpenText DASTの別のタブでスキャンが開かれます。
- 今日実行予定のスキャン
- 最近生成されたレポート
- OpenTextサーバからダウンロードされたメッセージ

スキャンの管理

[**スキャンの管理(Manage Scans)**]が選択されている場合、以前に実行されたスキャンのリストがOpenText DASTに表示されます。スキャンを開いたり、名前変更したり、削除したりできます。 [**接続(Connections)**]をクリックして、ローカル(自分のマシン上のSQL Server Express Editionデータベースに保存されているスキャン)またはリモート(SQL Server データ

ベース(設定されている場合)に保存されているスキャン)、またはその両方のデータベースを選択します。詳細については、「"スキャンの管理" ページ244」を参照してください。

スケジュールの管理(Manage Schedule)

[**スケジュールの管理(Manage Schedule)**]が選択されている場合、スケジュールされたスキャンのリストがOpenText DASTに表示されます。スキャンをスケジュールに追加したり、スケジュールされたスキャンを編集または削除したり、手動でスキャンを開始したりできます。詳細については、「"スケジュールされたスキャンの管理" ページ248」を参照してください。

参照情報

"OpenText DASTユーザインタフェース" ページ46

メニューバーについて

メニューバーのオプションは次のとおりです。

[ファイル(File)]メニュー

[**ファイル(File)**]メニューのコマンドについて、次の表で説明します。

コマンド	説明
新規(New)	ガイド付きスキャン、基本スキャン、APIスキャン、またはエンタープライズスキャンを選択できます。次いで関連するスキャンウィザードが起動して、スキャン開始のプロセスのステップを示します。
開く	スキャンまたは生成されたレポートを開くことができます。
スケジュール(Schedule)	[スケジュールされたスキャンの管理(Manage Scheduled Scans)]ウィンドウを開きます。このウィンドウでは、スケジュールされたスキャンを追加、編集、または削除できます。

コマンド	説明
スキャンのインポート	スキャンファイルをインポートできます。
エクスポート	このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。以下を実行できます。 • スキャンをエクスポートする • スキャン詳細をエクスポートする • Software Security Centerにスキャンをエクスポートする • Webアプリケーションファイアウォール(WAF)に保護ルールをエクスポートする
[閉じる]タブ	複数のタブが開いている場合に、選択したタブを閉じます。 **ヒント:** 開いている任意のタブを右クリックし、以下のコンテキストメニューオプションを使用できます。 • **閉じる**-クリックしたタブを閉じます。 • **これ以外をすべて閉じる(Close All But This)** -クリックしたタブを除くすべてのタブを閉じます。 • **すべて閉じる(Close All)** -すべてのタブを閉じます 同様に、中央クリックまたは<CTRL>+<F4>を使用して、1つのタブを閉じることができます。 再テストスキャンのためにタブを閉じる場合、スキャンの保持に関するプロンプトが表示されることがあります。詳細については、「"脆弱性の再テスト" ページ271」を参照してください。
終了(Exit)	OpenText DASTプログラムを終了します。

編集(Edit)]メニュー

編集(Edit)]メニューのコマンドについて、次の表で説明します。

コマンド	説明
デフォルトのスキャン設定	デフォルト設定(Default Settings)]ウィンドウを表示し、スキャンに使用するオプションを選択または変更できるようにします。
現在のスキャン	現在のスキャンのオプションを選択または変更できる設定ウィンドウを表

コマンド	説明
設定(Current Scan Settings)	示します。このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。
設定の管理(Manage Settings)	設定ファイルを追加、編集、または削除できるウィンドウを表示します。
アプリケーション設定	[アプリケーション設定(Application Settings)]ウィンドウを表示します。このウィンドウでは、OpenText DASTアプリケーションの操作を制御するオプションを選択または変更できます。詳細については、『"アプリケーション設定" ページ480』を参照してください。
URLのコピー(Copy URL)	選択したURLをWindowsクリップボードにコピーします。このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。
スキャンログのコピー(Copy Scan Log)	(選択したタブのスキャン用に)ログをWindowsクリップボードにコピーします。このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。

表示(View)]メニュー

表示(View)]メニューのコマンドについて、次の表で説明します。

コマンド	説明
折り返し(Word Wrap)	HTTP要求およびHTTP応答を表示するときに、表示エリアの右側の余白にソフトリターンを挿入します。このコマンドは、スキャンを含むタブが選択されている場合にのみ使用できます。
ツールバー	表示するツールバーを選択できます。詳細については、「"ツールバー" ページ57」を参照してください。

[ツール(Tools)]メニュー

[ツール(Tools)]メニューには、ツールアプリケーションを起動するコマンドが含まれています。

[スキャン(Scan)]メニュー

[スキャン(Scan)]メニューは、スキャンを含むタブにフォーカスがある場合にのみメニューバーに表示されます。 [スキャン(Scan)]メニューのコマンドについて、次の表で説明します。

コマンド	説明
開始/再開(Start/Resume)	スキャンを開始します。または、処理を一時停止した後で再開します。
一時停止	Web探索または監査を停止します。スキャンを続行するには、 **再開(Resume)**]をクリックします。
監査	Web探索を実行したサイトの脆弱性を評価します。このコマンドは、Web探索の完了後、またはステップモードを終了した後に使用します。
再スキャン(Rescan)	選択したスキャンで最後に使用された設定が事前入力された状態で [スキャンウィザード(Scan Wizard)]を起動します。 再スキャン(Rescan)]ドロップダウンメニューでは、次の項目を実行できます。 • もう一度スキャンする(Scan Again) ("サイトの再スキャン" ページ276を参照) • 脆弱性の再テスト(Retest Vulnerabilities) ("脆弱性の再テスト" ページ271を参照) • 増分の再利用(Reuse Incremental) ("増分スキャン" ページ278を参照) • 改善の再利用(Reuse Remediation) ("スキャンの再利用" ページ277を参照)
比較	同じターゲットに対する2つの異なるスキャンによって明らかになった脆弱性を比較します。「"スキャンの比較" ページ238」を参照してください。

[エンタープライズサーバ(Enterprise Server)]メニュー

[エンタープライズサーバ(Enterprise Server)]メニューには、次のコマンドが含まれています。

コマンド	説明
[WebInspect Enterpriseへの接続(Connect to WebInspect Enterprise)]または**[切断(Disconnect)]**	Fortify WebInspect Enterpriseサーバへの接続を確立または解除します。
スキャンのダウンロード(Download Scan)	サーバからハードドライブにコピーするスキャンを選択できるようにします。
スキャンの発行(Publish Scan)	ダイアログボックスが表示され、そこで脆弱性を確認して、エンタープライズサーバに送信できます。次いで脆弱性はFortify Software Security Centerサーバに送信されます。詳細については、「"スキャンの発行(Fortify WebInspect Enterprise接続)" ページ265」を参照してください。 **注記:** このオプションは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ使用できます。
スキャンのアップロード(Upload Scan)	サーバにデータを転送するスキャンを選択できます。ほとんどの場合、これは、アプリケーション設定**[スキャンの自動アップロード(auto upload scans)]**が選択されていない場合に使用されます。
設定の転送(Transfer Settings)	OpenText DAST設定ファイルを選択してサーバに転送できます。サーバで、これらの設定に基づいてスキャンテンプレートが作成されます。また、スキャンテンプレートを選択してOpenText DASTに転送することもできます。これにより、テンプレートに基づいて設定ファイルが作成されます。詳細については、「"エンタープライズサーバとの間での設定の転送" ページ264」を参照してください。
WebConsole	Fortify WebInspect EnterpriseのWebコンソールアプリケーションを起動します。

コマンド	説明
Enterprise Serverについて(About Enterprise Server)	Fortify WebInspect Enterpriseに関する情報を表示します。

注記: スタンドアロンライセンスを使用するOpenText DASTインストールシステムは、ユーザがFortify WebInspect Enterprise内の役割のメンバーである限り、いつでもエンタープライズサーバに接続できます。

[レポート(Reports)]メニュー

[レポート(Reports)]メニューのコマンドについて、次の表で説明します。

コマンド	説明
レポートの生成(Generate Report)	Report Generatorを起動します。
レポートの管理	標準レポートおよびカスタムレポートの種類の一覧が表示されます。カスタム設計されたレポートの名前変更、削除、またはエクスポートと、レポート定義ファイルのインポートを行えます。

[ヘルプ(Help)]メニュー

[**ヘルプ(Help)**]メニューには、このトピックで説明するコマンドが表示されます。

DASTヘルプ

このコマンドは、ヘルプファイルを開きます。

サポート

このコマンドは、カスタマサポートに連絡するための手順を表示します。

チュートリアル(Tutorials)

このコマンドは、OpenText DAST用のFortify Unplugged YouTube™チャンネルを開きます。

DASTコミュニティ

このコマンドは、ディスカッション、ヒント、セキュリティブログ、ニュース、およびイベントを提供するFortifyコミュニティを開きます。

DASTについて

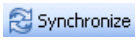
このコマンドは、ライセンス情報、許可ホスト、属性など、OpenText DASTアプリケーションに関する情報を表示します。

ツールバー

OpenText DASTウィンドウには、2つのツールバー(スキャンツールバーと標準ツールバー)があります。ツールバーを表示または非表示にするには、 [**表示(View)**]メニューから [**ツールバー(Toolbars)**]を選択します。

スキャンツールバーで使用可能なボタン

ボタン	機能
Start / Resume	スキャンを一時停止してからスキャンを再開できます。完了したスキャンには、(タイムアウトまたはその他のエラーによる)未送信のセッションが含まれていることがあります。 [**開始(Start)**]を

ボタン	機能
	クリックすると、OpenText DASTはそれらのセッションの再送信を試行します。
	実行中のスキャンを中断します。スキャンを続行するには、 **開始/再開(Start/Resume)**]ボタンをクリックします。
	Web探索のみのスキャンまたはステップモードスキャンを実行する場合は、実行後にこのボタンをクリックして監査を実行できます。詳細については、「"手動スキャンの実行" ページ231」を参照してください。
	このボタンは、スキャンを含むタブを選択した場合にのみ表示されます。 再スキャン(Rescan)]ドロップダウンメニューでは、次の項目を実行できます。 • もう一度スキャンする(Scan Again) ("サイトの再スキャン" ページ276を参照) • 脆弱性の再テスト(Retest Vulnerabilities) ("脆弱性の再テスト" ページ271を参照) • 増分の再利用(Reuse Incremental) ("増分スキャン" ページ278を参照) • 改善の再利用(Reuse Remediation) ("スキャンの再利用" ページ277を参照) 詳細については、「"再テストと再スキャン" ページ271」を参照してください。
	このボタンは、スキャンを含むタブを選択した場合にのみ表示されます。これにより、同じターゲットに対する2つの異なるスキャンによって明らかになった脆弱性を比較できます。詳細については、「"スキャンの比較" ページ238」を参照してください。
	このボタンは、OpenText DASTがFortify WebInspect Enterpriseに接続されており、フォーカスがあるタブでスキャンが開いている場合にのみ表示されます。スキャン設定をFortify WebInspect Enterpriseに送信できます。これにより、スキャン要求が作成され、次に利用可能なセンサのスキャンキューに入れられます。詳細情報については、"Fortify WebInspect Enterpriseでのスキャンの実行" ページ263を参照してください。
	このボタンは、Fortify WebInspect Enterpriseに接続した後でのみ表示されます。Fortify Software Security Centerアプリ

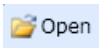
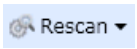
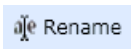
ボタン	機能
	ケーションとバージョンを指定できます。OpenText DASTは次にFortify Software Security Centerから脆弱性のリストをダウンロードし、ダウンロードした脆弱性と現在のスキャンで検出された脆弱性を比較し、適切なステータス(新規(New)]、既存(Existing)]、再導入(Reintroduced)]、または未検出(Not Found)])を割り当てます。詳細情報については、"Fortify Software Security Centerへの脆弱性対策の統合" ページ 267を参照してください。 **注記:** このオプションは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ使用できます。
Publish	このボタンは、Fortify WebInspect Enterpriseに接続した後でのみ表示され、OpenText DASTをFortify Software Security Centerと同期した後に有効になります。Fortify WebInspect EnterpriseからFortify Software Security Centerにアプリケーションバージョンデータをアップロードします。 **注記:** このオプションは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ使用できます。

標準ツールバーで使用可能なボタン

ボタン	機能
New	ガイド付きスキャン、基本スキャン、APIスキャン、またはエンタープライズスキャンを選択できます。次いで関連するスキャンウィザードが起動して、スキャン開始のプロセスのステップを示します。
Open	スキャンまたはレポートを開くことができます。
Compliance Manager	Compliance Managerを起動します。
Policy Manager	Policy Managerを起動します。

ボタン	機能
	Report Generatorを起動します。
	スキャンが特定の日時に実行されるようにスケジュールを設定できます。詳細については、「"スキャンのスケジュール" ページ247」を参照してください。
	中央のOpenTextデータベースと通信して、ご使用のシステムに適用できるアップデートがあるかどうかを判別し、アップデートがある場合はアップデートをインストールできるようにします。詳細については、「"SmartUpdate" ページ324」を参照してください。
	Fortify WebInspect Enterprise Webコンソールアプリケーションを起動します。このボタンは、Fortify WebInspect Enterpriseに接続している場合にのみ表示されます。

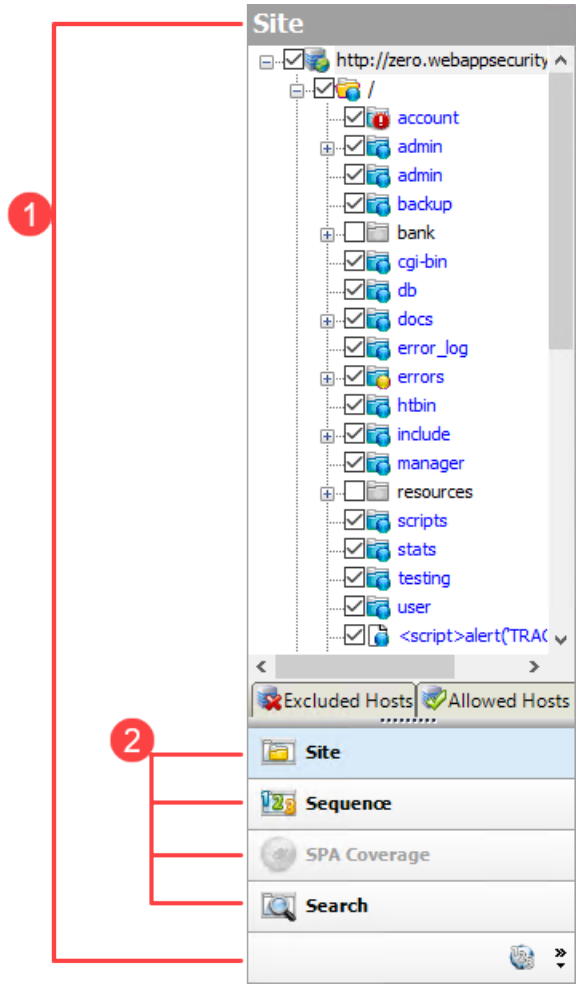
[スキャンの管理(Manage Scans)]ツールバーで使用可能なボタン

ボタン	機能
	スキャンを開くには、1つ以上のスキャンを選択して **[開く(Open)]**をクリックします(または、単にリスト内のエントリをダブルクリックします)。OpenText DASTによってスキャンデータがロードされ、それぞれのスキャンは個別のタブに表示されます。
	選択したスキャンで最後に使用された設定が取り込まれた状態でスキャンウィザードを起動するには、 **[再スキャン(Rescan)] > [もう一度スキャンする(Scan Again)]をクリックします。** 前回のスキャンで明らかになった脆弱性を含むセッションのみを再スキャンするには、スキャンを選択して、 **[再スキャン(Rescan)] > [脆弱性の再テスト(Retest Vulnerabilities)]**をクリックします。 詳細については、「"再テストと再スキャン" ページ271」を参照してください。
	選択したスキャンの名前を変更するには、 **[名前変更(Rename)]**をクリックします。

ボタン	機能
Delete	選択したスキャンを削除するには、 [**削除(Delete)**]をクリックします。
Import	スキャンをインポートするには、 [**インポート(Import)**]をクリックします。
Export	スキャンのエクスポート、スキャンの詳細のエクスポート、Fortify Software Security Centerへのスキャンのエクスポート、またはWAF (Webアプリケーションファイアウォール)への保護ルールのエクスポートを行うには、 [**エクスポート(Export)**]のドロップダウン矢印をクリックします。
Compare	スキャンを比較するには、(<Ctrl>を押しながらクリックして) 2つのスキャンを選択し、 [**比較(Compare)**]をクリックします。詳細については、「"スキャンの比較" ページ238」を参照してください。
Connections	デフォルトでは、ローカルSQL Server Express Editionと設定済みのSQL Server Standard Editionに保存されているスキャンがすべてOpenText DASTによって一覧表示されます。一方または両方のデータベースを選択する、またはSQL Server接続を指定するには、 [**接続(Connections)**]をクリックします。
Refresh	必要に応じて、 [**更新(Refresh)**]をクリックして表示を更新します。
Columns	表示する列を選択するには、 [**列(Columns)**]をクリックします。 [**上へ移動(Move Up)**]ボタンと [**下へ移動(Move Down)**]ボタンを使用して列を表示する順序を並べ替えたり、 [**スキャンの管理(Manage Scans)**]リストで、単に列見出しをドラッグアンドドロップしたりすることができます。

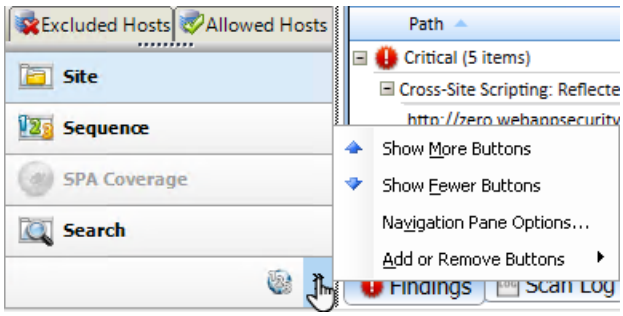
ナビゲーションペイン

スキャンを実行または表示すると、OpenText DASTウィンドウの左側にナビゲーションペインが表示されます。ナビゲーションペインに表示される内容(または「ビュー」)を決定する [**サイト(Site)**]ボタン、 [**シーケンス(Sequence)**]ボタン、 [**SPAカバレッジ(SPA Coverage)**]ボタン、 [**検索(Search)**]ボタン、および [**ステップモード(Step Mode)**]ボタンが含まれています。



項目	説明
1	ナビゲーションペイン
2	表示を変更するボタン

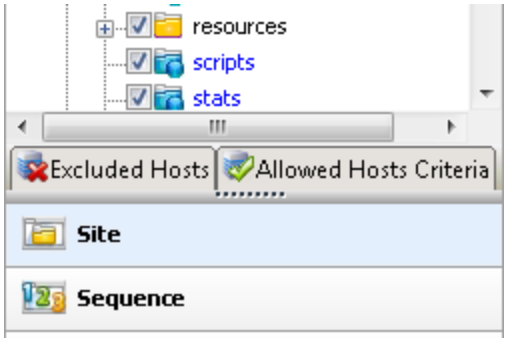
すべてのボタンが表示されていない場合は、ボタンリストの下部にあるドロップダウン矢印をクリックし、 **他のボタンを表示(Show More Buttons)**]を選択します。



サイトビュー

OpenText DASTのナビゲーションペインにはWebサイトまたはWebサービスの階層構造だけが表示され、それに加えて脆弱性が検出されたセッションが表示されます。サイトのWeb探索中、OpenText DASTでは各セッションの横のチェックボックスが選択され(デフォルト)、セッションの監査も行われることが示されます。Web探索と監査を順次実行する場合(サイトが完全にWeb探索されてから監査される場合)、監査を開始する前に関連するチェックボックスをオフにすることで、セッションを監査から除外できます。

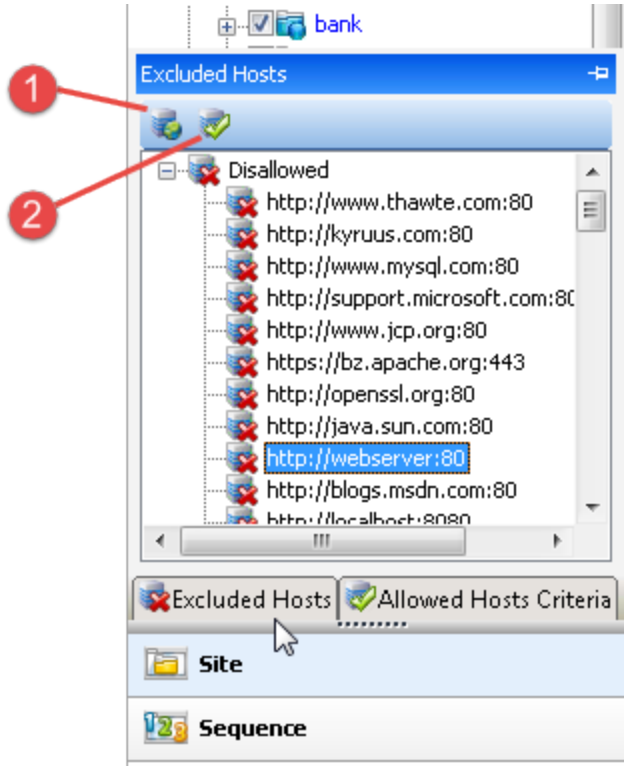
サイトビューには、 **除外ホスト(Excluded Hosts)**]と **許可ホストの基準(Allowed Hosts Criteria)**]という2つのポップアップタブもあります。



除外ホスト

除外ホスト(Excluded Hosts)]タブをクリックする(またはその上にポインタを置く)と、タブには許可されていないすべてのホストの一覧が表示されます。これらは、ターゲットサイト内の任意の場所から参照できるホストですが、 **許可ホスト(Allowed Hosts)**]設定(**デフォルトまたは現在のスキャン設定(Default/Current Scan Settings)**]> **スキャン設定(Scan Settings)**]> **許可ホスト(Allowed Hosts)**])で指定されていないので、スキャンできません。

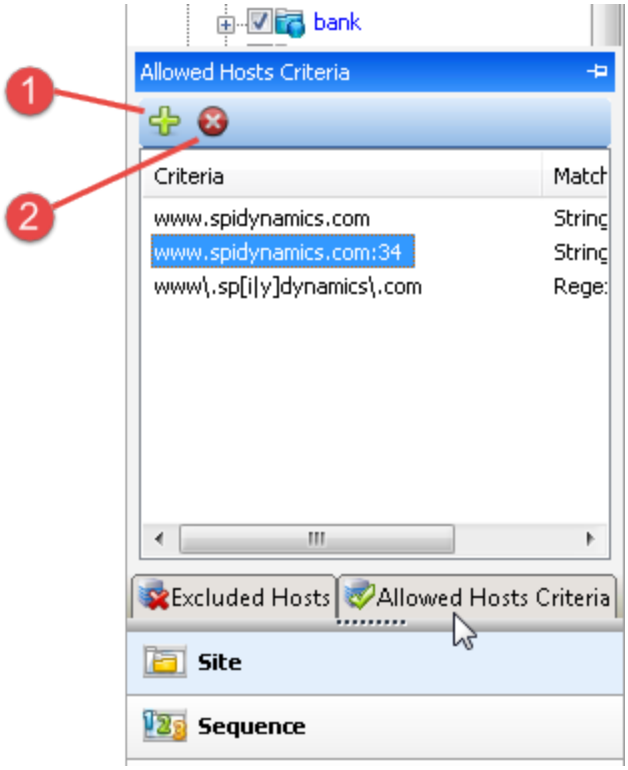
除外ホスト(Excluded Hosts)]タブを使用して、除外ホストを選択し、 **スキャンに追加(Add to scan)**]または **許可ホストの基準を追加(Add allowed host criteria)**]をクリックできます。



項目	説明
1	スキャンに追加-ホストをスキャンに追加すると、ホストルートディレクトリを表すノードがサイトツリー内に作成されます。OpenText DASTは、そのセッションをスキャンします。
2	許可ホストの基準を追加-許可ホストの基準にホストを追加すると、 [現在のスキャン設定(Current Scan Settings)]の許可ホストの一覧にURLが追加されます。OpenText DASTは、そのホストへの後続のリンクをスキャンに含めます。ただし、OpenText DASTがすでにそのホストへのリンクを含む唯一のリソースをスキャンした後で、許可ホストの基準にホストを追加した場合、追加されたホストはスキャンされません。

許可ホストの基準

[許可ホストの基準(Allowed Hosts Criteria)]タブをクリックする(またはその上にポインタを置く)と、OpenText DASTのスキャン設定(**[許可ホスト(Allowed Hosts)]**の下)で指定されたURL(または正規表現)がタブに表示されます。 **[削除(Delete)]**または **[許可ホストの基準を追加(Add allowed host criteria)]**をクリックすると、OpenText DASTで **[現在の設定(Current Settings)]**ダイアログボックスが開き、許可ホストの基準(リテラルURLまたはURLを表す正規表現)を追加、編集、または削除できます。



項目	説明
1	許可ホストの基準を追加-エントリを追加すると、OpenText DASTでは基準に一致するホストへの後続のリンクをスキャンに含めます。ただし、OpenText DASTがすでにそのホストへのリンクを含む唯一のリソースをスキャンした後で、ホストを指定した場合、追加されたホストはスキャンされません。
2	削除-許可ホストの一覧からエントリを削除した場合でも、OpenText DASTですでに検出したリソースはすべてスキャンに含まれます。

後でスキャンするためにこれらの設定を保存するには、 [設定(Settings)]ウィンドウの左ペインの下にある **[設定に名前を付けて保存(Save settings as)]**を選択します。

除外ホストまたは許可ホストの基準を変更する前に、スキャンを一時停止する必要があります。さらに、スキャンを一時停止したポイントによっては、追加または削除されたホストのスキャンが期待どおりに行われない可能性があります。たとえば、OpenText DASTがすでに追加されたホストへのリンクを含む唯一のリソースをスキャンした後で、許可ホストを追加した場合、追加されたホストはスキャンされません。

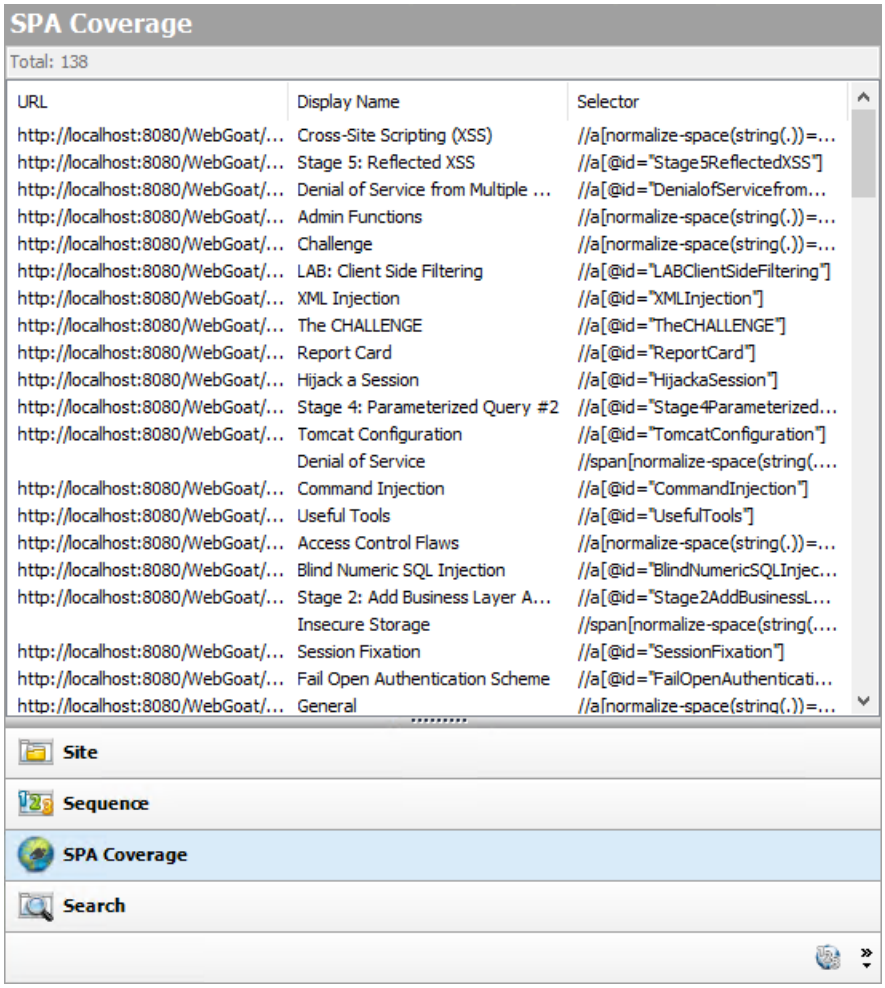
[シーケンス(Sequence)]ビュー

[シーケンス(Sequence)]ビューには、スキャン中にOpenText DASTが検出した順序でサーバリソースが表示されます。

注記: [サイト(Site)]ビューと[シーケンス(Sequence)]ビューのどちらにおいても、青いテキストで示されるのは、リンクを介して検出されたリソースではなく、OpenText DASTによって「推測された」ディレクトリまたはファイルです。たとえば、OpenText DASTは、ターゲットWebサイトに「backup」という名前のディレクトリが含まれているかどうかを検出する試行の際、要求「GET /backup/ HTTP/1.1」を常時送信します。

SPAカバレッジ(SPA Coverage)

[SPAカバレッジ(SPA Coverage)]ビューは、SPAサポートがスキャンに対して有効になっている場合にのみ使用できます。このビューには、Web探索プログラムがWeb探索中に操作したページ内の要素が表示されます。



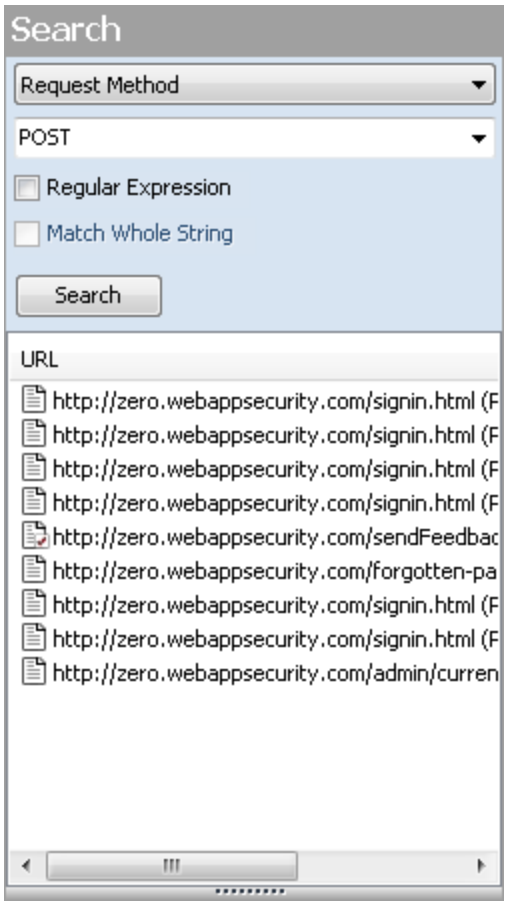
[SPAカバレッジ(SPA Coverage)]ビューには、要素が検出されたURLと、次の追加情報が一覧表示されます。

- **表示名(Display Name)** -表示されるテキスト、記号、リンク、HTMLタグ名、または検出された要素に関連するその他のUI情報。
- **セレクタ(Selector)** -ページ内の要素のXPathの場所。これは、要素に対する操作の検索と実行に使用されます。

詳細については、「"シングルページアプリケーションスキャンについて" ページ235」を参照してください。

[検索(Search)]ビュー

[検索(Search)]ビューでは、すべてのセッションでさまざまなHTTPメッセージコンポーネントを検索できます。たとえば、ドロップダウンリストから **[要求メソッド(Request Method)]**を選択し、検索文字列として **[POST]**を指定すると、OpenText DASTはHTTP要求がPOSTメソッドを使用しているすべてのセッションを一覧表示します。



[検索(Search)]ビューを使用するには:

1. ナビゲーションペインで、 **[検索(Search)]**をクリックします(ペインの下部)。
   すべてのボタンが表示されてはいない場合は、ボタンリストの下部にある **[ボタンの設定(Configure Buttons)]**ドロップダウンリストをクリックし、 **[他のボタンを表示(Show More Buttons)]**を選択します。
2. 一番上のリストから、検索するエリアを選択します。
3. コンボボックスで、検索する文字列を入力または選択します。
4. 文字列が正規表現を表している場合は、 **[正規表現(Regular Expression)]**チェックボックスをオンにします。詳細については、「"正規表現" ページ354」を参照してください。

5. 検索文字列と完全に一致する文字列全体をHTTPメッセージ内で検索するには、**[文字列全体を照合する(Match Whole String)]**チェックボックスをオンにします。完全一致では、大文字と小文字は区別されません。

   注記: このオプションは、特定の検索ターゲットには使用できません。

6. **[検索(Search)]**をクリックします。

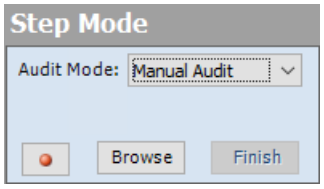
[ステップモード(Step Mode)]ビュー

ステップモードは、**[サイト(Site)]**ビューまたは**[シーケンス(Sequence)]**ビューで選択したセッションから始めて、サイト内を手動で移動する場合に使用します。

次のステップに従って、サイトをステップごとに移動します。

1. **[サイト(Site)]**または**[シーケンス(Sequence)]**ビューで、セッションを選択します。
2. **[ステップモード(Step Mode)]**ボタンをクリックします。

   ボタンが表示されていない場合は、**[ボタンの設定(Configure Buttons)]**ドロップダウンをクリックし、**[他のボタンを表示(Show More Buttons)]**を選択します。
3. ナビゲーションペインに**[ステップモード(Step Mode)]**が表示されたら、**[監査モード]**リストから**[ブラウズ時に監査する(Audit as you browse)]**か**[手動監査(Manual Audit)]**を選択します。**[手動監査(Manual Audit)]**をお勧めします。

4. **[記録(Record)]**をクリックします。
5. **[参照(Browse)]**をクリックします。

   選択したブラウザが開き、選択したセッションに関連付けられている応答が表示されます。必要な数のページを引き続き参照できます。
6. 完了したら、OpenText DASTに戻って**[完了(Finish)]**をクリックします。

   新しいセッションがナビゲーションペインに追加されます。
7. ステップ3で**[手動監査(Manual Audit)]**を選択した場合は、Auditをクリックします。

   OpenText DASTは、ステップモードで追加(または置換)したセッションを含む、監査されていないすべてのセッションを監査します。

ナビゲーションペインのアイコン

次の表を使用して、ナビゲーションペインに表示されるリソースを識別します。

ナビゲーションペインで使用されるアイコン

アイコン	説明
	サーバ/ホスト: サイトのツリー構造の最上位を表します。
	青色のフォルダ: Web探索ではなく「推測」によって検出されたフォルダです。
	黄色のフォルダ: Webサイト上でコンテンツを使用できるフォルダです。
	灰色のフォルダ: パスの切り捨てによる項目の検出を示すフォルダです。親が検出されると、フォルダはプロパティに応じて青または黄色で表示されます。
	ファイル。
	クエリまたはポスト。
	DOMイベント。

フォルダまたはファイルに重なって表示されるアイコンは、検出された脆弱性を示します

アイコン	説明
	感嘆符付きの赤い点は、オブジェクトに重大な脆弱性が含まれていることを示します。攻撃者は、サーバ上でコマンドを実行したり、個人情報を取得および変更したりできる可能性があります。
	赤色の点は、オブジェクトに高レベルの脆弱性が含まれていることを示します。一般に、ソースコード、Webルート外のファイル、および機密性の高いエラーメッセージの表示が可能になります。
	金色の点は、オブジェクトに中程度レベルの脆弱性が含まれていることを示します。これらは通常、HTML以外のエラーや、機密性が高い可能性がある問題です。
	青色の点は、オブジェクトに低レベルの脆弱性が含まれていることを示します。これらは通常注目すべき問題、またはより高いレベルの問題になる可能性のある問題です。
	青色の円の中にある「i」は、情報項目を示します。これらは、サイト内の興味深い点、または特定のアプリケーションやWebサーバです。
	赤色のチェックマークは、「ベストプラクティス」違反を示します。

ナビゲーションペインのショートカットメニュー

[サイト(Site)]ビューまたは[シーケンス(Sequence)]ビューの使用中にナビゲーションペインで項目を右クリックすると、ショートカットメニューに次のオプションが表示されます。

- **子の展開*(Expand Children*)** - ([サイト(Site)]ビューのみ)サイトツリーのブランチノードを展開します。
- **子の折りたたみ*(Collapse Children*)** - ([サイト(Site)]ビューのみ)ブランチノードを上位ノードに短縮します。
- **すべてをオン(Check All*)** - ([サイト(Site)]ビューのみ)親ノードとすべての子のチェックボックスをオンにします。
- **すべてをオフ(Uncheck All*)** - ([サイト(Site)]ビューのみ)親ノードとすべての子のチェックボックスをオフにします。
- **セッションレポートの生成*(Generate Session Report*)** - ([サイト(Site)]ビューのみ)選択したセッションの概要情報、攻撃の要求と攻撃の応答、URLとのリンク、コメント、フォーム、電子メールアドレス、およびチェックの説明を示すレポートを作成します。
- **サイトツリーのエクスポート*(Export Site Tree*)** - ([サイト(Site)]ビューのみ)指定した場所にXML形式でサイトツリーを保存します。
- **URLのコピー(Copy URL)** - URLをWindowsのクリップボードにコピーします。
- **ブラウザで表示(View in Browser)** - HTTP応答をブラウザで表示します。
- **リンク(Links)** - ([サイト(Site)]ビューのみ)選択したリソースへのリンクが含まれている、ターゲットサイトのすべてのリソースを一覧表示します。リンクは、HTMLタグ、スクリプト、またはHTMLフォームによってレンダリングできます。また、選択したセッションのHTTP応答内のリンクによって参照されるすべてのリソースも([リンク先(Linked To)]の下に)一覧表示されます。表示されているリンクをダブルクリックすると、OpenText DASTによって、ナビゲーションペインのフォーカスが、参照されているセッションに移動します。または、Webブラウザでセッションを表示することにより、リンクされたリソースを参照することもできます([Webブラウザ(Web Browser)]をクリック)。
- **追加(Add)** - OpenText DASTスキャン以外の方法(手動検査、その他のツールなど)で検出された場所を情報として追加できます。その後、検出された脆弱性をそれらの場所に追加して、サイトのより完全な説明を分析用にアーカイブできます。
  - **ページ(Page)** -個別のURL (リソース)。
  - **ディレクトリ(Directory)** -ページのコレクションを含むフォルダ。

    [**ページ(Page)**]または[**ディレクトリ(Directory)**]を選択すると、ディレクトリまたはページに名前を付けてHTTP要求と応答を編集するためのダイアログボックスが表示されます。
  - **バリエーション(Variation)** -その場所の特定の属性を一覧にした場所のサブノード。たとえば、*login.asp*の場所には、「*(Query) Username=12345&Password=12345&Action=Login"*」というバリエーションがあります。バリエーションは、サブノードに加えて脆弱性が付加されている可能性があるという点で、他の場所と同じです。

[バリエーション(Variation)]を選択すると、[バリエーションの追加(Add Variation)]ダイアログボックスが表示されます。このダイアログボックスでは、バリエーション属性の編集、*Post*または*Query*の指定、およびHTTP要求と応答の編集を行うことができます。

- **脆弱性(Vulnerability)** -セキュリティ上の特定の脅威。

  [脆弱性(Vulnerability)]を選択すると、[脆弱性の編集(Edit Vulnerabilities)]ダイアログボックスが表示されます。このダイアログボックスでは、バリエーション属性の編集、*Post*または*Query*の指定、およびHTTP要求と応答の編集を行うことができます。詳細については、「"脆弱性の編集" ページ296」を参照してください。

- **脆弱性の編集(Edit Vulnerabilities)** -手動で追加した場所を編集したり、脆弱性を編集したりすることができます。詳細については、「"脆弱性の編集" ページ296」を参照してください。
- **場所の削除(Remove Location)** -選択したセッションをナビゲーションペイン([サイト(Site)]ビューと[シーケンス(Sequence)]ビューの両方)から削除し、関連する脆弱性もすべて削除します。

  注記: 削除された場所(セッション)およびそれに関連する脆弱性を回復できます。詳細については、「"削除されたセッションの回復" ページ304」を参照してください。

- **マーク付けする(Mark as)** -脆弱性に誤検出のフラグを付けます。説明を追加できます。脆弱性がリストから削除されます。[スキャン情報(Scan Info)]パネルで**[抑制された検出事項(Suppressed Findings)]**を選択すると、すべての誤検出および無視された脆弱性のリストを表示できます。

  注記: 抑制された検出事項を脆弱性に戻すことができます。詳細については、「"抑制された検出事項" ページ83」を参照してください。

- **送信先(Send to)** - OpenText DASTのアプリケーション設定で指定されたプロファイルを使用して、選択した脆弱性を欠陥に変換し、OpenText Application Lifecycle Management (ALM)に割り当てることができます。
- **サーバの削除(Remove Server)** -ナビゲーションペインからサーバを削除し、残りのスキャンアクティビティにそのサーバを含めないようにします。このコマンドは、サーバを右クリックした場合にのみ表示されます。
- **Web探索(Crawl)** -選択したURLのWeb探索を再実行します。
- **添付ファイル(Attachments)** -選択したセッションに関連するメモの作成、フォローアップのためのセッションへのフラグ付け、脆弱性のメモの追加、脆弱性スナップショットの追加を行うことができます。
- **ツール(Tools)** -使用可能なツールのサブメニューを表示します。
- **現在のセッションでフィルタ(Filter by Current Session)** -サマリペイン内の項目の表示を、選択したセッションのSummaryDataIDを持つ項目に制限します。

*ナビゲーションペインで[サイト(Site)]ビューを使用している場合のみ、ショートカットメニューにコマンドが表示されます。

参照情報

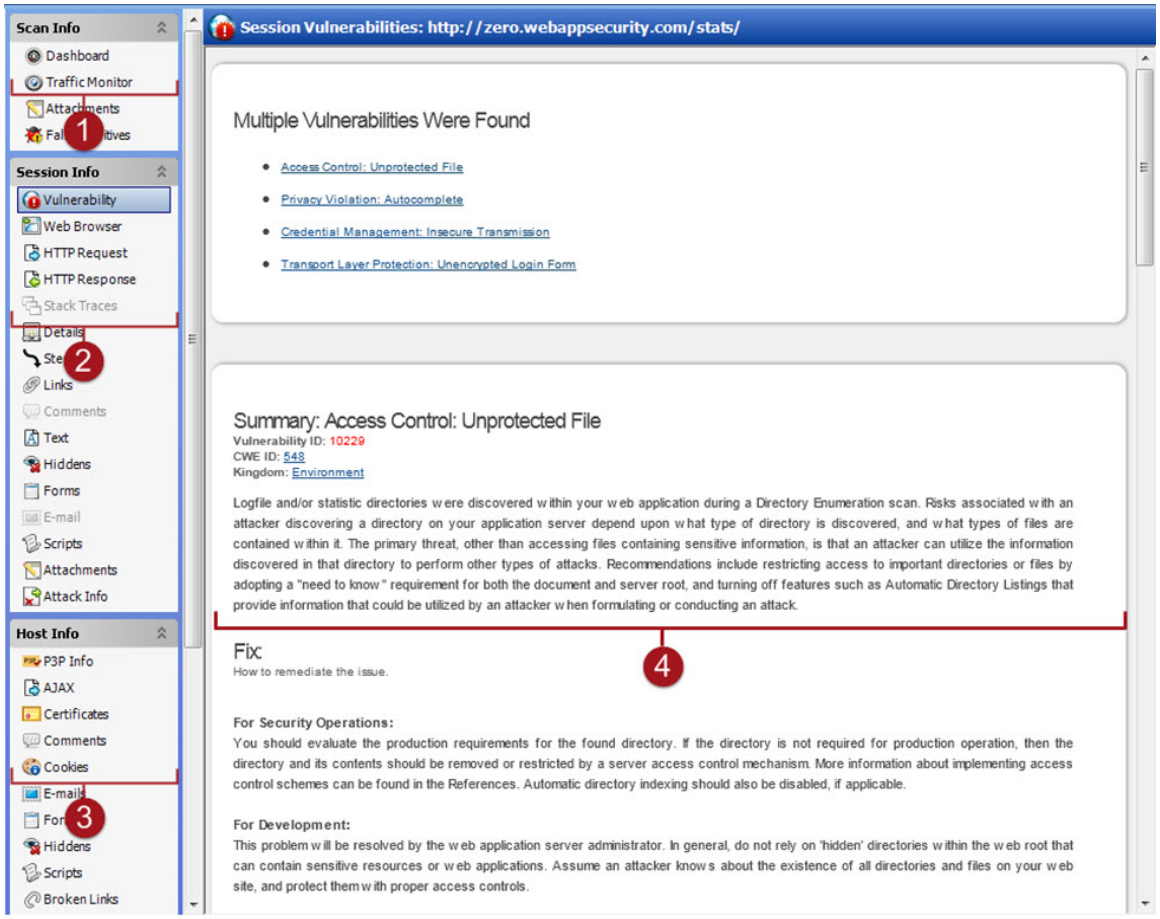
"OpenText DASTユーザインタフェース" ページ46

"[検索(Search)]ビュー" ページ289

"結果の検査" ページ284

情報ペイン

スキャンを実行または表示する際、情報ペインに、3つの折りたたみ可能な情報パネルと、1つの情報表示エリアが表示されます。



項目	説明
1	[スキャン情報(Scan Info)]パネル(" [スキャン情報(Scan Info)]パネル" 次のページを参照)
2	[セッション情報(Session Info)]パネル(" [セッション情報(Session Info)]パネル" ページ86を参照)
3	[ホスト情報(Host Info)]パネル(" [ホスト情報(Host Info)]パネル" ページ95を参照)
4	情報表示エリア

左側の列にあるこれらの3つの情報パネルの1つで項目をクリックし、表示する情報のタイプを選択します。

ヒント: 脆弱性情報を表示する際にリンクをたどる場合、ナビゲーションペインで強調表示されたセッションをクリックすると戻ることができます。

参照情報

"サマリペイン" ページ104

"OpenText DASTユーザインタフェース" ページ46

"ナビゲーションペイン" ページ61

"[スキャン情報(Scan Info)]パネル" 下

"[セッション情報(Session Info)]パネル" ページ86

"[ホスト情報(Host Info)]パネル" ページ95

[スキャン情報(Scan Info)]パネル

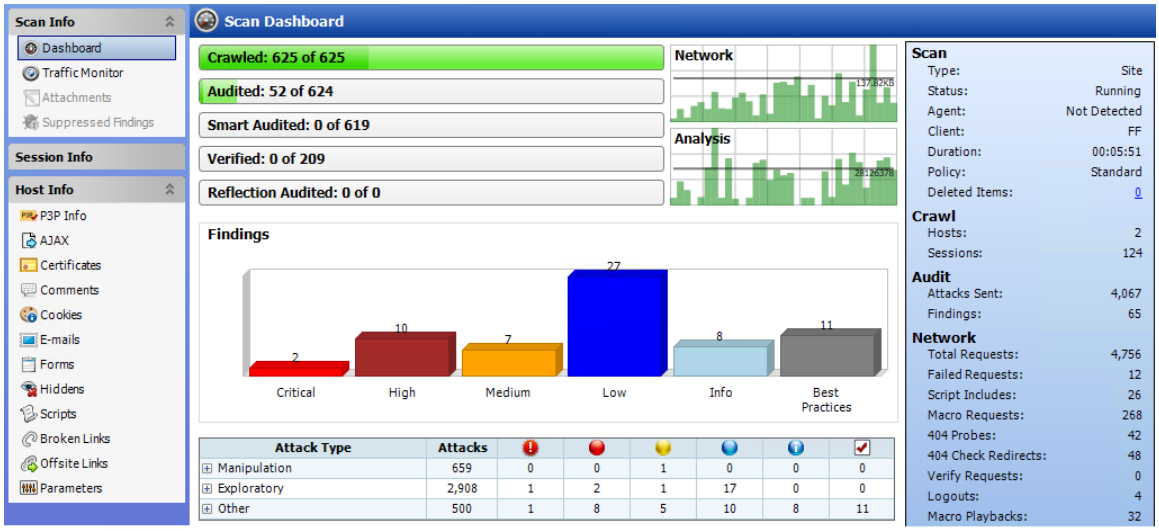
[スキャン情報(Scan Info)]パネルには、次の選択肢があります。

- ダッシュボード
- Traffic Monitor
- 添付ファイル
- 抑制された検出事項

ダッシュボード

[ダッシュボード(Dashboard)]を選択すると、スキャン結果のリアルタイムの概要とスキャン進行状況のグラフィックが表示されます。このセクションは**[デフォルト(Default)]**または**[現在の設定(Current)]**でこのオプションを選択した場合にのみ表示されます。詳細については、"ダッシュボード" ページ76を参照してください。

ダッシュボードのイメージ



Traffic Monitor

OpenText DASTのナビゲーションペインには、通常、Webサイトまたは Webサービスの階層構造だけが表示され、それに加えて脆弱性が検出されたセッションが表示されます。Traffic MonitorまたはTraffic Viewerを使用すると、OpenText DASTによって送信されたすべてのHTTP要求と、Webサーバから受信した関連するHTTP応答を表示および確認できます。

Traffic MonitorまたはTraffic Viewerは、スキャンの実行前にTraffic Monitorロギングが有効になっている場合にのみ利用できます。

詳細については、「"Traffic Monitor (Traffic Viewer)" ページ282」を参照してください。

添付ファイル(Attachments)

[添付ファイル(Attachments)]を選択すると、スキャンに追加されたすべてのセッションのメモ、脆弱性のメモ、フォローアップ用フラグ、および脆弱性スクリーンショットの一覧が表示されます。各添付ファイルは、特定のセッションに関連付けられています。このフォームには、スキャンメモ(特定のセッションではなく、スキャン全体に適用されるメモ)も一覧表示されます。

スキャンメモを作成したり、既存の添付ファイルを編集または削除したりできます。

スキャンメモを作成するには、(情報表示エリアの) **[追加(Add)]**メニューをクリックします。

添付ファイルを編集するには、添付ファイルを選択して **[編集(Edit)]**をクリックします。

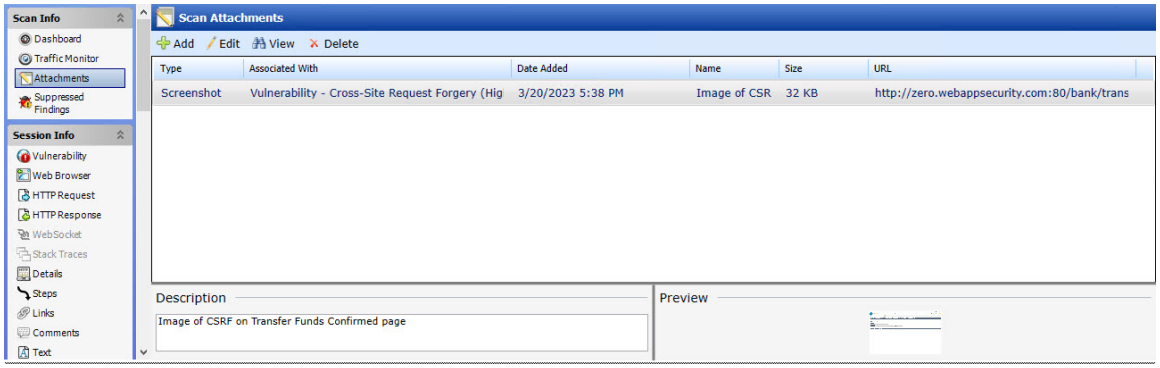
OpenText DASTユーザインタフェースの他のエリアで添付ファイルを作成するには、次のいずれかを実行します。

- ナビゲーションペインでセッションを右クリックし、ショートカットメニューから **[添付ファイル(Attachments)]**を選択します。
- サマリペインの **[検出事項(Findings)]**タブでURLを右クリックし、ショートカットメニューから **[添付ファイル(Attachments)]**を選択します。

OpenText Application Lifecycle Management (ALM)に不具合を送信すると、OpenText DASTによってメモが自動的にセッションに追加されます。

詳細については、「"添付ファイル(Attachments) -スキャン情報(Scan Info)" ページ82」を参照してください。

添付ファイルのイメージ

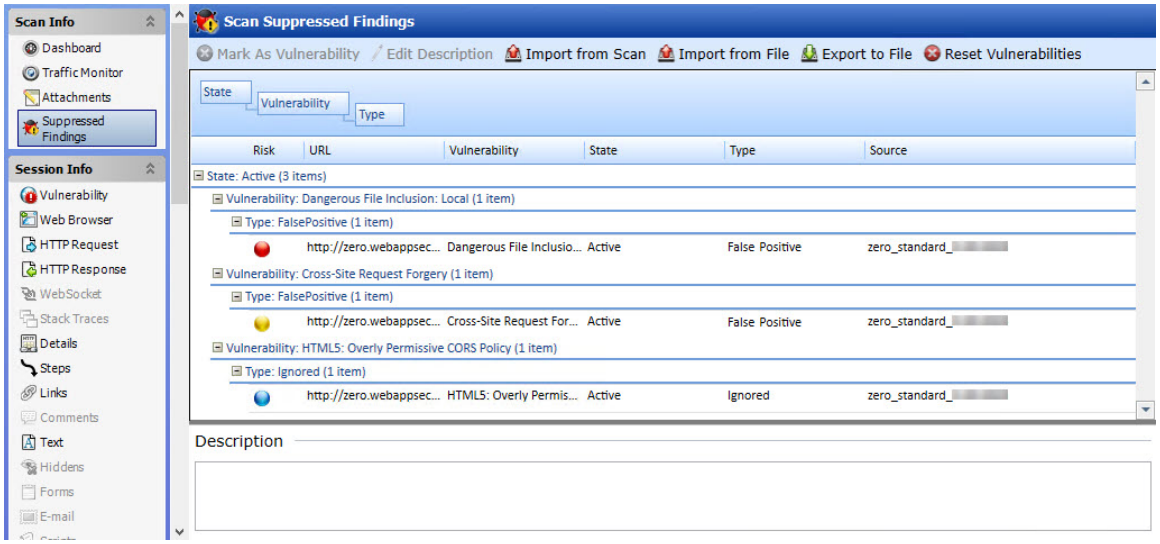


抑制された検出事項

この機能は、OpenText DASTが脆弱性を含むものとして最初にフラグを立てたものの、後でユーザが誤検出と判断したか無視することにしたすべてのURLを一覧表示します。

詳細については、「"抑制された検出事項" ページ83」を参照してください。

抑制された検出事項のイメージ



参照情報

" セッション情報(Session Info)]パネル" ページ86
" ホスト情報(Host Info)]パネル" ページ95
"OpenText DASTユーザインタフェース" ページ46
"ダッシュボード" 次のページ

"Traffic Monitor (Traffic Viewer)" ページ282

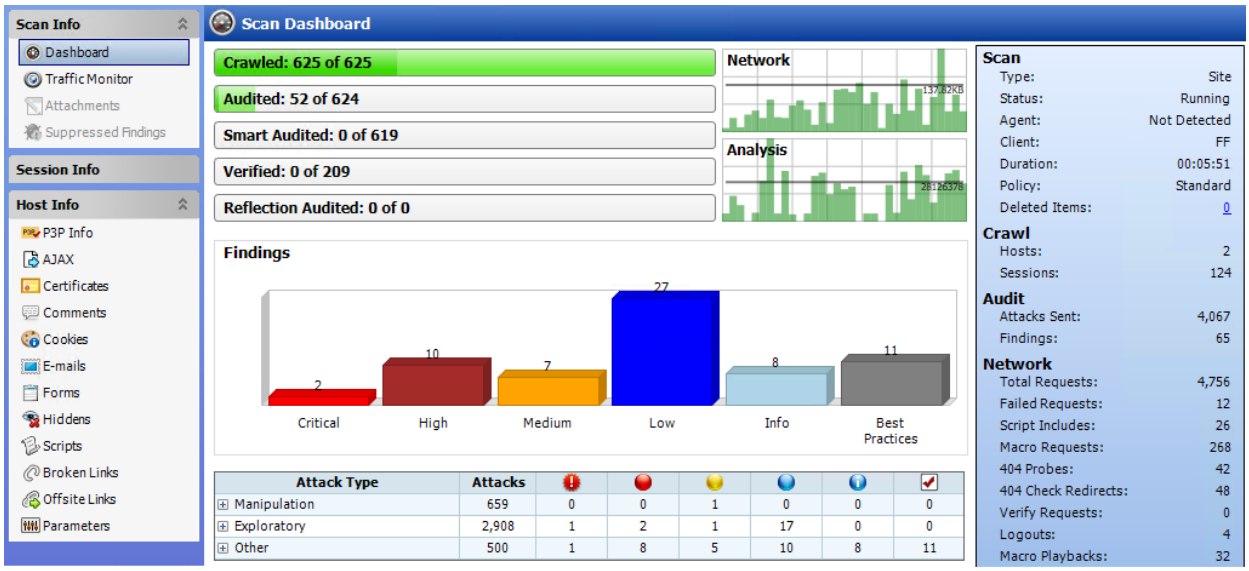
"添付ファイル(Attachments) -スキャン情報(Scan Info)" ページ82

ダッシュボード

ダッシュボード(Dashboard)]を選択すると、スキャン結果のリアルタイムの概要とスキャン進行状況のグラフィックが表示されます。

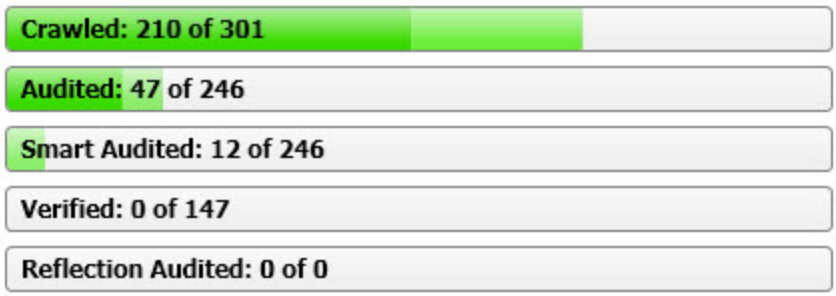
ダッシュボードのイメージ

次のイメージは、スキャンが進行中のスキャンダッシュボードを示しています。



進行状況バー

各バーは、そのスキャンフェーズにおける進行状況を表します。

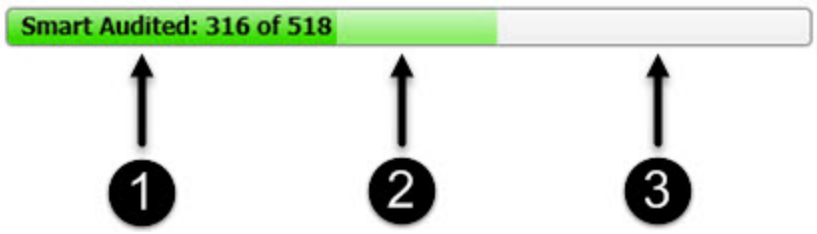


進行状況バーの説明

次の表に、進行状況バーの説明を示します。

進行状況バー	説明
Web探索済み (Crawled)	Web探索済みのセッションの数/Web探索するセッションの総数。
監査済み (Audited)	監査済みのセッションの数/監査するセッションの総数。 総数には、スマート監査によって処理されるサーバタイプに関連するもの以外のすべてのチェックが含まれます。
スマート監査済み(Smart Audited)	スマート監査を使用して監査済みのセッションの数/スマート監査のセッションの総数。 スマート監査では、OpenText DASTが、Webアプリケーションをホストしているサーバのタイプを検出します。OpenText DASTは、サーバタイプに固有のチェックを実行し、サーバタイプに対して有効でないチェックを回避します。
検証済み (Verified)	検証済みの永続的XSS脆弱セッションの数/検証する永続的XSS脆弱セッションの総数。 永続的XSS監査が有効になっている場合は、OpenText DASTが、脆弱なすべてのセッションに対して2件目の要求を送信し、OpenText DASTが過去に行ったプローブに対するすべての応答を検査します。プローブが特定された場合は、OpenText DASTがそれらのページ間のリンクを内部的に記録します。
反射監査済み (Reflection Audited)	監査済みの永続的XSS脆弱リンク済みセッションの数/監査する永続的XSS脆弱リンク済みセッションの総数。 永続的XSS監査が有効になっている場合は、永続的XSSの検証ステップで検出されたリンク済みセッションを監査するために必要な作業を表します。

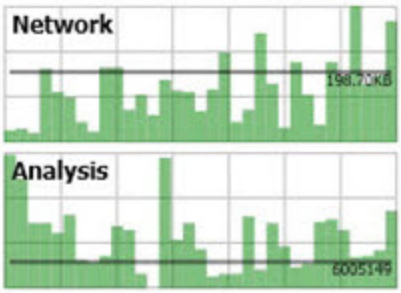
進行状況バーの色



1. 濃い緑色は、処理されたセッションを表します。
2. 薄い緑色は、除外、中止、または拒否されたセッション(処理対象と見なされていたが、設定などの理由でスキップされたセッション)を表します。
3. 薄い灰色は、未処理のセッションを表します。

アクティビティメータ

OpenText DASTは、スキャンで発生しているアクティビティに関する情報をポーリングして、アクティビティメータにデータを表示します。このデータは、スキャンアクティビティのリアルタイムスナップショットを表します。この情報は、スキャンが停止しているのか、活発に動作しているのかを判断するのに役立ちます。



アクティビティメータの説明

次の表に、アクティビティメータの説明を示します。

メータ	説明
ネットワーク (Network)	OpenText DASTによって送受信されるデータの量。 グラフには、このデータが過去1秒間に送受信されたB、KB、またはMB単位で表示されます。
分析	すべてのスレッドの処理において、OpenText DASTによって1秒あたりに実行される作業の量。

検出事項のグラフィック

次の表で、 [検出事項(Findings)] の棒グラフとグリッドについて説明します。

グラフィック	説明
検出事項のグラフ	スキャンで特定された重大度レベルごとの問題の総数。
攻撃統計グリッド	攻撃の種類と監査エンジン別に分類された、行われた攻撃と検出された問題の数。

統計パネル-スキャン

次の表に、統計パネルの [スキャン(Scan)] セクションの説明を示します。

項目	説明
Type	スキャンのタイプ: [サイト(Site)]、[サービス(Service)]、または [サイト再テスト(Site Retest)]。
スキャンステータス	ステータス: [実行中(Running)]、[一時停止(Paused)]、[中断(Interrupted)]、または [完了(Complete)]。
エージェント(Agent)	OpenText DAST Agentを意味し、[検出(Detected)] または [未検出(Not Detected)] のどちらかを示します。特定のチェック(SQLインジェクション、コマンド実行、クロスサイトスクリプティングなど)の場合、OpenText DAST AgentはOpenText DAST HTTP要求を傍受し、ターゲットモジュールでランタイム分析を実行します。この分析によって脆弱性が存在することが確認されると、OpenText DAST AgentはHTTP応答にスタックトレースを追加します。開発者は、このスタックトレースを分析して、改善が必要なエリアを調査できます。
クライアント(Client)	スキャン用に指定されたレンダリングエンジン。オプションは次のとおりです。 • IE (Internet Explorer) • FF (Firefox) • iPhone • iPad • Android • Windows Phone • Windows RT
期間(Duration)	スキャンが実行されている時間の長さ(スキャンが異常終了した場合は間違っている可能性があります)。
ポリシー	スキャンに使用されるポリシーの名前。スキャンで複数のポリシーを使用した場合は、選択したポリシーの数がハイパーリンクとして表示されます。リンクをクリックすると、選択したポリシーが表示されます。
削除された項目(Deleted Items)	ユーザがスキャンから削除したセッションと脆弱性の数。 セッションを削除するには、ナビゲーションペインでセッションを右クリックし、ショートカットメニューから **[場所の削除(Remove Location)]** を選択します。詳細については、「"ナビゲーションペイン" ページ61」を参照してく

項目	説明
	ださい。 脆弱性を削除するには、サマリペインで脆弱性を右クリックし、ショートカットメニューから **[脆弱性を無視(Ignore Vulnerability)]** を選択します。詳細については、「"サマリペイン" ページ104」を参照してください。 削除されたセッションまたは脆弱性を復元するには: 1. スキャンダッシュボードで、削除された項目に関連付けられた番号をクリックします。 **[削除された項目の回復(Recover Deleted Items)]** ウィンドウが表示されます。 2. ドロップダウンメニューから **[脆弱性(Vulnerabilities)]** または **[セッション(Sessions)]** のどちらかを選択します。 3. 1つ以上の項目を選択します。 4. **[回復(Recover)]** をクリックします。

統計パネル-Web探索

次の表に、統計パネルの **[Web探索(Crawl)]** セクションの説明を示します。

項目	説明
ホスト(Hosts)	スキャンに含まれるホストの数。
セッション(Sessions)	セッションの総数(AJAX要求、スクリプトとスクリプトフレームのインクルード、およびWSDLインクルードを除く)。

統計パネル-監査

次の表に、統計パネルの **[監査(Audit)]** セクションの説明を示します。

項目	説明
送信攻撃数(Attacks Sent)	送信された攻撃の総数。
問題数(Issues)	検出された問題の総数(すべての脆弱性とベストプラクティス)。

統計パネル-ネットワーク

次の表に、統計パネルの [ネットワーク(Network)] セクションの説明を示します。

項目	説明
要求の総数 (Total Requests)	行われた要求の総数。
失敗要求数 (Failed Requests)	失敗した要求の総数。
スクリプトインクルード数(Script Includes)	スクリプトインクルードの総数。
マクロ要求数 (Macro Requests)	マクロ実行の一部として行われた要求の総数。
404プローブ (404 Probes)	「ファイルが見つからない」ステータスを判断するために発行された「ファイルが見つからない」プローブの数。
404チェックリダイレクト数(404 Check Redirects)	404プローブがリダイレクトになった回数。
検証要求数 (Verify Requests)	保存されたパラメータの検出のために行われた要求。
ログアウト数 (Logouts)	ログアウトが検出され、ログインマクロが実行された回数。
マクロ再生数 (Macro Playbacks)	マクロが実行された回数。
AJAX要求数 (AJAX Requests)	発行されたAJAX要求の総数。

項目	説明
スクリプトイベント数(Script Events)	処理されたスクリプトイベントの総数。
送信キロバイト数(Kilobytes Sent)	送信されたキロバイトの総数。
受信キロバイト数(Kilobytes Received)	受信されたキロバイトの総数。

参照情報

" [スキャン情報(Scan Info)]パネル" ページ73
" [セッション情報(Session Info)]パネル" ページ86
" [ホスト情報(Host Info)]パネル" ページ95

添付ファイル(Attachments) -スキャン情報(Scan Info)

[添付ファイル(Attachments)]を選択すると、スキャンに追加されたすべてのセッションのメモ、脆弱性のメモ、フォローアップ用フラグ、および脆弱性スクリーンショットの一覧が表示されます。各添付ファイルは、特定のセッションに関連付けられています。このフォームには、スキャンメモ(特定のセッションではなく、スキャン全体に適用されるメモ)も一覧表示されます。

スキャンメモを作成したり、既存の添付ファイルを編集または削除したりできます。

添付ファイルを表示するには、添付ファイルを選択して **[表示(View)]**をクリックします(または単に添付ファイルをダブルクリックします)。

スキャンメモを作成するには、(情報表示エリアの) **[追加(Add)]**メニューをクリックします。詳細については、「"情報ペイン" ページ72」を参照してください。

添付ファイルを編集するには、添付ファイルを選択して **[編集(Edit)]**をクリックします。スクリーンショットは編集できないことに注意してください。

これらの機能は、添付ファイルを右クリックし、ショートカットメニューからオプションを選択して使用することもできます。 **[セッションへ移動(Go to session)]**を選択すると、 [セッション情報-添付ファイル(Session Info - Attachments)]ペインが開き、その添付ファイルに関連付けられているセッションがナビゲーションペインで強調表示されます。

OpenText DASTユーザインタフェースの他のエリアで添付ファイルを作成するには、次のいずれかを実行します。

- ナビゲーションペインでセッションを右クリックし、ショートカットメニューから **[添付ファイル(Attachments)]** を選択します。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。
- サマリペインの **[検出事項(Findings)]** タブでURLを右クリックし、ショートカットメニューから **[添付ファイル(Attachments)]** を選択します。詳細については、「" [検出事項(Findings)]タブ" ページ104」を参照してください。

OpenText Application Lifecycle Management (ALM)に不具合を送信すると、OpenText DASTによってメモが自動的にセッションに追加されます。

参照情報

" [スキャン情報(Scan Info)]パネル" ページ73

抑制された検出事項

この機能は、OpenText DASTにより脆弱性を含むものとして最初にフラグを立てられたものの、ユーザによって「誤検出」または「無視(Ignore)」としてマークされたすべてのURLを一覧表示します。

抑制された検出事項について

OpenText DASTでは、次のタイプの抑制された検出事項が許可されます。

- **誤検出** - 開発者がさらに調査した結果、脆弱なURL、操作、パラメータではないと判断された検出事項。
- **無視** - セキュリティリードまたは開発者が無視することにした検出事項。一般に、これらは、悪用のリスクをほとんど伴わない低レベルまたは情報的な結果か、テスト範囲外の緩和策が存在する検出事項です。

  たとえば、安全ではない自己署名証明書を使用しているなど、サーバと同じ方法では設定されていない開発者マシンでスキャンを実行する場合があります。ただし、実稼働環境では、サーバは安全な実際の証明書を使用します。スキャン中に、OpenText DASTによってこの脆弱性にフラグが設定されますが、修正する必要がある問題ではないので、無視できます。

抑制された検出事項のインポート

以前のスキャンから、誤検出として分析された脆弱性や無視された脆弱性のリストをインポートできます。続いて、OpenText DASTは、以前のスキャンの抑制された検出事項を現在のスキャンで検出された脆弱性と相関させ、新たに出現した脆弱性に誤検出または無視のフラグを立てます。

たとえば、クロスサイトスクリプティングの脆弱性がスキャン番号1でURL http://www.mysite.com/foo/barに検出され、さらに分析を行った後、開発者がそれに誤検出のフラグを立てたとします。スキャン番号1の誤検出をwww.mysite.comのスキャン番号2にインポートした場合に、2番目のスキャンで同じURL(http://www.mysite.com/foo/bar)でクロス

サイトスクリプティングの脆弱性が検出されると、OpenText DASTは自動的にその脆弱性を誤検出に変更します。

非アクティブ/アクティブの抑制された検出事項リスト

抑制された検出事項は、インポートされると、「非アクティブな抑制された検出事項(Inactive Suppressed Findings)」というラベルのリストに最初にロードされます。そのリスト内の抑制された検出事項が現在のスキャンの脆弱性と一致する場合、その項目は「非アクティブな抑制された検出事項(Inactive Suppressed Findings)」リストから「アクティブな抑制された検出事項(Active Suppressed Findings)」リストに移動されます。一致しない項目は、「非アクティブな抑制された検出事項(Inactive Suppressed Findings)」リストに残ります。

抑制された検出事項をスキャンの設定中にロードする

スキャンウィザードでスキャンを設定する場合、特定のスキャンまたはファイルから、抑制された検出事項をロードすることができます。スキャン中、OpenText DASTは、抑制された検出事項を検出すると、それらを相互に関連付けます。スキャンの実行中に一致した誤検出をスキャンダッシュボードで確認することもできます。

抑制された検出事項の操作

1. 「**スキャン情報(Scan Info)**」パネルから「**抑制された検出事項(Suppressed Findings)**」を選択します。
2. 必要に応じて、脆弱性の説明の横にあるプラス記号(⊞)をクリックして、関連付けられているURLと状態を表示します。
3. 誤検出項目の場合は、URLをクリックして、ユーザが脆弱性を「**誤検出(False Positive)**」としてマークした際に入力したコメント(情報ペインの下部)を表示します。
4. 次の表の説明に従って操作を進めます。

目的...	その場合...
他のスキャンから抑制された検出事項をインポートする	"スキャンを選択して、抑制された検出事項をインポートする" ページ260の手順に従います。
JSONファイルから抑制された検出事項をインポートする	a. 「**ファイルからインポート(Import from File)**」をクリックします。 標準のWindowsファイル選択ダイアログボックスが開きます。 b. インポートするファイルを選択し、「**開く(Open)**」をクリックします。
抑制された検出事項をJSONファイルにエクスポートする	a. 「**ファイルにエクスポート(Export to File)**」をクリックします。 標準のWindowsの「名前を付けて保存」ダイアログボックスが開きます。

目的...	その場合...
	注記: ファイルにエクスポートされた抑制された検出事項のデフォルトディレクトリは、*<directory>*:\ProgramData\HP\HP WebInspect\Settings\SuppressedFindingsです。 b. [**ファイル名(File name)**]ボックスに、抑制された検出事項ファイルの名前を入力します。 c. [**Save**]をクリックします。
抑制された検出事項を脆弱性に戻す	a. アクティブな[**抑制された検出事項(Suppressed Findings)**]リストから項目を選択し、[**脆弱性としてマーク(Mark as Vulnerability)**]をクリックします。 [脆弱性としてマーク(Mark as Vulnerability)]ダイアログボックスが開きます。 b. "脆弱性としてマーク" ページ301の手順に従います。
すべての抑制された検出事項を脆弱性に戻す	a. [**脆弱性のリセット(Reset Vulnerabilities)**]をクリックします。 確認ダイアログボックスが開きます。 b. [**Yes**]をクリックします。 抑制された検出事項が、[検出事項(Findings)]タブに戻されます。
非アクティブな抑制された検出事項リストから項目を削除する	項目を選択し、[**非アクティブから削除(Remove From Inactive)**]をクリックします。
誤検出の説明を編集する	a. 項目を選択し、[**説明の編集(Edit Description)**]をクリックします。 [誤検出の説明を編集する(Edit False Positive Description)]ダイアログボックスが開きます。 b. 説明を編集し、[**OK**]をクリックします。

参照情報

脆弱性を誤検出として指定する方法については、"ナビゲーションペインのショートカットメニュー" ページ70または"[検出事項(Findings)]タブ" ページ104を参照してください。

OpenText DASTウィンドウの詳細については、「"OpenText DASTユーザインタフェース" ページ46」を参照してください。

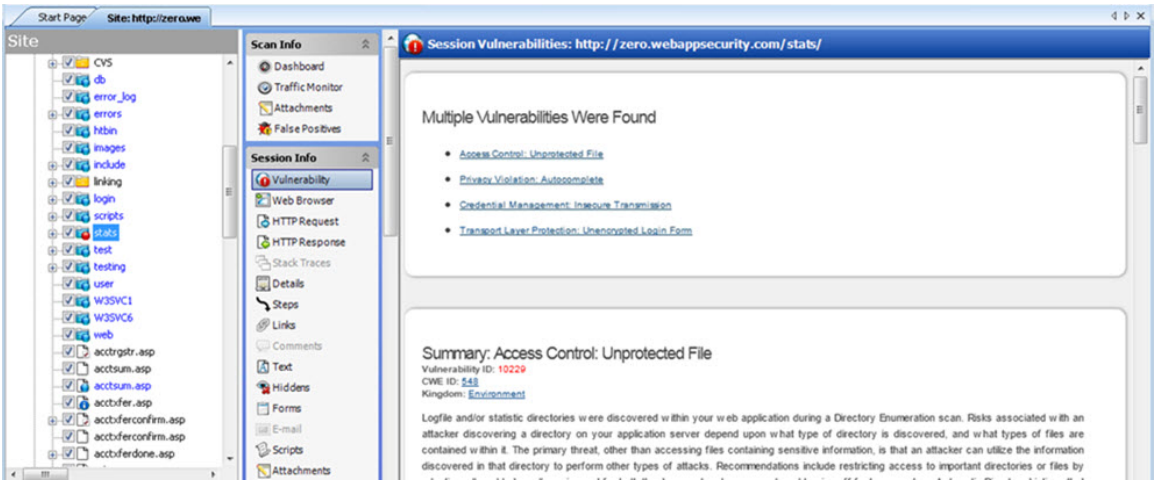
[セッション情報(Session Info)]パネル

OpenText DASTでは、ナビゲーションペインの [サイト(Site)]ビューまたは [シーケンス(Sequence)]ビューを使用して、スキャンで作成された各セッションがリストされます。セッションを選択し、 **[セッション情報(Session Info)]**パネルでオプションを1つクリックして、そのセッションに関する関連情報を表示します。

次のスキャンの例では、OpenText DASTがHTTP要求GET /stats/stats.html HTTP/1.1を送信しています。

脆弱性を表示するには:

1. ナビゲーションペインで [Stats.html]を選択します。
2. [セッション情報(Session Info)]パネルで、 **[脆弱性(Vulnerability)]**をクリックします。



選択可能なオプション

次の表に、 **[セッション情報(Session Info)]**パネルで使用可能なオプションを一覧にします。一部のオプションは、特定のスキャン(基本スキャンまたはWebサービススキャン)でのみ表示されます。また、選択されているセッションに関連するオプションのみが有効になります。たとえば、セッションにフォームが含まれていない場合には **[フォーム(Forms)]**は選択できません。

オプション	説明
脆弱性(Vulnerability)	ナビゲーションペインで選択されているセッションの脆弱性情報を表示します。
Webブラウザ(Web Browser)[1]	ナビゲーションペインで選択されているセッションで、Webブラウザによってレンダリングされたサーバ応答を表示します。
HTTP要求	OpenText DASTから、スキャン対象のサイトをホストするサーバに送信

オプション	説明
(HTTP Request)	された生HTTP要求を表示します。
HTTP応答 (HTTP Response)	OpenText DASTの要求に対するサーバの生HTTP応答を表示します。 応答に1つ以上の攻撃署名(脆弱性が検出されたことを示す)が含まれている場合は、次のいずれかのボタンをクリックして攻撃署名を切り替えることができます。  Flash (.swf)ファイルを選択した場合、OpenText DASTはバイナリデータの代わりにHTMLを表示します。これにより、OpenText DASTは読み取り可能なフォーマットでリンクを表示できます。
スタックトレース (Stack Traces)	この機能は、OpenText DAST Agentがターゲットサーバにインストールされ、実行されているときにこのエージェントをサポートするように設計されています。 特定のチェック(SQLインジェクション、コマンド実行、クロスサイトスクリプティングなど)の場合、OpenText DAST AgentはOpenText DAST HTTP要求を傍受し、ターゲットモジュールでランタイム分析を実行します。この分析によって脆弱性が存在することが確認されると、OpenText DAST AgentはHTTP応答にスタックトレースを追加します。開発者は、このスタックトレースを分析して、改善が必要なエリアを調査できます。
詳細(Details)[1]	要求および応答の詳細(応答のサイズや要求のメソッドなど)を一覧にします。 [応答(Response)]セクションには、コンテンツタイプの2つのエントリ、つまり返されるものと検出されたものが含まれていることに注意してください。 **返されるコンテンツタイプ(Returned Content Type)**]は、HTTP応答のContent-Typeエンティティヘッダフィールドで指定されたメディアタイプを示します。 **検出されたコンテンツタイプ(Detected Content Type)**]は、OpenText DASTによって判別された実際のコンテンツタイプを示します。
ステップ(Steps)[1]	ナビゲーションペインで選択されているセッションまたはサマリペインで選択されているURLに到達するためにOpenText DASTがたどったルートを表示します。親セッション(リストの一番上)から始まり、それ以降にアクセスしたURLが順番に表示され、スキャン方法に関する詳細が提供されます。

オプション	説明
リンク(Links)[1]	このオプションでは、選択したリソースへのリンクを含むターゲットサイトのすべてのリソースが([リンク元(Linked From)]の下に)一覧表示されます。リンクは、HTMLタグ、スクリプト、またはHTMLフォームによってレンダリングできます。また、選択したセッションのHTTP応答内のリンクによって参照されるすべてのリソースも([リンク先(Linked To)]の下に)一覧表示されます。
コメント(Comments)[1]	HTTP応答に埋め込まれているすべてのコメントを(HTML形式で)表示します。
テキスト(Text)[1]	ナビゲーションペインで選択されているセッションのHTTP応答に含まれるすべてのテキストを表示します。
非表示(Hiddens)[1]	コントロールタイプが「hidden」の各入力要素の名前属性を表示します。
フォーム(Forms)[1]	ブラウザがフォームをレンダリングするために解釈するHTMLを表示します。
電子メール(E-mail)[1]	応答に含まれるすべての電子メールアドレスを表示します。
スクリプト(Scripts)[1]	サーバ応答に埋め込まれているクライアントサイドのスクリプトをすべて表示します。
添付ファイル(Attachments)	選択されているオブジェクトに関連付けられているすべてのメモ、フラグ、およびスクリーンショットを表示します。 添付ファイルを作成するには、次のいずれかを実行できます。 • ナビゲーションペインでセッション(基本またはガイド付きスキャン)、操作、または脆弱性(Webサービススキャン)を右クリックし、ショートカットメニューから [**添付ファイル(Attachments)**]を選択します。 • サマリペインの [**検出事項(Findings)**]タブでURLを右クリックし、ショートカットメニューから [**添付ファイル(Attachments)**]を選択します。 • ナビゲーションペインでセッション(基本スキャン)、操作、または脆弱性(Webサービススキャン)を選択し、 [**セッション情報(Session Info)**]パネルから [**添付ファイル(Attachments)**]を選択し、(情報ペインの) [**追加(Add)**]メニューをクリックします。 OpenText Application Lifecycle Management (ALM)に問題を送信するたびに、OpenText DASTによってメモがセッション情報に自動的に追

オプション	説明
	加されます。
攻撃情報(Attack Info)[1]	攻撃シーケンス番号、URL、使用されている監査エンジンの名前、および脆弱性テストの結果が表示されます。攻撃情報は、通常、攻撃が検出されたセッションではなく、攻撃が作成されたセッションに関連付けられます。選択された脆弱なセッションに関する攻撃情報が表示されない場合は、親セッションを選択してから、 **[攻撃情報(Attack Info)]** をクリックします。
XML要求(XML Request)[2]	要求に埋め込まれているSOAPエンベロープが表示されます(Webサービススキャンで操作を選択した場合に使用可能)。
XML応答(XML Response)[2]	応答に埋め込まれているSOAPエンベロープが表示されます(Webサービススキャンで操作を選択した場合に使用可能)。
Webサービス要求(Web Service Request)[2]	要求に埋め込まれているWebサービススキーマと値が表示されます(Webサービススキャンで操作を選択した場合に使用可能)。
Webサービス応答(Web Service Response)[2]	応答に埋め込まれているWebサービススキーマと値が表示されます(Webサービススキャンで操作を選択した場合に使用可能)。

[1]基本スキャンまたはガイド付きスキャンのみ

[2] Webサービススキャンのみ

ほとんどのオプションでは、情報ペイン上部に検索機能が表示され、指定するテキストを検索できます。正規表現を使用して検索を実行するには、 **[正規表現(Regex)]** ボタンを選択してから **[検索(Find)]** をクリックします。

ヒント: 脆弱性情報を表示する際にリンクをたどる場合、ナビゲーションペインで強調表示されたセッションをクリックすると戻ることができます。

参照情報

"OpenText DASTユーザインタフェース" ページ46

" [ホスト情報(Host Info)]パネル" ページ95

"ナビゲーションペイン" ページ61

" [スキャン情報(Scan Info)]パネル" ページ73

"サマリペイン" ページ104

"正規表現" ページ354

脆弱性(Vulnerability)

このオプションを選択すると、ナビゲーションペインで選択したセッション、またはサマリペインで選択した脆弱性の脆弱性情報が表示されます。通常、脆弱性の説明、脆弱性ID、CWE (Common Weakness Enumeration) ID、界、影響(この脆弱性による影響)、および脆弱性の修復方法に関する指示が含まれます。

Webブラウザ(Web Browser)

このオプションを選択すると、ナビゲーションペインで選択したセッションのサーバ応答が、Webブラウザによってレンダリングされる形で表示されます。

HTTP要求(HTTP Request)

このオプションを選択すると、OpenText DASTによってスキャン中のサイトのホストサーバに送信された(ナビゲーションペインで選択したセッションに関する)生のHTTP要求が表示されます。

要求で強調表示されるテキスト

HTTP要求で、OpenText DASTは次のようにテキストを強調表示します。

- 黄色の強調表示は、GET、POST、またはPUTステータス行とクッキーヘッダを示します。
- 赤色の強調表示は、攻撃ペイロードと脆弱性(検出された場合)を示します。

HTTP応答(HTTP Response)

このオプションは、ナビゲーションペインで選択したセッションに関する、OpenText DASTの要求に対するサーバの生のHTTP応答を表示します。

応答に1つ以上の攻撃署名(脆弱性が検出されたことを示す)が含まれている場合は、次のいずれかのボタンをクリックして攻撃署名を切り替えることができます。

Flash (.swf)ファイルを選択した場合、OpenText DASTはバイナリデータの代わりにHTMLを表示します。これにより、OpenText DASTは読み取り可能なフォーマットでリンクを表示できます。

応答で強調表示されるテキスト

HTTP応答で、OpenText DASTは赤色の強調表示を使用して、検出された脆弱性を示します。

スタックトレース(Stack Traces)

この機能は、OpenText DAST Agentがターゲットサーバにインストールされ、実行されているときにこのエージェントをサポートするように設計されています。

特定のチェック(SQLインジェクション、コマンド実行、クロスサイトスクリプティングなど)の場合、OpenText DAST AgentはOpenText DAST HTTP要求を傍受し、ターゲットモジュールでランタイム分析を実行します。この分析によって脆弱性が存在することが確認されると、OpenText DAST AgentはHTTP応答にスタックトレースを追加します。開発者は、このスタックトレースを分析して、改善が必要なエリアを調査できます。

詳細(Details)

このオプションは、ナビゲーションペインで選択したセッションの要求と応答の詳細(応答のサイズや要求メソッドなど)を一覧表示します。

[応答(Response)]セクションには、コンテンツタイプの2つのエントリ、つまり返されるものと検出されたものが含まれていることに注意してください。 **[返されるコンテンツタイプ(Returned Content Type)]**は、HTTP応答のContent-Typeエンティティヘッダフィールドで指定されたメディアタイプを示します。 **[検出されたコンテンツタイプ(Detected Content Type)]**は、OpenText DASTによって判別された実際のコンテンツタイプを示します。

ステップ(Steps)

このオプションを選択すると、ナビゲーションペインで選択したセッションまたはサマリペインで選択したURLに到達するために、OpenText DASTがたどったルートが表示されます。親セッション(リストの一番上)から始まり、それ以降にアクセスしたURLが順番に表示され、スキャン方法に関する詳細が提供されます。

リンク(Links)

このオプションでは、選択したリソースへのリンクを含むターゲットサイトのすべてのリソースが([リンク元(Linked From)]の下に)一覧表示されます。リンクは、HTMLタグ、スクリプト、またはHTMLフォームによってレンダリングできます。

また、選択したセッションのHTTP応答内のリンクによって参照されるすべてのリソースも([リンク先(Linked To)]の下に)一覧表示されます。

表示されているリンクをダブルクリックすると、ナビゲーションペインのフォーカスが、参照されているセッションに移動します。または、Webブラウザでセッションを表示することにより、リンクされたリソースを参照することもできます([**Webブラウザ(Web Browser)**]をクリック)。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。

コメント - セッション情報

このオプションは、ナビゲーションペインで選択されたセッションのHTTP応答に埋め込まれたすべてのコメントを表示します。

開発者が、サイトのセキュリティを侵害するために使用可能な重要な情報をコメントに残す場合があります。たとえば、テーブル内のフィールドの必須の順序についてのコメント、といった一見無害な情報が、サイトのセキュリティを侵害するのに必要となる重大な情報を攻撃者に与えてしまうことがあります。

情報ペインの最上部にある [**検索(Search)**] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [**正規表現(Regex)**] ボタンを選択してから [**検索(Find)**] をクリックします。

コメントをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [**コピー(Copy)**] を選択します。

Text

このオプションは、ナビゲーションペインで選択されているセッションのHTTP応答に含まれるすべてのテキストを表示します。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。

非表示(Hiddens): セッション情報(Session Info)

OpenText DASTは、すべてのフォームを分析し、「非表示」タイプのすべてのコントロール(レンダリングされていないが、フォームで送信される値を持つコントロール)を一覧表示します。しばしば開発者は非表示のコントロールにパラメータを含めますが、攻撃者がこれを編集して再送信する可能性があります。

情報ペインの最上部にある [**検索(Search)**] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [**正規表現(Regex)**] ボタンを選択してから [**検索(Find)**] をクリックします。

HTMLテキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [**コピー(Copy)**] を選択します。

フォーム(Forms): セッション情報(Session Info)

OpenText DASTは、ナビゲーションペインで選択されたセッションに対して検出されたすべてのHTMLフォームを一覧表示します。

情報ペインの最上部にある [**検索(Search)**] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [**正規表現(Regex)**] ボタンを選択してから [**検索(Find)**] をクリックします。

フォームをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [**コピー(Copy)**] を選択します。

OpenText DASTウィンドウの詳細については、「"OpenText DASTユーザインタフェース" ページ46」を参照してください。

電子メール(E-mail)

OpenText DASTは、ナビゲーションペインから選択されたセッションに含まれるすべての電子メールアドレスを一覧表示します。

情報ペインの最上部にある [**検索(Search)**] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [**正規表現(Regex)**] ボタンを選択してから [**検索(Find)**] をクリックします。

電子メールアドレスをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [**コピー(Copy)**] を選択します。

スクリプト(Scripts) -セッション情報(Session Info)

OpenText DASTは、セッションで検出されたスクリプトをすべて一覧表示します。

情報ペインの最上部にある [**検索(Search)**] 機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [**正規表現(Regex)**] ボタンを選択してから [**検索(Find)**] をクリックします。詳細については、「"正規表現" ページ354」を参照してください。

スクリプトをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [**コピー(Copy)**] を選択します。

OpenText DASTウィンドウの詳細については、「"OpenText DASTユーザインタフェース" ページ46」を参照してください。

添付ファイル(Attachments) -セッション情報(Session Info)

次の添付ファイルをセッションに関連付けることができます。

- セッションのメモ
- フォローアップ用フラグセッション
- 脆弱性のメモ
- 脆弱性のスクリーンショット

注記: メモをスキャンに関連付け、 [**スキャン情報(Scan Info)**] パネルで [**添付ファイル(Attachments)**] を選択して、そのスキャンに追加されたすべての添付ファイルを表示することもできます。

[**添付ファイル(Attachments)**] を選択すると、選択したセッションに関連付けられているすべてのメモ、フラグ、およびスクリーンショットの一覧が表示されます。

添付ファイルの表示

添付ファイルを表示するには:

- 添付ファイルを選択して [**表示(View)**] をクリックします(または単に添付ファイルをダブルクリックします)。

セッションの添付ファイルの追加

セッションの添付ファイルを追加するには:

1. 次のいずれかを実行してセッションを選択します。
   - サマリペインの [**検出事項(Findings)**] タブで、脆弱なURLを右クリックします。詳細については、「" 検出事項(Findings)]タブ" ページ104」を参照してください。

- ナビゲーションペインで、セッションまたはURLを右クリックします。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。

2. ショートカットメニューで [**添付ファイル(Attachments)**] をクリックし、添付ファイルの種類を選択します。

   注記: 別の方法として、ナビゲーションペインでセッションを選択し、 [**セッション情報(Session Info)**] パネルで [**添付ファイル(Attachments)**] をクリックし、(情報表示エリア内の) [**追加(Add)**] メニューからコマンドを選択します。詳細については、「"情報ペイン" ページ72」を参照してください。

3. 選択した添付ファイルの種類に関連するコメントを入力します。
4. 1つ以上の脆弱性の横にあるチェックボックスをオンにします。
5. [**脆弱性スクリーンショット(Vulnerability Screenshot)**] を選択した場合:
   a. [**名前(Name)**] ボックスにスクリーンショットの名前を入力します。最大長は、40文字です。
   b. [参照(Browse)] ボタン … をクリックしてグラフィックファイルを見つけるか、イメージをメモリにキャプチャした場合は、 [**クリップボードからコピー(Copy from Clipboard)**] をクリックします。
6. [**OK**] をクリックします。

添付ファイルの編集

添付ファイルを編集するには:

1. 次のいずれかを実行します。
   - スキャンに追加された添付ファイルをすべて表示するには、 [**スキャン情報(Scan Info)**] パネルで [**添付ファイル(Attachments)**] をクリックします。
   - 特定のセッションに追加された添付ファイルのみを表示するには、 [**セッション情報(Session Info)**] パネルで [**添付ファイル(Attachments)**] をクリックし、ナビゲーションペインでセッションをクリックします。サマリペインでURLを選択することもできます。
2. 添付ファイルを選択し、 [**編集(Edit)**] をクリックします。
3. 必要に応じてコメントを変更します。

   注記: スクリーンショットの添付ファイルは編集できません。

4. [**OK**] をクリックします。

ヒント: 追加、編集、表示、および削除機能は、情報表示エリア内の添付ファイルを右クリックし、ショートカットメニューからオプションを選択して使用することもできます。

攻撃情報(Attack Info)

このオプションを使用すると、ナビゲーションペインで選択されたセッションに関して、攻撃シーケンス番号、URL、使用されている監査エンジンの名前、および脆弱性テストの結果が表示されます。

攻撃情報は、通常、攻撃が検出されたセッションではなく、攻撃が作成されたセッションに関連付けられます。選択された脆弱なセッションに関する攻撃情報が表示されない場合は、親セッションを選択してから、 **[攻撃情報(Attack Info)]**をクリックします。

Webサービス要求(Web Service Request)

このオプションを選択すると、要求に埋め込まれているWebサービススキーマと値が表示されます(Webサービススキャンで操作を選択した場合に使用可能)。Webサービススキャン中にのみ使用できます。

Webサービス応答(Web Service Response)

このオプションを選択すると、応答に埋め込まれているWebサービススキーマと値が表示されます(Webサービススキャンで操作を選択した場合に使用可能)。Webサービススキャン中にのみ使用できます。

XML要求

このオプションを選択すると、選択した要求に埋め込まれている関連XMLスキーマが表示されます(WebサービススキャンでWSDLオブジェクトを選択した場合に使用可能)。

XML応答

このオプションを選択すると、ナビゲーションペインで選択したセッションの応答に埋め込まれている関連XMLスキーマが表示されます(WebサービススキャンでWSDLオブジェクトを選択した場合に使用可能)。

[ホスト情報(Host Info)]パネル

この折りたたみ可能なパネルに一覧表示されている項目をクリックすると、サイト(またはホスト)のWeb探索または監査中に検出されたその項目タイプのすべてのインスタンスがOpenText DASTに表示されます。

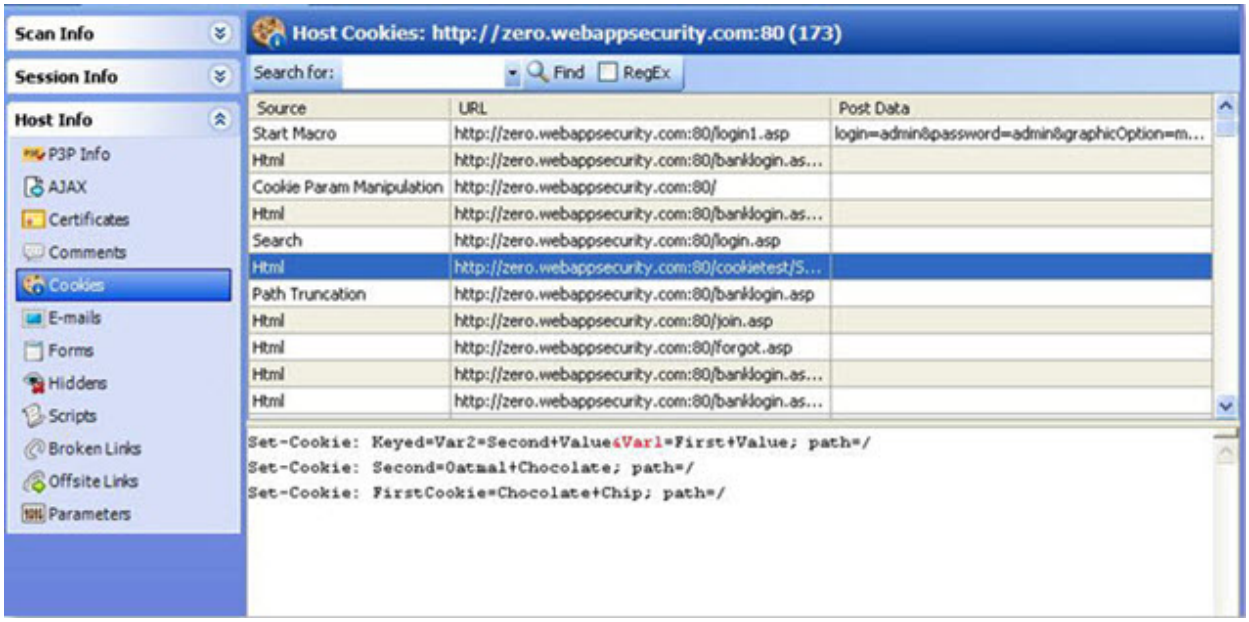
項目をダブルクリックすると、OpenText DASTによって、その項目を含むセッションがナビゲーションペインで強調表示されます。項目(電子メールアドレスなど)をクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから **[コピー(Copy)]**を選択します。

ほとんどの場合、情報ペインの最上部にある **[検索(Search)]**機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 **[正規表現(Regex)]**ボタンを選択してから **[検索(Find)]**をクリックします。

注記: Webサービススキャンを実行している場合、 [ホスト情報(Host Info)]パネルは表示されません。

次の図で、 **[クッキー(Cookies)]**を選択すると、クッキーが検出されたすべてのセッションのリストが表示されます。リストから項目を選択すると、選択したセッションに関連付けられたクッキーがOpenText DASTに表示されます。

[ホスト情報(Host Info)]パネルのイメージ



選択可能なオプション

[ホスト情報(Host Info)]オプションについて、次の表で説明します。

オプション	説明
P3P情報(P3P Info)	P3P (Platform for Privacy Preferences Project)情報を表示します。詳細については、「"P3P情報(P3P info)" 次のページ」を参照してください。
AJAX	AJAXエンジンとAJAX要求を含むすべてのページのリストを表示します。詳細については、「"AJAX" ページ98」を参照してください。
証明書(Certificates)	サイトに関連付けられているすべての証明書のリストを表示します。詳細については、「"証明書(Certificates)" ページ99」を参照してください。
Comments	コメントを含むすべてのURLのリストを表示します。詳細については、「"コメント - ホスト情報" ページ99」を参照してください。
クッキー(Cookies)	クッキーを含むすべてのURLのリストを表示します。詳細については、「"クッキー(Cookies)" ページ100」を参照してください。
電子メール(E-Mails)	応答に電子メールアドレスを含むすべてのURLのリストを表示します。詳細については、「"電子メール(E-mails) -ホスト情報(Host Info)" ページ100」を参照してください。
フォーム(Forms)	フォームを含むすべてのURLのリストを表示します。詳細については、「"フォーム(Forms) -ホスト情報(Host Info)" ページ101」を参照してくださ

オプション	説明
	い。
非表示(Hiddens)	コントロールタイプが「hidden」の入力要素を含むすべてのURLのリストを表示します。詳細については、「"非表示(Hiddens) -ホスト情報(Host Info)" ページ101」を参照してください。
スクリプト	サーバの応答に埋め込まれるクライアントサイドスクリプトを含むすべてのURLのリストを表示します。詳細については、「"スクリプト(Scripts) -ホスト情報(Host Info)" ページ102」を参照してください。
壊れたリンク(Broken Links)	存在しないターゲットへのハイパーリンクを含むすべてのURLのリストを表示します。詳細については、「"壊れたリンク(Broken Links)" ページ102」を参照してください。
サイト外リンク(Offsite Links)	他のサイトへのハイパーリンクが含まれたすべてのURLのリストを表示します。詳細については、「"サイト外リンク(Offsite Links)" ページ103」を参照してください。
パラメータ(Parameters)	埋め込みパラメータを含むすべてのURLのリストを表示します。詳細については、「"パラメータ(Parameters)" ページ103」を参照してください。

P3P情報(P3P info)

このオプションには、P3P (Platform for Privacy Preferences Project)情報が表示されます。

注記: World Wide Web Consortiumによると、P3Pに関する作業は中止されました。

World Wide Web ConsortiumのP3Pにより、Webサイトで、ユーザエージェントが自動的に取得して簡単に解釈可能な標準形式でプライバシープラクティスを表現できます。P3Pユーザエージェントを使用すると、ユーザはサイトプラクティスを(マシンと人の両方が読み取り可能な形式で)受信したり、必要に応じてこれらのプラクティスに基づいて意思決定を自動化したりすることができます。そのため、ユーザは、アクセスする各サイトでプライバシーポリシーを読む必要がありません。

P3P準拠のWebサイトでは、収集する情報の種類とその情報の使用方法がポリシーで宣言されます。P3P対応のWebブラウザでは、このポリシーをユーザの保存された環境設定と比較することで、実行する操作を決定できます。たとえば、ユーザは自身の閲覧習慣に関する情報が収集されないようにブラウザの環境設定を行うことができます。この目的でクッキーを使用することがポリシーに記載されているWebサイトにユーザがアクセスすると、ブラウザによってクッキーが自動的に拒否されます。

P3Pユーザエージェント

Microsoft Internet Explorer 6では、P3Pプライバシーポリシーを表示し、P3Pポリシーを独自の設定と比較して、特定のサイトからのクッキーを許可するかどうかを決定できます。

http://www.privacybird.com/で入手できるPrivacy Bird (元はAT&Tが開発)は、完全な機能を備えたP3Pユーザエージェントであり、ユーザがアクセスする各Webサイトで自動的にプライバシーポリシーの検索を行います。次いで、ポリシーと、保存されているユーザのプライバシー環境設定とを比較し、矛盾が発生した場合はユーザに通知します。

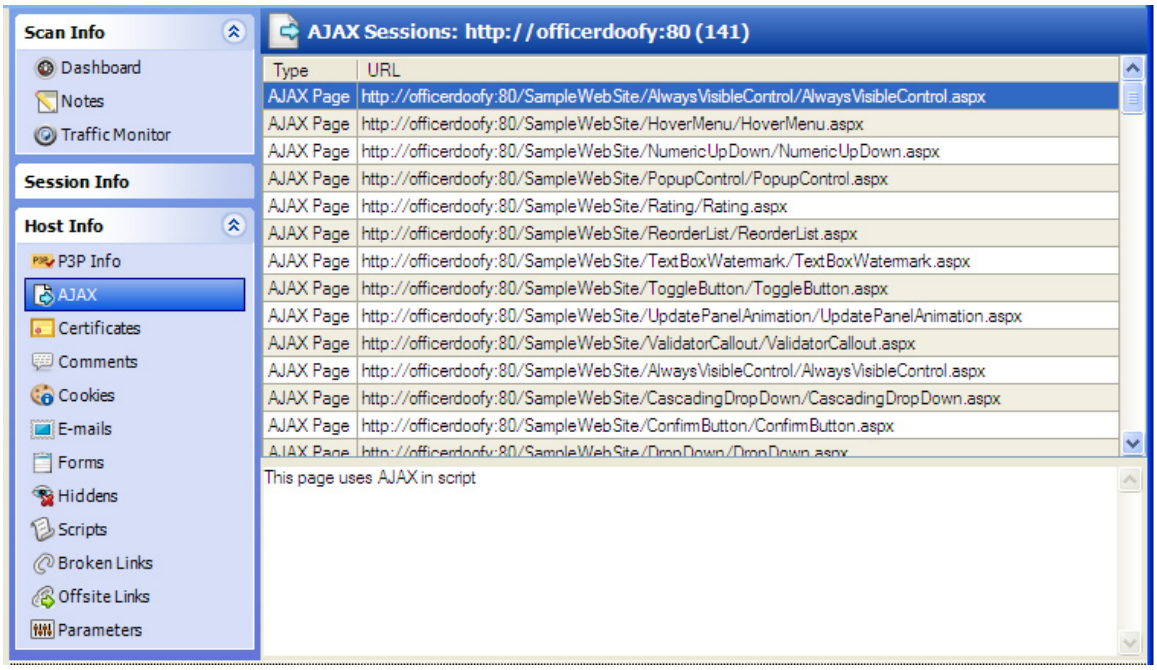
参照情報

" [ホスト情報(Host Info)]パネル" ページ95

AJAX

AJAXは、Asynchronous JavaScript and XMLHttpRequestの頭字語です。

このオプションを選択すると、OpenText DASTには、AJAXエンジンとAJAX要求を含むすべてのページが表示されます。



このビューには、2種類のAJAX行項目があります。

- AJAXページ(上の図を参照)
- 要求

リスト内の項目をクリックすると、OpenText DASTに、「This page uses AJAX in script」と表示される(ページタイプの場合)か、クエリおよび/またはPOSTデータパラメータが一覧表示されます(要求タイプの場合)。

AJAXの動作

AJAXは、それ単体の技術ではなく、HTMLまたはXHTML、カスケーディングスタイルシート、JavaScript、ドキュメントオブジェクトモデル、XML、XSLT、XMLHttpRequestオブジェクトなどの既存の技術の組み合わせです。これらの技術をAJAXモデルで組み合わせると、Webアプリ

ケーションはブラウザページ全体を再ロードせずに、ユーザインタフェースを迅速かつインクリメンタルに更新できます。

ブラウザは、セッションの最初にWebページをロードする代わりに、AJAXエンジンをロードします。これはユーザインタフェースのレンダリングとサーバとの通信の両方を担当します。通常ならHTTP要求が生成されるはずの各ユーザアクションは、代わりにAJAXエンジンに対するJavaScript呼び出しの形を取ります。サーバとの通信を必要としないユーザアクション(たとえば、単純なデータ検証、メモリ内のデータの編集、および一部のナビゲーションさえ)への応答は、エンジンによって処理されます。エンジンがサーバと通信する必要がある場合(処理用のデータの送信、追加のインタフェースコードのロード、または新しいデータの取得)、エンジンによってこれらの要求が非同期に、通常はXMLを使用して発行されます。ユーザとアプリケーションのやり取りが停止することはありません。

証明書(Certificates)

証明書は、特定のWebサイトが安全で本物であることを示すものです。これにより、他のWebサイトが元の安全なサイトの識別情報を推測できなくなります。セキュリティ証明書によって識別情報が公開鍵に関連付けられます。証明書の所有者だけが、対応する秘密鍵を知っています。これにより、所有者は「デジタル署名」を作成したり、対応する公開鍵で暗号化された情報を復号化したりすることができます。

コメント - ホスト情報

開発者が、サイトのセキュリティを侵害するために使用可能な重要な情報をコメントに残す場合があります。たとえば、テーブル内のフィールドの必須の順序についてのコメント、といった一見無害な情報が、サイトのセキュリティを侵害するのに必要となる重大な情報を攻撃者に与えてしまうことがあります。

検出されたコメントを表示するには:

1. [**ホスト情報(Host Info)**]パネルから [**コメント(Comments)**]を選択し、コメントが含まれているすべてのURLを一覧にします。
2. [**URL**]をクリックして、そのURLに含まれるコメントを表示します。
3. エントリをダブルクリックして、コメントを含むセッションをナビゲーションペインで探します。フォーカスが、 [**セッション情報(Session Info)**]パネルの [**コメント(Comments)**]選択肢に切り替わります。

情報ペインの最上部にある [**検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [**正規表現(Regex)**]ボタンを選択してから [**検索(Find)**]をクリックします。

コメントをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [**コピー(Copy)**]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

クッキー(Cookies)

クッキーには、後で使用するためにサーバによってクライアント上に保存された情報(ユーザの優先設定や設定情報など)が含まれています。クッキーには基本形式が2種類あります。個別のファイルと、1つの連続ファイル内のレコードです。たいてい複数のセットが存在します。これは、異なる場所に複数のブラウザがインストールされていることの結果です。多くの場合、「忘れられた」クッキーには、他人に見られたくない暴露情報が含まれています。

検出されたクッキーを表示するには:

1. [**ホスト情報(Host Info)**]パネルから [**クッキー(Cookies)**]を選択し、Web探索または監査中にクッキーが検出されたすべてのURLを一覧表示します。
2. URLをクリックして、そのURLに含まれるクッキーを表示します。
3. エントリをダブルクリックして、クッキーを含むセッションをナビゲーションペインで探します。フォーカスが、 [**セッション情報(Session Info)**]パネルの [**HTTP応答(HTTP Response)**]選択肢に切り替わります。

情報ペインの最上部にある [**検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [**正規表現(Regex)**]ボタンを選択してから [**検索(Find)**]をクリックします。

クッキーコードをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [**コピー(Copy)**]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

電子メール(E-mails) -ホスト情報(Host Info)

OpenText DASTは、スキャン中に検出された電子メールアドレスをすべて一覧表示します。電子メールアドレスを表示するには:

1. [**ホスト情報(Host Info)**]パネルから [**電子メール(E-mail)**]を選択し、電子メールアドレスを含むすべてのURLを一覧表示します。
2. URLをクリックすると、そのURLに含まれる電子メールアドレスが表示されます。
3. エントリをダブルクリックして、電子メールアドレスを含むセッションをナビゲーションペインで探します。 [**セッション情報(Session Info)**]パネルの [**電子メール(E-mail)**]選択項目にフォーカスが切り替わります。

情報ペインの最上部にある [**検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [**正規表現(Regex)**]ボタンを選択してから [**検索(Find)**]をクリックします。

電子メールアドレスをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [**コピー(Copy)**]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

フォーム(Forms) -ホスト情報(Host Info)

OpenText DASTは、スキャン中に検出されたHTMLフォームをすべて一覧表示します。

1. [ホスト情報(Host Info)]パネルから [フォーム(Forms)]を選択し、フォームが含まれているすべてのURLを一覧表示します。
2. URLをクリックすると、そのURLに含まれるフォームのソースHTMLが表示されます。
3. エントリをダブルクリックして、フォームを含むセッションをナビゲーションペインで探します。 [セッション情報(Session Info)]パネルの [フォーム(Forms)]選択項目にフォーカスが切り替わります。

情報ペインの最上部にある [検索(Search)]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [正規表現(Regex)]ボタンを選択してから [検索(Find)]をクリックします。

フォームをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [コピー(Copy)]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

非表示(Hiddens) -ホスト情報(Host Info)

OpenText DASTは、すべてのフォームを分析し、「非表示」タイプのすべてのコントロール(レンダリングされていないが、フォームで送信される値を持つコントロール)を一覧表示します。しばしば開発者は非表示のコントロールにパラメータを含めますが、攻撃者がこれを編集して再送信する可能性があります。

1. [ホスト情報(Host Info)]パネルから [非表示(Hiddens)]を選択し、非表示のコントロールを含むすべてのURLを一覧表示します。
2. URLをクリックすると、そのURLに含まれる「非表示」のコントロールの名前と値の属性が表示されます。
3. エントリをダブルクリックして、非表示のコントロールを含むセッションをナビゲーションペインで探します。 [セッション情報(Session Info)]パネルの [非表示(Hiddens)]選択項目にフォーカスが切り替わります。

情報ペインの最上部にある [検索(Search)]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、 [正規表現(Regex)]ボタンを選択してから [検索(Find)]をクリックします。

HTMLテキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから [コピー(Copy)]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

スクリプト(Scripts) -ホスト情報(Host Info)

OpenText DASTは、スキャン中に検出されたスクリプトをすべて一覧表示します。検出されたスクリプトを表示するには:

1. [**ホスト情報(Host Info)**]パネルから[**スクリプト(Scripts)**]を選択し、スクリプトが含まれているすべてのURLを一覧表示します。
2. URLをクリックして、そのURLに含まれるスクリプトを表示します。
3. エントリをダブルクリックして、スクリプトを含むセッションをナビゲーションペインで探します。

情報ペインの最上部にある[**検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[**正規表現(Regex)**]ボタンを選択してから[**検索(Find)**]をクリックします。

スクリプトをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから[**コピー(Copy)**]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

OpenText DASTウィンドウの詳細については、「"OpenText DASTユーザインタフェース" ページ46」を参照してください。

参照情報

" [ホスト情報(Host Info)]パネル" ページ95

"ナビゲーションペイン" ページ61

"正規表現" ページ354

壊れたリンク(Broken Links)

OpenText DASTは、サイト上の正常に機能しないハイパーリンクのすべてを検索して文書化します。壊れたリンクを探すには:

1. [**ホスト情報(Host Info)**]パネルから[**壊れたリンク(Broken Links)**]を選択し、正常に機能しないハイパーリンクを含むすべてのURLを一覧にします。
2. エントリをダブルクリックして、壊れたリンクを含むセッションをナビゲーションペインで探します。フォーカスが、[**セッション情報(Session Info)**]パネルの[**HTTP応答(HTTP Response)**]選択肢に切り替わります。

情報ペインの最上部にある[**検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[**正規表現(Regex)**]ボタンを選択してから[**検索(Find)**]をクリックします。

HTMLテキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから[**コピー(Copy)**]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

サイト外リンク(Offsite Links)

OpenText DASTは、他のサイトへのハイパーリンクをすべて検索して文書化します。

他のサイトへのハイパーリンクを調べるには:

1. [**ホスト情報(Host Info)**]パネルから[**サイト外リンク(Offsite Links)**]を選択し、他のサイトへのハイパーリンクが含まれているすべてのURLを一覧表示します。
2. エントリをダブルクリックして、サイト外リンクを含むセッションをナビゲーションペインで探します。フォーカスが、[**セッション情報(Session Info)**]パネルの[**HTTP応答(HTTP Response)**]選択肢に切り替わります。

情報ペインの最上部にある[**検索(Search)**]機能を使用して、指定したテキストを探します。正規表現を使用して検索を実行するには、[**正規表現(Regex)**]ボタンを選択してから[**検索(Find)**]をクリックします。

HTMLテキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから[**コピー(Copy)**]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

OpenText DASTウィンドウの詳細については、「"OpenText DASTユーザインタフェース" ページ46」を参照してください。

パラメータ(Parameters)

パラメータには、次のいずれかを指定できます。

- HTTP要求のURLの一部として送信される(または別のヘッダに含まれる)クエリ文字列。
- Postメソッドを使用して送信されるデータ。

パラメータを含むすべてのURLを一覧表示するには:

1. [**ホスト情報(Host Info)**]パネルから[**パラメータ(Parameters)**]を選択します。
2. URLをクリックして、そのURLに含まれるパラメータを表示します。
3. エントリをダブルクリックして、パラメータを含むセッションをナビゲーションペインで探します。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。

情報ペインの最上部にある[**検索(Search)**]機能を使用して、選択したURLから、指定したテキストを検索します。正規表現を使用して検索を実行するには、[**正規表現(Regex)**]ボタンを選択してから[**検索(Find)**]をクリックします。詳細については、「"正規表現" ページ354」を参照してください。

テキストをクリップボードにコピーするには、テキストを強調表示して、ショートカットメニューから[**コピー(Copy)**]を選択します。

URLをダブルクリックすると、OpenText DASTのナビゲーションペインで、そのURLを含むセッションが強調表示されます。

詳細については、「"OpenText DASTユーザインタフェース" ページ46」を参照してください。

参照情報

" [ホスト情報(Host Info)]パネル" ページ95

サマリペイン

スキャンを実行または表示するときには、ウィンドウの下部にある横長のサマリペインを使用して、まとめて表示される脆弱性リソースを確認し、脆弱性情報に素早くアクセスし、OpenText DASTログ記録情報を確認します。

このペインには以下のタブがあります。

- 検出事項(Findings) (" [検出事項(Findings)]タブ" 下を参照)
- 未検出(Not Found) (" [未検出(Not Found)]タブ" ページ108を参照)
- スキャンログ(Scan Log) (" [スキャンログ(Scan Log)]タブ" ページ108を参照)
- サーバ情報(Server Information) (" [サーバ情報(Server Information)]タブ" ページ109を参照)

参照情報

"OpenText DASTユーザインタフェース" ページ46

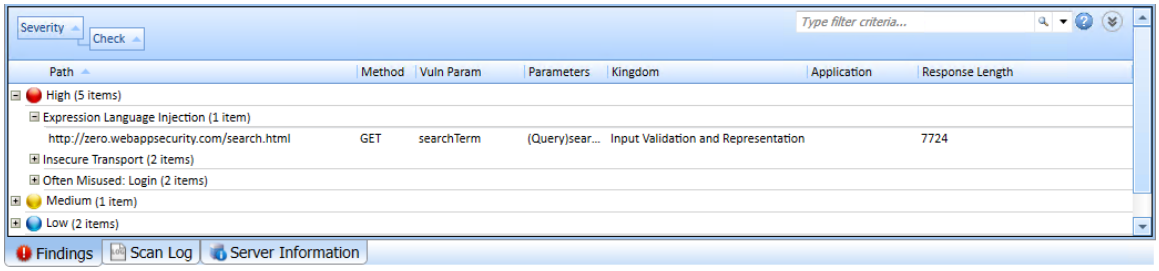
"サマリペインのフィルタとグループの使用" ページ290

"脆弱性の再テスト" ページ271

"脆弱性のロールアップ" ページ299

[検出事項(Findings)]タブ

[検出事項(Findings)]タブには、Webアプリケーションの監査中に検出された各脆弱性に関する情報が一覧表示されます。



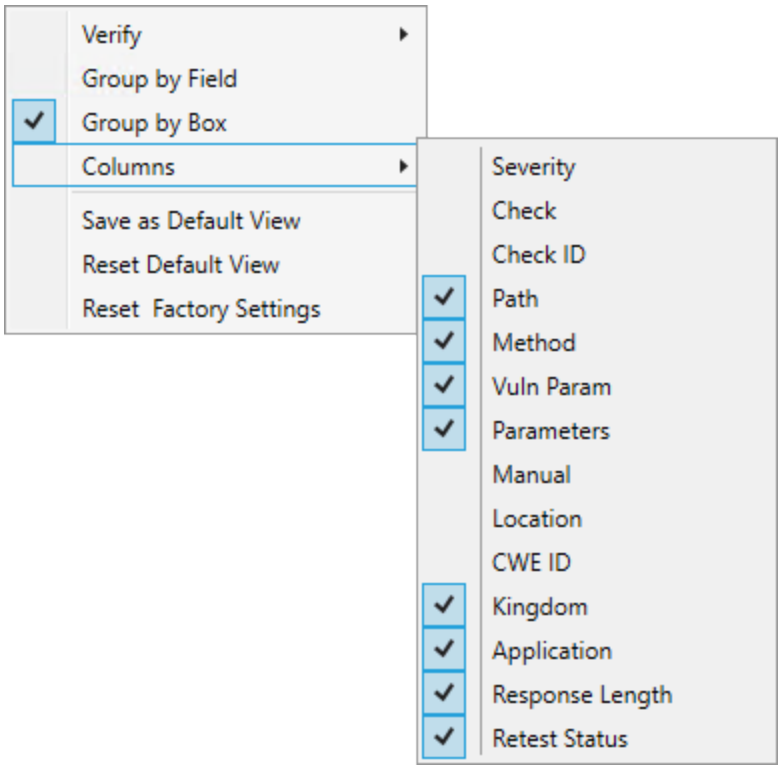
このタブには、スキャン中に検出された懸案事項の情報も表示されます。これらは脆弱性とは見なされませんが、サイトまたは特定のアプリケーションやWebサーバにおける興味深い事項を示します。

さらに、このタブには、スキャン中に検出されたベストプラクティスの問題も含まれています。同様に、これらは脆弱性とは見なされませんが、Web開発で一般的に認められるベストプラクティスに関連し、サイト品質とサイト開発のセキュリティに関する全体的なプラクティス(またはその欠如)の指標となります。

注記: **検出事項(Findings)**]タブで結果をグループ化し、フィルタ処理することもできます。詳細については、「"サマリペインのフィルタとグループの使用" ページ290」を参照してください。

使用可能な列

データの複数の列を表示できます。表示する情報を選択するには、列ヘッダバーを右クリックし、ショートカットメニューから **列(Columns)**]を選択します。



使用可能な列は次のとおりです。

- **重大度(Severity):** 脆弱性の相対的な評価(低(low)から重大(critical)まで)。関連するアイコンについては、以下を参照してください。
- **チェック(Check)**: 特定の脆弱性に対するOpenText DASTプローブ。たとえば、クロスサイトスクリプティング、暗号化されていないログインフォームなどです。
- **チェックID (Check ID)**: 特定の脆弱性の有無をチェックする、OpenText DASTプローブの識別番号。たとえば、チェックID 742は、データベースサーバのエラーメッセージについてテストします。
- **パス(Path)**: リソースへの階層パス。
- **メソッド(Method)**: 攻撃に使用されるHTTPメソッド。
- **スタック(Stack)**: OpenText DAST Agentから取得したスタックトレース情報。列は、スキャン中にOpenText DAST Agentが有効になっている場合にのみ使用できます。
- **脆弱なパラメータ(Vuln Param)**: 脆弱なパラメータの名前。
- **パラメータ(Parameters)**: パラメータの名前、およびそれらに割り当てられた値。

- **手動(Manual)**: 脆弱性が手動で作成された場合は、チェックマークが表示されます。
- **重複(Duplicates):** 同じソースに対して追跡可能な、OpenText DAST Agentによって検出された脆弱性。列は、スキャン中にOpenText DAST Agentが有効になっている場合にのみ使用できます。
- **場所(Location)**: パスとパラメータ。
- **CWE ID**: 脆弱性に関連付けられたCommon Weakness Enumeration識別子。
- **界(Kingdom)**: OpenText Software Security Research Groupが開発したソフトウェアセキュリティエラーの分類を使用して、この脆弱性が分類されるカテゴリ。
- **アプリケーション(Application)**: 脆弱性が見つかったアプリケーションまたはフレームワーク(ASP.NETやMicrosoft IISサーバなど)。
- **保留中ステータス(Pending Status)**: このスキャンが発行されると仮定した場合のステータス(自動的にOpenText DASTによって、または手動で割り当てられる)。
- **発行済みステータス(Published Status)**: 以前に発行されている場合の、Fortify Software Security Centerに存在するステータス。
- **再現性(Reproducible)**: 取り得る値は、「再現済み(Reproduced)」、「未検出/修復済み(Not Found/Fixed)」、または「新規(New)」です。列は、サイト再テスト(脆弱性の再テスト)でのみ使用できます。
- **応答長(Response Length)**: 脆弱なセッションの応答サイズ(バイト単位)。
- **再テストのステータス(Retest Status)**: 1つ以上の問題で実行された検証スキャンのステータス。この列は、再テストスキャンでのみ使用できます。詳細については、「"脆弱性の再テスト" ページ271」を参照してください。

脆弱性の重大度

「**検出事項(Findings)**」タブの脆弱性の重大度は、次のアイコンで示されます。

重大	High	中間	Low
			

検出事項の操作

リスト内の項目をクリックすると、関連するセッションがナビゲーションペインで強調表示され、関連する情報が情報ペインに表示されます。詳細については、「"ナビゲーションペイン" ページ61」および「"情報ペイン" ページ72」を参照してください。

セッションを選択し、「**セッション情報(Session Info)**」パネルからオプションを選択して、関連する情報を表示することもできます。

PostパラメータおよびQueryパラメータの場合は、「**パラメータ(Parameters)**」列のエントリをクリックすると、パラメータのより分かりやすい概要が表示されます。

リスト内の項目を右クリックすると、ショートカットメニューを使用して次の操作を実行できます。

- **URLのコピー(Copy URL)** - URLをWindowsのクリップボードにコピーします。
- **選択した項目のコピー(Copy Selected Item(s))** -選択した項目のテキストをWindowsクリップボードにコピーします。
- **すべての項目のコピー(Copy All Items)** -すべての項目のテキストをWindowsクリップボードにコピーします。
- **エクスポート(Export)** -すべての項目または選択した項目を含むカンマ区切り値(csv)ファイルを作成し、Microsoft Excelで表示します。
- **ブラウザで表示(View in Browser)** - HTTP応答をブラウザで表示します。
- **現在の値によるフィルタ(Filter by Current Value)** -選択した基準を満たす脆弱性だけを表示するよう制限します。たとえば、 [メソッド(Method)]列で「Post」を右クリックして、 **[現在の値によるフィルタ(Filter by Current Value)]**を選択すると、Postメソッドを使用したHTTP要求を送信して検出された脆弱性だけがリストに表示されます。

  注記: フィルタ基準は、サマリペインの右上隅のコンボボックスに表示されます。または、このコンボボックスを使用してフィルタ基準を手動で入力または選択することもできます。追加の詳細および構文ルールについては、"サマリペインのフィルタとグループの使用" ページ290を参照してください。

- **SSCステータスの変更(Change SSC Status)** - Fortify Software Security Centerに発行する前に脆弱性/問題のステータスを変更します。

  注記: このオプションは、Fortify Software Security Centerと統合されたFortify WebInspect Enterpriseに接続されている場合にのみ使用できます。

- **重大度の変更(Change Severity)** -重大度レベルを変更できます。
- **脆弱性の編集(Edit Vulnerability)** - [脆弱性の編集(Edit Vulnerabilities)]ダイアログボックスが表示され、脆弱性のさまざまな特性を変更できます。詳細については、「"脆弱性の編集" ページ296」を参照してください。
- **脆弱性のロールアップ(Rollup Vulnerabilities)** -複数の脆弱性が選択されている場合に使用できます。選択した脆弱性を、OpenText DAST、Fortify WebInspect Enterprise、およびレポート内で「[Rollup]」というタグの接頭部を持つ単一インスタンスにロールアップできます。詳細については、「"脆弱性のロールアップ" ページ299」を参照してください。

  注記: ロールアップされた脆弱性を選択した場合、このメニューオプションは **[脆弱性のロールアップを元に戻す(Undo Rollup Vulnerabilities)]**になります。

- **再テスト(Retest)** -選択した1つ以上の脆弱性、すべての脆弱性、または特定の重大度の脆弱性の再テストを実行します。詳細については、「"脆弱性の再テスト" ページ271」を参照してください。
- **マーク付けする(Mark as)** -脆弱性に誤検出(説明を追加可能)または無視のフラグを設定します。どちらの場合も、その脆弱性はリストから削除されます。 [スキャン情報(Scan Info)]パネルで **[抑制された検出事項(Suppressed Findings)]**を選択すると、すべての誤検出および無視された脆弱性のリストを表示できます。

注記: 抑制された検出事項を脆弱性に戻すことができます。詳細については、「"抑制された検出事項" ページ83」を参照してください。

- **送信(Send to)** -脆弱性を欠陥に変換し、OpenText Application Lifecycle Management (ALM)データベースに追加します。
- **場所の削除(Remove Location)** -選択したセッションをナビゲーションペイン([サイト(Site)]ビューと [シーケンス(Sequence)]ビューの両方)から削除し、関連する脆弱性もすべて削除します。

注記: 削除された場所(セッション)およびそれに関連する脆弱性を回復できます。詳細については、「"削除されたセッションの回復" ページ304」を参照してください。

- **Web探索(Crawl)** -選択したURLのWeb探索を再実行します。
- **ツール(Tools)** -使用可能なツールのサブメニューを表示します。
- **添付ファイル(Attachments)** -選択したセッションに関連するメモの作成、フォローアップのためのセッションへのフラグ付け、脆弱性のメモの追加、または脆弱性スクリーンショットの追加を行うことができます。

グループ見出しを右クリックすると、ショートカットメニューで次の操作を実行できます。

- **すべてのグループの縮小/展開(Collapse/Expand All Groups)**
- **グループの縮小/展開(Collapse/Expand Group)**
- **選択した項目のコピー(Copy Selected Item(s))**
- **すべての項目のコピー(Copy All Items)**
- **重大度の変更(Change Severity)**
- **マーク付けする(Mark as)**
- **送信(Send to)**
- **場所の削除(Remove Location)**

[未検出(Not Found)]タブ

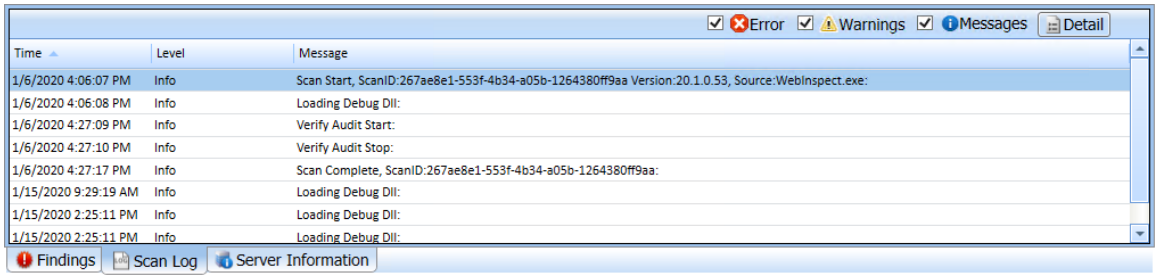
このタブは、Fortify WebInspect Enterpriseに接続した後、かつスキャンをFortify Software Security Centerと同期させた後にのみ表示されます。特定のアプリケーションバージョンで前回のスキャンによって検出されたが、現在のスキャンでは検出されていない脆弱性が一覧表示されます。これらの脆弱性はダッシュボード上のカウントには含まれないため、ナビゲーションペインの [サイト(Site)]ビューや [シーケンス(Sequence)]ビューには表示されません。

ショートカットメニューのオプション、グループ化、およびフィルタリング機能は、 **検出事項(Findings)**]タブで示されている機能のサブセットです。

[スキャンログ(Scan Log)]タブ

OpenText DASTスキャンアクティビティに関する情報を表示するには、 **[スキャンログ(Scan Log)]**タブを使用します。たとえば、Webアプリケーションに対して特定の監査手法が適用される時刻がここに一覧表示されます。さらに、スキャンに影響を与えかねない潜在的な問題

についての洞察を与えるアラートレベルのメッセージが [スキャンログ(Scan Log)] に表示されます。



[アプリケーション設定(Application Settings)] ウィンドウの [ログ記録(Logging)] オプションを使用して、ログレベル(デバッグ、情報、警告、エラー、または重大)を選択できます。詳細については、「"アプリケーション設定:ログ記録" ページ499」を参照してください。

ペイン上部の [**エラー(Errors)**]、 [**警告(Warnings)**]、 [**メッセージ(Messages)**] の各ボタンを使用して、表示されるメッセージの種類をフィルタできます。

ヒント: アラートレベルのメッセージは、 [**警告(Warnings)**] フィルタに含まれます。

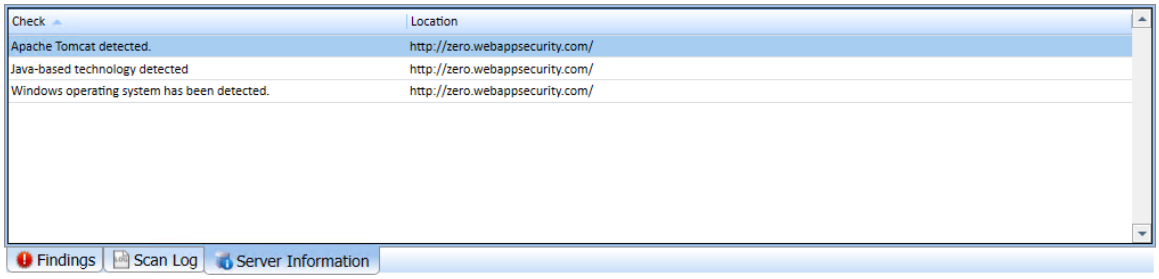
スキャンログの特定のエントリに関する詳細情報を表示するには、エントリを選択して [**詳細(Detail)**] をクリックします。

また、エントリを右クリックして、ショートカットメニューから次のオプションを選択することもできます。

- [選択した行をクリップボードにコピーする(Copy selected row to clipboard)]。
- [すべての項目をクリップボードにコピーする(Copy all items to clipboard)]。
- [このメッセージの詳細を確認する(Get more information about this message)]。

[サーバ情報(Server Information)] タブ

[サーバ情報(Server Information)] タブには、サーバに関連する重要な項目が一覧表示されます。項目またはイベントはサーバごとに1回だけ表示されます。



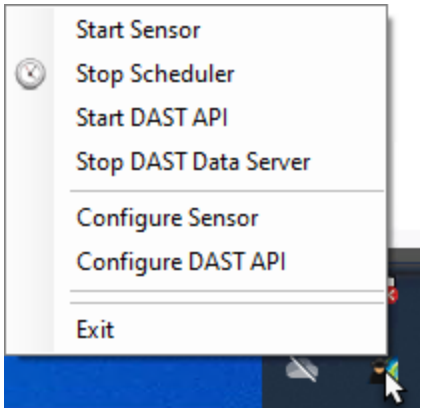
OpenText DAST Monitor

OpenText DAST Monitorプログラムは、タスクバーの通知エリアのアイコンとして表示されます。このプログラムのコンテキストメニューから、次の操作を実行できます。

- センササービスの開始または停止
- スケジューラサービスの開始または停止
- DAST Data Serverサービスの開始または停止

  重要! {/b}DAST Data Serverサービスは、スキャン中に収集されるTraffic Monitorデータベースで使用されるため、OpenText DASTスキャンにおいて不可欠です。また、自動ログアウト検出、Web Proxyツール、Traffic Viewerツール、FASTプロキシなどの他の機能とも関連があります。カスタマサポートからの指示がない限り、DAST Data Serverを停止しないでください。

- Enterprise Serverセンサの設定
- OpenText DAST APIの設定と開始または停止



特定のイベントが発生するたびにポップアップメッセージも表示されます。

第4章:スキャンの操作

この章では、OpenText DASTが実行できる各種スキャンと、それらのスキャンの実行方法について説明します。スキャンのスケジュール手順と、完了したスキャンのインポート、エクスポート、および管理の手順が収録されています。

ガイド付きスキャンの概要

ガイド付きスキャンを使用すると、最良のステップでアプリケーションに合わせてスキャンを設定できます。

左ペインにガイド付きスキャンの進行状況が表示されるため、スキャンの設定を指定するときに進行状況を簡単に確認できます。右ペインには、各ウィザードページ上のスキャンオプションが表示されます。

ガイド付きスキャンウィザードでは、次の操作を実行できます。

- アプリケーションへのコネクティビティを検証する
- アプリケーション全体またはワークフローのみをテストする
- ログイン手順を記録する
- 推奨される設定変更を確認する

ガイド付きスキャンはテンプレートに基づいています。事前定義テンプレートとモバイルテンプレートのどちらを使用するかを選択できます。

事前定義テンプレート

次に挙げる3つの事前定義テンプレートオプションから選択できます。

- **標準スキャン**: このオプションは、カバレッジを重視する場合に使用します。大規模なサイトにこのテンプレートを使用すると数日かかる場合があります。
- **クイックスキャン**: このオプションは、深く掘り下げることよりも適用範囲の広さとパフォーマンスを重視する場合に使用します。非常に大規模なサイトに特に適しています。
- **徹底スキャン**: サイト上で徹底的なWeb探索を実行するために使用します。これらの設定を使用する場合は、サイトを各部に分割して、サイトの小部分だけをスキャンすることをお勧めします。大規模なサイトにはお勧めしません。

モバイルテンプレート

次の2つのモバイルテンプレートオプションの中から選択できます。

- **モバイルスキャン**: このオプションは、OpenText DASTまたはFortify WebInspect Enterpriseのインスタンスがインストールされているマシンからモバイルサイトをスキャンする場合に使用

します。このオプションを選択すると、OpenText DASTまたはFortify WebInspect Enterpriseはサイト全体ではなくサイトのモバイルバージョンをフェッチします。

- **ネイティブスキャン**: このオプションは、ネイティブモバイルアプリケーションを手動でWeb探索し、Webトラフィックをワークフローマクロとしてキャプチャする場合に使用します。モバイルアプリケーションを実行しているAndroid、Windows、またはiOSデバイスまたはソフトウェアエミュレータ(AndroidおよびiOSのみ)でトラフィックを生成します。

ガイド付きスキャンテンプレートを選択すると、左ペインにステージとステップが表示されます。このペインでは、これらの間を簡単に移動して、スキャンの設定を指定できます。

参照情報

"事前定義テンプレートの使用" 次のページ

"モバイルスキャンテンプレートの使用" ページ130

"ネイティブスキャンテンプレートの使用" ページ147

ガイド付きスキャンの実行

左ペインにガイド付きスキャンの進行状況が表示されるため、スキャンの設定を指定するときに進行状況を簡単に確認できます。右ペインには、各ウィザードページ上のスキャンオプションが表示されます。

ガイド付きスキャンの最初のページには、実行するスキャンのタイプを選択するオプションが表示されます。3つの主要なタイプから選択できます。

事前定義テンプレート(標準、クイック、または詳細)

次に挙げる3つの事前定義テンプレートオプションから選択できます。

- **標準スキャン**: デフォルトのスキャン設定は、パフォーマンスよりもカバレッジを重視して設計されています。これらの設定を使用して大規模なサイトをWeb探索するには数日かかる場合があります。
- **クイックスキャン**: 深く掘り下げることよりも、範囲の広さとパフォーマンスを重視したスキャン。非常に大規模なサイトに特に適しています。
- **徹底スキャン**: 徹底スキャンの設定は、サイトの徹底的なWeb探索を実行するように設計されています。これらの設定を使用する場合は、サイトをいくつかの部分に分割して、サイトの小部分だけをスキャンすることをお勧めします。大規模なサイトにはお勧めしません。

詳細については、「"事前定義テンプレートの使用" 次のページ」を参照してください。

モバイルスキャンテンプレート

このテンプレートは、Webアプリケーションのスキャン中にモバイルデバイスをエミュレートします。

詳細については、「"モバイルスキャンテンプレートの使用" ページ130」を参照してください。

ネイティブスキャンテンプレート

このテンプレートは、ネイティブモバイルアプリケーションを手動でWeb探索し、Webトラフィックをワークフローマクロとしてキャプチャします。

詳細については、「"ネイティブスキャンテンプレートの使用" ページ147」を参照してください。

参照情報

"ガイド付きスキャンの概要" ページ111

"OpenText DAST ポリシー" ページ509

事前定義テンプレートの使用

ガイド付きスキャンウィザードでは、Webサイトのスキャンに必要なステージとステップを順に実行します。前のステップまたはステージに戻る必要がある場合は、 [戻る]ナビゲーションボタンをクリックするか、ガイド付きスキャンツリー内のステップをクリックして、そこに直接移動します。

推奨

OpenTextでは、スキャンを一度に1回だけ実行することをお勧めします。SQL Expressを使用する場合は特に、サイトのサイズによっては、同時(または並行)スキャンを実行すると、OpenText DASTホスト上のRAM、CPU、およびディスクリソースの使用率が高くなる場合があります。

ガイド付きスキャンの起動

ガイド付きスキャンを起動するには:

- OpenText DASTのユーザは、左側のペインの [ガイド付きスキャンの開始(Start a Guided Scan)]オプションをクリックするか、またはメニューバーから **[ファイル(File)] > [新規(New)] > [ガイド付きスキャン(Guided Scan)]**を選択します。
- Fortify WebInspect Enterpriseのユーザは、Webコンソールで [アクション(Actions)]の下にある **[ガイド付きスキャン(Guided Scan)]**をクリックします。

ガイド付きスキャンウィザードが起動し、ガイド付きスキャンテンプレートのリストが表示されます。次に挙げる3つの事前定義テンプレートオプションから選択できます。

- **標準スキャン**: このオプションは、カバレッジを重視する場合に使用します。大規模なサイトにこのテンプレートを使用すると数日かかる場合があります。
- **クイックスキャン**: このオプションは、深く掘り下げることよりも適用範囲の広さとパフォーマンスを重視する場合に使用します。非常に大規模なサイトに特に適しています。
- **徹底スキャン**: サイト上で徹底的なWeb探索を実行するために使用します。これらの設定

を使用する場合は、サイトを各部に分割して、サイトの小部分だけをスキャンすることをお勧めします。大規模なサイトにはお勧めしません。

いずれかの**事前定義テンプレート**を選択します。

レンダリングエンジンについて

選択するレンダリングエンジンによって、ガイド付きスキャンの設定時に新しいマクロの記録または既存のマクロの編集を行うときに開かれるWeb Macro Recorderが決まります。レンダリングエンジンのオプションは次のとおりです。

- **セッションベース(Session-based)** -このオプションを選択すると、セッションベースのWeb Macro Recorderが指定されます。これはInternet Explorerブラウザテクノロジを使用します。
- **イベントベース(Event-based) (優先)** - このオプションを選択すると、TruClientおよびFirefox技術を使用するイベントベースのWebマクロレコーダが指定されます。

Webサイトの確認

Webサイトを確認するには:

1. [開始URL(Start URL)]ボックスで、スキャンするサイトの完全なURLまたはIPアドレスを入力または選択します。

   URLを入力する場合は、正確に入力する必要があります。たとえば「MYCOMPANY.COM」と入力すると、OpenText DASTまたはFortify WebInspect EnterpriseはWWW.MYCOMPANY.COMなどのバリエーションはスキャンしません([許可ホスト(Allowed Hosts)]設定で代替URLを指定している場合を除く)。

   無効なURLまたはIPアドレスを指定すると、エラーが発生します。階層ツリー内の特定の位置からスキャンを実行する場合は、スキャンの開始点(http://www.myserver.com/myapplication/など)を追加します。

   IPアドレスによるスキャンでは、(相対パスではなく)完全修飾URLを使用するリンクを追跡しません。

   注記: OpenText DASTでは、WebサイトスキャンおよびWebサービススキャンでIPv6 (Internet Protocolバージョン6)アドレスがサポートされています。開始URLを指定する場合は、IPv6アドレスを括弧で囲む必要があります。例:

   - http://[::1]
     OpenText DASTは「localhost」をスキャンします。
   - http://[fe80::20c:29ff:fe32:bae1]/subfolder/
     OpenText DASTは、指定されたアドレスのホストのスキャンを「subfolder」ディレクトリから開始します。
   - http://[fe80::20c:29ff:fe32:bae1]:8080/subfolder/

> OpenText DASTは、ポート8080で実行されているサーバのスキャンを「subfolder」から開始します。

OpenText DASTおよびFortify WebInspect Enterpriseでは、IPV4 (Internet Protocol バージョン4)とIPV6 (Internet Protocolバージョン6)の両方がサポートされています。IPV6アドレスは括弧で囲む必要があります。

2. (オプション)スキャン範囲を特定のエリアに限定するには、 **[フォルダに限定(Restrict to Folder)]**チェックボックスをオンにし、リストから次のいずれかのオプションを選択します。

   [ディレクトリのみ(自己) (Directory only (self))]。OpenText DASTおよびFortify WebInspect Enterpriseは、指定されたURLのみをWeb探索または監査(またはその両方)します。たとえば、このオプションを選択してwww.mycompany/one/two/というURLを指定すると、OpenText DASTまたはFortify WebInspect Enterpriseは「two」ディレクトリのみを評価します。

   [ディレクトリおよびサブディレクトリ(Directory and subdirectories)]。OpenText DASTおよびFortify WebInspect Enterpriseは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも上位のディレクトリにはアクセスしません。

   [ディレクトリおよび親ディレクトリ(Directory and parent directories)]。OpenText DASTおよびFortify WebInspect Enterpriseは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも下位のディレクトリにはアクセスしません。

   [フォルダに限定(Restrict to folder)]スキャンオプションの制限については、"「フォルダに限定」に関する制限" ページ227を参照してください。

3. **[検証(Verify)]**をクリックします。

   Webサイトが、共通アクセスカード(CAC)またはパスワードで保護されている証明書を使用してクライアント証明書で認証するように設定されている場合、ガイド付きスキャンでは次のメッセージが表示されます。

   サイト *<URL>*がクライアント証明書を要求しています。今すぐ設定しますか? (The site <URL> is requesting a client certificate. Would you like to configure one now?)

   CACを使用するクライアント証明書またはパスワードで保護されている証明書を設定するには:

   a. **[Yes]**をクリックします。

      [クライアント証明書の選択(Select a Client Certificate)]ウィンドウが表示されます。

   b. [証明書ストア(Certificate Store)]で、 **[現在のユーザ(Current User)]**を選択します。

      使用可能な証明書のリストが [証明書(Certificate)]エリアに表示されます。

   c. 「(Protected)」というプレフィクスが付いた証明書を見つけて選択します。

      選択した証明書に関する情報と [パスワード/PIN (Password/PIN)]フィールドが [証明書情報(Certificate Information)]エリアに表示されます。

   d. パスワードまたはPINが必要な場合は、 **[パスワード/PIN (Password/PIN)]**フィールドに入力します。

注記: パスワードまたはPINが必要であるのに、ここで入力していないと、スキャン中にWindowsの [セキュリティ] ウィンドウのプロンプトが表示されるたびに、パスワードまたはPINを入力することが必要になります。

重要! {/b}デフォルトでは、OpenText DASTはOpenSSLを使用します。OpenSSLではなく特定のSSL/TLSプロトコルを使用している場合、スキャン設定のProfiler部分はパスワードで保護されている証明書で動作しない場合があります。

e. **[テスト(Test)]** をクリックします。

4. プロキシサーバ経由でターゲットサイトにアクセスする必要がある場合は、メイン画面の左下にある **[プロキシ(Proxy)]** をクリックして [プロキシ設定(Proxy Settings)] エリアを表示し、 **[プロキシ設定(Proxy Settings)]** リストからオプションを選択します。
   - **直接接続(プロキシ無効)(Direct Connection (proxy disabled))**
   - **プロキシ設定の自動検出(Auto detect proxy settings)**: WPAD (Web Proxy Autodiscovery Protocol)を使用してプロキシ自動設定ファイルを見つけ、このファイルを使用してブラウザのWebプロキシ設定を行います。
   - **システムのプロキシ設定を使用する(Use System proxy settings)**: ローカルマシンからプロキシサーバ情報をインポートします。
   - **Firefoxプロキシ設定を使用する(Use Firefox proxy settings)**: Firefoxからプロキシサーバ情報をインポートします。
   - **PACファイルを使用してプロキシ設定を行う(Configure proxy settings using a PAC File)**: PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。このオプションを選択した場合は、 **[編集(Edit)]** をクリックしてPACの場所(URL)を入力します。
   - **プロキシを明示的に設定する(Explicitly configure proxy settings)**: 指示に従ってプロキシサーバ設定を指定します。このオプションを選択した場合は、表示されるフィールドにプロキシ情報を入力します。

   重要! {/b}Socks4プロキシサーバは認証に対応しません。認証が必要なSocksプロキシサーバを使用する場合は、Socks5プロキシを使用する必要があります。

   注記: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が [プロキシーを使用しない] に設定されている場合、またはWindowsの [LANにプロキシサーバを使用する] 設定が選択されていない場合、プロキシサーバは使用されません。

   Webサイトまたはディレクトリ構造のスクリーンショットが表示されたら、開始URLへの接続の検証が正常に完了しています。

5. **[次へ(Next)]** をクリックします。
   [スキャンタイプの選択(Choose Scan Type)] ウィンドウが表示されます。

スキャンタイプの選択

1. [スキャン名(Scan Name)]ボックスにスキャンの名前を入力します。
2. 次のいずれかのスキャンタイプを選択します。
   - **標準(Standard)**: OpenText DASTおよびFortify WebInspect Enterpriseは自動分析を実行し、ターゲットURLから開始します。これは標準的なスキャン開始方法です。
   - **ワークフロー(Workflows)**: このオプションを選択すると、ガイド付きスキャンにワークフローステージが追加されます。
3. [スキャン方法(Scan Method)]エリアで、次のいずれかのスキャン方法を選択します。
   - **Web探索のみ(Crawl Only)**。このオプションを選択すると、サイトの階層データ構造が完全にマッピングされます。Web探索が完了したら、[監査(Audit)]をクリックしてアプリケーションの脆弱性を評価できます。
   - **Web探索および監査(Crawl and Audit)**。OpenText DASTおよびFortify WebInspect Enterpriseは、サイトの階層データ構造をマッピングし、各リソース(ページ)を監査します。選択したデフォルト設定に応じて、各リソースの検出時またはサイト全体のWeb探索後に監査を実行できます。Web探索および監査の同時実行と順次実行の詳細については、「"スキャン設定:方法" ページ402」を参照してください。
   - **監査のみ(Audit Only)**。OpenText DASTおよびFortify WebInspect Enterpriseは、選択されたポリシーの手法を適用して脆弱性リスクを判断しますが、Webサイトの Web探索は行いません。サイト上のリンクをたどることも評価することもありません。
4. [ポリシー(Policy)]エリアの[ポリシー(Policy)]リストからポリシーを選択します。ポリシーの管理の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Policy Manager」の章を参照してください。
5. [Web探索のカバレッジ(Crawl Coverage)]エリアで、**[Web探索のカバレッジ(Crawl Coverage)]**スライダを使用してカバレッジのレベルを選択します。Web探索のカバレッジレベルの詳細については、"Web検索範囲と徹底性の設定" ページ208を参照してください。
6. **[シングルページアプリケーション(Single-Page Applications)]**エリアで、SPA (single-page application)のWeb探索および監査のオプションを選択します。有効にすると、DOMスクリプトエンジンは、Web探索中に、JavaScriptインクルード、フレームとiframeのインクルード、CSSファイルインクルード、およびAJAX呼び出しを検索してから、それらのイベントによって生成されたすべてのトラフィックを監査します。[シングルページアプリケーション(Single-Page Applications)]のオプションは次のとおりです。
   - **自動(Automatic)** - OpenText DASTがSPAフレームワークを検出すると、自動的にSPAサポートモードに切り替わります。
   - **有効(Enabled)** - SPAフレームワークがターゲットアプリケーションで使用されていることを示します。

   注意! {/b}SPAサポートは、シングルページアプリケーションに対してのみ有効にするべきです。SPAサポートを有効にしてSPA以外のWebサイトをスキャンすると、ス

キャンが遅くなります。

- **無効(Disabled)** - SPAフレームワークがターゲットアプリケーションで使用されていないことを示します。

詳細については、「"シングルページアプリケーションスキャンについて" ページ235」を参照してください。

7. [**次へ(Next)**]ボタンをクリックします。
ログインステージが表示され、左側のペインでネットワーク認証が強調表示されます。

ネットワーク認証の設定

ネットワークでユーザ認証が必要な場合は、ここで設定できます。ネットワークでユーザ認証が不要な場合は、[次へ(Next)]ナビゲーションボタン、またはガイド付きスキャンツリーの次の該当ステップをクリックして続行します。

ネットワーク認証を設定するには:

1. [**ネットワーク認証(Network Authentication)**]チェックボックスをクリックします。
2. 認証メソッドのドロップダウンリストから、**メソッド**を選択します。認証メソッドは次のとおりです。
   - **ADFS CBT**
   - **自動**
   - **基本**
   - **ダイジェスト**
   - **Kerberos**
   - **ネゴシエート(Negotiate)**
   - **NT LAN Manager (NTLM)**
   - **OAuth 2.0 Bearer**
3. 次のいずれかを実行します。
   - OAuth 2.0 Bearer*以外*のすべての認証方法では、[**ユーザ名(User name)**]ボックスにユーザIDを入力し、[**パスワード(Password)**]ボックスにユーザのパスワードを入力します。
   - OAuth 2.0 Bearerメソッドの場合は、[**設定(Configure)**]をクリックし、"OAuth 2.0のBearer資格情報の設定" ページ447の手順に従います。

クライアント証明書の使用

ネットワーク認証にクライアント証明書を使用するには:

1. ネットワーク認証にクライアント証明書を使用するには、 **[クライアント証明書(Client Certificate)]**を選択します。
2. **[証明書ストア(Certificate Store)]**エリアで、次のいずれかを選択してから、 **[マイ(My)]**または **[ルート(Root)]**ラジオボタンを選択します。
   - **[ローカルマシン(Local Machine)]**。OpenText DASTは、 **[証明書ストア(Certificate Store)]**エリアで選択した内容に基づいて、ローカルマシン上の証明書を使用します。
   - **[現在のユーザ(Current User)]**。OpenText DASTは、 **[証明書ストア(Certificate Store)]**エリアで選択した内容に基づいて、現在のユーザの証明書を使用します。
3. **[証明書情報(Certificate Information)]**エリアに証明書の詳細を表示するには、証明書を選択します。
4. **[次へ(Next)]**ボタンをクリックします。
   [アプリケーション認証(Application Authentication)]ページが表示されます。

アプリケーション認証の設定

サイトで認証が必要な場合は、このステップを使用してログインマクロを作成、選択、または編集することにより、ログインプロセスを自動化してサイトのカバレッジを拡大できます。ログインマクロは、アプリケーションにアクセスしてログインするために必要なアクティビティの記録です。通常は、ユーザ名とパスワードを入力し、 **[ログイン]**や **[ログオン]**などのボタンをクリックします。

ログインマクロを使用するスキャンの **[スキャン設定:認証(Scan Settings: Authentication)]**で **[マクロ検証を有効にする(Enable macro validation)]**が選択されている場合、OpenText DASTはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

注記: マクロテストは、2要素認証を含むマクロに対してはサポートされていません。

重要! {/b}2要素認証を含むマクロを使用する場合は、スキャンを開始する前に、2要素認証アプリケーションの設定を行う必要があります。詳細については、「"アプリケーション設定:2要素認証" ページ491」を参照してください。

ログインマクロでは、次のオプションを使用できます。

- "権限のエスカレーションなしでログインマクロを使用する" 次のページ
- "権限のエスカレーションのためにログインマクロを使用する" 次のページ
- "Fortify WebInspect Enterpriseに接続しているときにログインマクロを使用する" ページ122

マスクされた値のサポート

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、OpenText DASTでガイド付きスキャンを設定するときにも、それらの値はマスクされます。

権限のエスカレーションなしでログインマクロを使用する

ログインマクロを使用するには:

1. **[このサイトでログインマクロを使用する(Use a login macro for this site)]** チェックボックスをオンにします。
2. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン([..])をクリックして、保存されているマクロを参照します。
   - **[ログインマクロ(Login Macro)]** フィールドに表示されている既存のログインマクロを編集するには、 **[編集(Edit)]** をクリックします。
   - 新しいマクロを記録するには、 **[作成(Create)]** をクリックします。

   新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。
3. **[次へ(Next)]** ボタンをクリックします。

   標準スキャンを選択した場合は、 **[最適化タスク(Optimization Tasks)]** ページが表示されます。ワークフロースキャンを選択した場合は、 **[ワークフローの管理(Manage Workflows)]** ページが表示されます。

権限のエスカレーションのためにログインマクロを使用する

権限のエスカレーションポリシーか、有効な権限のエスカレーションチェックを含む別のポリシーを選択した場合、高い権限を持つユーザアカウント用のログインマクロが少なくとも1つ必要です。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。

ログインマクロを使用するには:

1. **[高い権限のユーザアカウントログインマクロ(High-Privilege User Account Login Macro)]** チェックボックスをオンにします。このログインマクロは、サイト管理者やモデレータアカウントなど、より高い権限を持つユーザアカウント用です。
2. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン([..])をクリックして、保存されているマクロを参照します。

- [ログインマクロ(Login Macro)]フィールドに表示されている既存のログインマクロを編集するには、**[編集(Edit)]**をクリックします。
- 新しいマクロを記録するには、**[作成(Create)]**をクリックします。

新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。

最初のマクロを記録または選択して[次へ(Next)]の矢印をクリックすると、[低い権限のログインマクロを設定する(Configure Low Privilege Login Macro)]プロンプトが表示されます。

3. 次のいずれかを実行します。
   - 認証モードでスキャンを実行するには、**[はい(Yes)]**をクリックします。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。

     ガイド付きスキャンが[ログインマクロの選択(Select Login Macro)]ウィンドウに戻り、低い権限のログインマクロを作成または選択できるようになります。ステップ4に進みます。
   - スキャンを非認証モードで実行するには、**[いいえ(No)]**をクリックします。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。

     アプリケーション認証のステップが完了しました。標準スキャンを選択した場合は、[最適化タスク(Optimization Tasks)]ページが表示されます。ワークフロースキャンを選択した場合は、[ワークフローの管理(Manage Workflows)]ページが表示されます。
4. **[低い権限のユーザアカウントログインマクロ(Low-Privilege User Account Login Macro)]**チェックボックスをオンにします。このログインマクロは、サイトコンテンツのビューアやコンシューマなど、低い権限のユーザアカウント用です。
5. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン([..])をクリックして、保存されているマクロを参照します。
   - [ログインマクロ(Login Macro)]フィールドに表示されている既存のログインマクロを編集するには、**[編集(Edit)]**をクリックします。
   - 新しいマクロを記録するには、**[作成(Create)]**をクリックします。

   新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。
6. 2つ目のマクロを記録または選択した後、**[次へ(Next)]**ボタンをクリックします。

   標準スキャンを選択した場合は、[最適化タスク(Optimization Tasks)]ページが表示されます。ワークフロースキャンを選択した場合は、[ワークフローの管理(Manage Workflows)]ページが表示されます。

Fortify WebInspect Enterpriseに接続しているときにログインマクロを使用する

Fortify WebInspect Enterpriseに接続されているOpenText DASTの場合は、Fortify WebInspect Enterpriseマクロリポジトリからログインマクロをダウンロードして使用できます。

マクロをダウンロードするには:

1. [**このサイトでログインマクロを使用する(Use a login macro for this site)**]チェックボックスをオンにします。
2. [**ダウンロード(Download)**]をクリックします。
   [Fortify WebInspect Enterpriseからマクロをダウンロードする(Download a Macro from Fortify WebInspect Enterprise)]ウィンドウが表示されます。
3. ドロップダウンリストから[**アプリケーション(Application)**]と[**バージョン(Version)**]を選択します。
4. [**マクロ(Macro)**]ドロップダウンリストからリポジトリマクロを選択します。
5. [**OK**]をクリックします。

注記: リポジトリマクロを選択すると、[最終確認(Final Review)]ページの[**自動でスキャンをWIEにアップロードする(Automatically Upload Scan to WIE)**]の[**アプリケーション(Application)**]と[**バージョン(Version)**]が自動的に同期されます。

ログインマクロを自動的に作成する

ユーザ名とパスワードを入力して、OpenText DASTでログインマクロを自動的に作成できます。

注記: 権限のエスカレーションおよびマルチユーザログインスキャンに対して、また、セッションベースのレンダリングエンジンを使用するスキャンに対して自動でログインマクロを作成することはできません。

ログインマクロを自動的に作成するには:

1. [**ログインマクロの自動生成(Auto-gen Login Macro)**]を選択します。
2. [**ユーザ名(Username)**]フィールドにユーザ名を入力します。
3. [**パスワード(Password)**]フィールドにパスワードを入力します。

オプションで、[**テスト(Test)**]をクリックして、ログインフォームの検索、マクロの生成、マクロ検証テストの実行を行ってから、ガイド付きスキャンウィザードの次のステージに進みます。完了前に検証テストをキャンセルする必要がある場合は、[**キャンセル(Cancel)**]をクリックします。

マクロが無効で、アプリケーションへのログインが失敗すると、エラーメッセージが表示されます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

ワークフローの設定

ワークフローステージは、サイトステージで [スキャンタイプ(Scan Type)] として [ワークフロー(Workflows)] を選択した場合にのみ表示されます。 [標準(Standard)] を選択した場合、ワークフローステージは表示されません。ワークフローマクロを作成すると、マクロで指定したページをOpenText DASTで確実に監査できます。OpenText DASTはマクロに含まれているURLのみを監査し、監査中に検出されたハイパーリンクはたどりません。ログアウト署名は不要です。この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。

重要! {/b}ログインマクロをワークフローマクロと起動マクロのどちらかまたはその両方と組み合わせて使用する場合は、すべてのマクロが同じタイプでなければなりません。すべてが.webmacroファイル、すべてがBurp Proxyキャプチャ、またはすべてが.harファイルのいずれかです。同じスキャンで異なる種類のマクロを使用することはできません。

ワークフローの設定を完了するには、 [ワークフロー(Workflow)] テーブルで次のいずれかをクリックします。

- **[記録(Record)]**。Web Macro Recorderが開き、マクロを作成できます。
- **[編集(Edit)]**。Web Macro Recorderが開き、選択したマクロがロードされます。
- **[削除(Delete)]**。選択したマクロが削除されます(ただしディスクからは削除されません)。
- **[インポート(Import)]**。標準のファイル選択ウィンドウが開き、過去に記録された.webmacroファイル、Burp Proxyキャプチャ、または.harファイルを選択できます。

  注記: コンピュータにOpenText UFT One (Unified Functional Testing)がインストールされている場合は、OpenText DASTがこれを自動的に検出し、UFT .usrファイルをインポートするためのオプションを表示します。

  詳細については、「"ガイド付きスキャンでの機能テストファイルのインポート" ページ162」を参照してください。
- **[エクスポート(Export)]**。標準のファイル選択ウィンドウが開き、記録したマクロを保存できます。

ワークフローマクロを指定して再生すると、 [ワークフロー(Workflows)] テーブルにそのマクロが表示され、許可ホストが **[ガイド付きスキャン(Guided Scan)] > [ワークフロー(Workflows)] > [ワークフロー(Workflows)] > [マネージャワークフロー(Manager Workflow)]** ページに追加されます。特定のホストへのアクセスを有効または無効にできます。詳細については、「"スキャン設定: 許可ホスト" ページ421」を参照してください。

Burp Proxy結果の追加

Burp Proxyセキュリティテストを実行した場合、テスト中に収集されたトラフィックをワークフローマクロにインポートできます。これにより、同じエリアの再スキャンにかかる時間が短縮されます。

ワークフローマクロにBurp Proxy結果を追加するには:

1. [ワークフロー(Workflows)]画面が表示されていない場合は、[ガイド付きスキャン(Guided Scan)]ツリーの[**ワークフローの管理(Manage Workflows)**]ステップをクリックします。
2. [**インポート(Import)**]ボタンをクリックします。
   [マクロのインポート(Import Macro)]ファイルセレクタが表示されます。
3. ファイルの種類ボックスのフィルタを[Webマクロ(*.webmacro)(Web Macro (*.webmacro))]から[Burp Proxy (*.*)]に変更します。
4. Burp Proxyファイルに移動し、目的のファイルを選択します。
5. [**開く(Open)**]をクリックします。

Profilerの使用

OpenText DAST Profilerは、ターゲットWebサイトの事前テストを実行し、特定の設定を変更すべきかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Profilerは、サイトに入るために権限付与が必要であるものの、有効なユーザ名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Profilerの提案に従って、続行する前に必要な情報を設定することができます。

同様に、設定では、OpenText DASTが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにOpenText DAST設定を変更することを推奨します。

Profilerを起動するには:

1. [**プロファイル(Profile)**]をクリックします。
   Profilerが実行されます。詳細については、「"Server Profiler" ページ283」を参照してください。
   結果は、[設定(Settings)]セクションの[スキャンの最適化(Optimize scan for)]ボックスに表示されます。
2. [スキャンの最適化(Optimize scan for)]ドロップダウンボックスに表示される提案を受け入れるかまたは拒否します。提案を拒否するには、ドロップダウンメニューから[なし(None)]または代わりの提案を選択します。
3. 必要に応じて、要求された情報を入力します。
4. [**次へ(Next)**]ボタンをクリックします。

Profilerを実行していない場合でも、いくつかのオプションが表示されることがあります。これについては、以降のセクションで説明します。

Webフォームの自動入力(Autofill web forms)

OpenText DASTがターゲットサイトのスキャン中に検出されるフォームの入力コントロールの値を送信するようにするには、[**Web探索時のWebフォームの自動入力(Auto-fill Web forms during crawl)**]を選択します。OpenText DASTは、事前パッケージ化されたデフォルトファイル、またはWeb Form Editorを使用して作成したファイルから値を抽出します。『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Web Form Editor」に関する章を参照してください。以下を実行できます。

1. 省略記号ボタン(...)をクリックして、ファイルを見つけてロードします。
2. [**編集(Edit)**]をクリックして、選択したファイル(またはデフォルト値)をWeb Form Editorで編集します。
3. [**作成(Create)**]をクリックしてWeb Form Editorを開き、ファイルを作成します。

許可ホストを追加する

[許可ホスト(Allowed Host)]設定は、Web探索して監査するドメインを追加する場合に使用します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここに追加します。詳細については、「"スキャン設定:許可ホスト" ページ421」を参照してください。

許可するドメインを追加するには:

1. [**追加(Add)**]をクリックします。
2. [許可ホストの指定(Specify Allowed Host)]ウィンドウで、URL(またはURLを表す正規表現)を入力し、[**OK**]をクリックします。

識別された抑制された検出事項を再利用する

以前のスキャンで誤検出に変更された、または無視された脆弱性をインポートできます。これらの誤検出または無視された項目が現在のスキャンで検出された脆弱性と一致する場合、その脆弱性は誤検出に変更されるか、無視されます。既存のスキャンまたは抑制された検出事項ファイルから、抑制された検出事項をインポートできます。詳細については、「"抑制された検出事項" ページ83」を参照してください。

識別された抑制された検出事項を再利用するには:

1. [**抑制された検出事項のインポート(Import Suppressed Findings)**]を選択します。
2. 次の表に従って続行します。

使用する情報...	その場合...
既存のスキャン	a. [**抑制された検出事項をスキャンからインポートするには、ここをクリックします(Click here to import suppressed findings from scans)**]をクリックします。 [スキャンを選択して、抑制された検出事項をインポートする(Select a Scan to Import Suppressed Findings)]ダイアログが開きます。

使用する情報...	その場合...
	b. 現在スキャンしている同じサイトからの、抑制された検出事項を含むスキャンを1つ以上選択します。 c. [OK]をクリックします。
抑制された検出事項ファイル	a. [抑制された検出事項をファイルからインポートするには、ここをクリックします(Click here to import suppressed findings from a file)]をクリックします。 標準のWindowsファイル選択ダイアログボックスが開きます。 b. インポートするファイルを選択し、[開く(Open)]をクリックします。 c. 必要に応じて、ステップaとbを繰り返して追加のファイルを選択します。

サンプルマクロの適用

OpenTextのサンプルバンキングアプリケーション(zero.webappsecurity.com)では、Webフォームログインが使用されています。このサイトをスキャンする場合は、[**サンプルマクロの適用(Apply sample macro)**]を選択して、ログインスクリプトを含む事前パッケージ化されたマクロを実行します。

トラフィック分析

Web Proxyツールを使用してOpenText DASTにより発行されたHTTP要求とターゲットサーバから返された応答を検査するには、[**Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)**]を選択します。

OpenText DASTはWebサイトのスキャン中に、Webサイトの階層構造を明らかにするセッションと、脆弱性が検出されたセッションのみをナビゲーションペインに表示します。ただし[**Traffic Monitorを有効にする(Enable Traffic Monitor)**]を選択すると、OpenText DASTでは[**Traffic Monitor**]ボタンが[スキャン情報(Scan Info)]パネルに追加されます。これにより、OpenText DASTが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。

メッセージ

Profilerが変更を推奨しない場合は、ガイド付きスキャンウィザードに「設定の変更は推奨されません。現在のスキャン設定はこのサイトに最適です。(No settings changes are recommended. Your current scan settings are optimal for this site.)」というメッセージが表示されます。

[**次へ(Next)**]をクリックします。

[最終確認(Final Review)]ページが表示され、左側のペインで[**詳細オプションの設定(Configure Detailed Options)**]が強調表示されます。

追加オプションの設定

詳細オプションを設定するには、次の設定を指定します。

識別された誤検出を再利用する(Reuse Identified False Positives)

OpenText DASTによってすでに識別されている誤検出を再利用するには、 **[誤検出(False Positives)]** ボックスをオンにします。

トラフィック分析

1. Web Proxyツールを使用するには、 **[Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)]** を選択して、OpenText DASTが発行したHTTP要求と、ターゲットサーバから返された応答を調べます。

   Web Proxyはスタンドアロンの自己完結型プロキシサーバであり、デスクトップ上で設定および実行できます。Web Proxyを使用すると、スキャナ、Webブラウザ、またはHTTP要求を送信してサーバから応答を受信するその他のツールからのトラフィックを監視できます。Web Proxyは、デバッグと侵入スキャンのためのツールです。サイトのブラウズ中に、すべての要求とサーバの応答を確認できます。
2. OpenText DASTによって送信された各HTTP要求と、サーバから受信した関連HTTP応答を表示および確認するには、 **[Traffic Monitor]** ボックスを選択します。

   OpenText DASTはWebサイトのスキャン中に、Webサイトの階層構造を明らかにしたセッションと、脆弱性が検出されたセッションのみを表示します。ただし **[Traffic Monitorを有効にする(Enable Traffic Monitor)]** を選択すると、OpenText DASTではOpenText DASTが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。
3. **[次へ(Next)]** をクリックします。

   [設定の検証とスキャンの開始(Validate Settings and Start Scan)] ページが表示され、左側のペインで **[詳細オプションの設定(Configure Detailed Options)]** が強調表示されます。

設定の検証とスキャンの開始

このページのオプションを使用すると、現在のスキャン設定を保存することができます。また、OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、Fortify WebInspect Enterpriseとやり取りすることができます。

1. スキャン設定をXMLファイルとして保存するには、 **[ここをクリックして設定を保存する(Click here to save settings)]** を選択します。標準の **[名前を付けて保存(Save as)]** ウィンドウを使用して、ファイルに名前を付けて保存します。
2. OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、ツールバーに **[テンプレート(Templates)]** セクションが表示されます。次の表に従って続行します。

目的の作業	その場合の手順
現在のスキャン設定をテンプレートとしてFortify WebInspect Enterpriseデータベースに保存する **注記:** 既存のテンプレートを編集する場合、[保存(Save)]を実行すると、実際には更新が行われます。設定の編集を保存したり、テンプレート名を変更したりすることができます。ただし、アプリケーション、バージョン、またはグローバルテンプレートの設定は変更できません。	a. 次のいずれかを実行します。 ◦ ツールバーの[テンプレート(Templates)]セクションで[**保存(Save)**]をクリックします。 ◦ [**ここをクリックしてテンプレートを保存する(Click here to save template)**]を選択します。 [テンプレートの保存(Save Template)]ウィンドウが表示されます。 b. [**アプリケーション(Application)**]ドロップダウンリストからアプリケーションを選択します。 c. [**バージョン(Version)**]ドロップダウンリストからアプリケーションバージョンを選択します。 d. [**テンプレート(Template)**]フィールドに名前を入力します。
テンプレートからスキャン設定をロードする	a. ツールバーの[テンプレート(Templates)]セクションで[**ロード(Load)**]をクリックします。 現在のスキャン設定が失われるという確認メッセージが表示されます。 b. [**Yes**]をクリックします。 [テンプレートのロード(Load Template)]ウィンドウが表示されます。 c. [**アプリケーション(Application)**]ドロップダウンリストからアプリケーションを選択します。 d. [**バージョン(Version)**]ドロップダウンリストからアプリケーションバージョンを選択します。 e. [**テンプレート(Template)**]ドロップダウンリストからテンプレートを選択します。

目的の作業	その場合の手順
	f. [ロード(Load)]をクリックします。 ガイド付きスキャンがサイトステージに戻り、Webサイトの検証と、テンプレートからのステップごとの設定の実行が行えるようになります。

3. OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、このページに [Fortify WebInspect Enterprise]セクションが表示されます。Fortify WebInspect Enterpriseを操作するには、次のようにします。
   a. [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。
   b. [バージョン(Version)]ドロップダウンリストからアプリケーションバージョンを選択します。
   c. 次の表に従って続行します。

スキャンの実行方法	その場合の手順
Fortify WebInspect Enterpriseでセンサを使用する	i. [WebInspect Enterpriseで実行(Run in WebInspect Enterprise)]を選択します。 ii. [センサ(Sensor)]ドロップダウンリストからセンサを選択します。 iii. スキャンの[優先度(Priority)]を選択します。
OpenText DASTを使用する	i. [DASTで実行(Run in DAST)]を選択します。 ii. スキャン結果をFortify WebInspect Enterpriseの指定したアプリケーションおよびバージョンに自動的にアップロードする場合は、[WebInspect Enterpriseへの自動アップロード(Auto Upload to WebInspect Enterprise)]を選択します。 **注記:** スキャンが正常に完了しない場合、Fortify WebInspect Enterpriseにはアップロードされません。

4. [今すぐスキャン(Scan Now)]エリアでスキャン設定を見直し、[スキャンの開始(Start Scan)]をクリックしてスキャンを開始します。

参照情報

"ガイド付きスキャンの概要" ページ111

モバイルスキャンテンプレートの使用

モバイルスキャンテンプレートを使用してモバイルWebサイトスキャンを作成すると、OpenText DASTまたはFortify WebInspect Enterprise内から、デスクトップバージョンのブラウザを使用してWebサイトのモバイルバージョンをスキャンできます。

モバイルスキャンは、Webサイトスキャンとほぼ同じであり、事前定義テンプレートの1つを使用して標準、徹底、またはクイックスキャンを実行するときに検出する設定オプションを反映します。唯一の違いは、ブラウザでモバイルブラウザをエミュレートできるようにするためにユーザエージェントヘッダを選択する必要がある点です。

OpenText DASTおよびFortify WebInspect Enterpriseには4つのモバイルユーザエージェントのオプションがあり、その中から選択することができますが、カスタムオプションを作成することや、別のバージョンのAndroid、Windows Phone、または他のモバイルデバイス用のユーザエージェントを作成することができます。ユーザエージェントヘッダの作成については、"カスタムユーザエージェントヘッダの作成" 次のページを参照してください。

推奨

OpenTextでは、スキャンを一度に1回だけ実行することをお勧めします。SQL Expressを使用する場合は特に、サイトのサイズによっては、同時(または並行)スキャンを実行すると、OpenText DASTホスト上のRAM、CPU、およびディスクリソースの使用率が高くなる場合があります。

モバイルスキャンの起動

モバイルスキャンを起動するには:

1. ガイド付きスキャンを開始します。
   a. OpenText DASTの場合は、OpenText DASTの[開始ページ(Start page)]で、**[ガイド付きスキャンの開始(Start a Guided Scan)]**をクリックします。
   b. Fortify WebInspect Enterpriseの場合は、Webコンソールの[アクション(Actions)]で**[ガイド付きスキャン(Guided Scan)]**をクリックします。
2. [モバイルテンプレート(Mobile Templates)]セクションで**[モバイルスキャン(Mobile Scan)]**を選択します。
3. ツールバーの**[モバイルクライアント(Mobile Client)]**アイコンをクリックします。
4. 使用する**レンダリングエンジン**を選択します。選択するレンダリングエンジンによって、ガイド付きスキャンの設定時に新しいマクロの記録または既存のマクロの編集を行うときに開かれるWeb Macro Recorderが決まります。レンダリングエンジンのオプションは次のとおりです。
   - **セッションベース(Session-based)** -このオプションを選択すると、セッションベースのWeb Macro Recorderが指定されます。これはInternet Explorerブラウザテクノロジを使用します。

- **イベントベース(Event-based) (優先)** - このオプションを選択すると、TruClientおよびFirefox技術を使用するイベントベースのWebマクロレコーダが指定されます。

5. レンダリングエンジンからサイトに提供するエージェント文字列を表すユーザエージェントを選択します。独自のユーザ文字列を作成した場合は、[カスタム(Custom)]として表示されます。ユーザエージェントがリストにない場合は、カスタムユーザエージェントを作成できます。「"カスタムユーザエージェントヘッダの作成" 下」を参照してください。

ガイド付きスキャンウィザードで[ネイティブモバイルステージ: Webサイトの検証(Native Mobile Stage: Verify website)]の最初のステップが表示されます。

カスタムユーザエージェントヘッダの作成

OpenText DASTおよびFortify WebInspect Enterpriseには、Android、Windows、およびiOSデバイス用のユーザエージェントが含まれています。いずれかのオプションを使用する場合には、カスタムユーザエージェントヘッダを作成する必要はありません。Webブラウザに別のモバイルデバイスまたは特定のOSバージョンを名乗らせるには、カスタムユーザエージェントヘッダを作成します。

カスタムユーザエージェントを作成するには:

1. ガイド付きスキャンのツールバーで[**詳細(Advanced)**]をアイコンをクリックします。
2. [スキャン設定(Scan Settings)]ウィンドウが表示されます。
3. [スキャン設定(Scan settings)]列で、[**クッキー/ヘッダ(Cookies/Headers)**]を選択します。
4. 設定エリアの[カスタムヘッダの追加(Append Custom Headers)]セクションで、User-Agent文字列をダブルクリックします。

   [カスタムヘッダの指定(Specify Custom Header)]ボックスが表示されます。
5. 「User-Agent:」と入力し、その後に目的のデバイスのユーザエージェントヘッダ文字列を入力します。
6. [**OK**]をクリックします。

   これで、新しいカスタムユーザエージェントをモバイルクライアントとして選択できるようになりました。

Webサイトの確認

Webサイトを確認するには:

1. [**開始URL(Start URL)**]ボックスで、スキャンするサイトの完全なURLまたはIPアドレスを入力または選択します。

   URLを入力する場合は、正確に入力する必要があります。たとえば「MYCOMPANY.COM」と入力すると、OpenText DASTまたはFortify WebInspect EnterpriseはWWW.MYCOMPANY.COMなどのバリエーションはスキャンしません([許可ホスト(Allowed Hosts)]設定で代替URLを指定している場合を除く)。

無効なURLまたはIPアドレスを指定すると、エラーが発生します。階層ツリー内の特定の位置からスキャンを実行する場合は、スキャンの開始点(http://www.myserver.com/myapplication/など)を追加します。

IPアドレスによるスキャンでは、(相対パスではなく)完全修飾URLを使用するリンクを追跡しません。

OpenText DASTおよびFortify WebInspect Enterpriseでは、IPV4 (Internet Protocolバージョン4)とIPV6 (Internet Protocolバージョン6)の両方がサポートされています。IPV6アドレスは括弧で囲む必要があります。

注記: OpenText DASTでは、WebサイトスキャンおよびWebサービススキャンでIPv6 (Internet Protocolバージョン6)アドレスがサポートされています。開始URLを指定する場合は、IPv6アドレスを括弧で囲む必要があります。例:

- http://[::1]
  OpenText DASTは「localhost」をスキャンします。
- http://[fe80::20c:29ff:fe32:bae1]/subfolder/
  OpenText DASTは、指定されたアドレスのホストのスキャンを「subfolder」ディレクトリから開始します。
- http://[fe80::20c:29ff:fe32:bae1]:8080/subfolder/
  OpenText DASTは、ポート8080で実行されているサーバのスキャンを「subfolder」から開始します。

2. (オプション)スキャン範囲を特定のエリアに限定するには、**[フォルダに限定(Restrict to Folder)]**チェックボックスをオンにし、リストから次のいずれかのオプションを選択します。
   - **[ディレクトリのみ(自己) (Directory only (self))]**。OpenText DASTおよびFortify WebInspect Enterpriseは、指定されたURLのみをWeb探索または監査(またはその両方)します。たとえば、このオプションを選択してwww.mycompany/one/two/というURLを指定すると、OpenText DASTまたはFortify WebInspect Enterpriseは「two」ディレクトリのみを評価します。
   - **[ディレクトリおよびサブディレクトリ(Directory and subdirectories)]**。OpenText DASTおよびFortify WebInspect Enterpriseは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも上位のディレクトリにはアクセスしません。
   - **[ディレクトリおよび親ディレクトリ(Directory and parent directories)]**。OpenText DASTおよびFortify WebInspect Enterpriseは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも下位のディレクトリにはアクセスしません。

   [フォルダに限定(Restrict to folder)]スキャンオプションの制限については、"「フォルダに限定」に関する制限" ページ227を参照してください。
3. **[検証(Verify)]**をクリックします。

Webサイトが、共通アクセスカード(CAC)またはパスワードで保護されている証明書を使用してクライアント証明書で認証するように設定されている場合、ガイド付きスキャンでは次のメッセージが表示されます。

サイト *<URL>*がクライアント証明書を要求しています。今すぐ設定しますか? (The site <URL> is requesting a client certificate. Would you like to configure one now?)

CACを使用するクライアント証明書またはパスワードで保護されている証明書を設定するには:

a. [**Yes**]をクリックします。

[クライアント証明書の選択(Select a Client Certificate)]ウィンドウが表示されます。

b. [証明書ストア(Certificate Store)]で、 **現在のユーザ(Current User)**]を選択します。

使用可能な証明書のリストが [証明書(Certificate)]エリアに表示されます。

c. 「(Protected)」というプレフィクスが付いた証明書を見つけて選択します。

選択した証明書に関する情報と [パスワード/PIN (Password/PIN)]フィールドが [証明書情報(Certificate Information)]エリアに表示されます。

d. パスワードまたはPINが必要な場合は、 **[パスワード/PIN (Password/PIN)]**フィールドに入力します。

> **注記:** パスワードまたはPINが必要であるのに、ここで入力していないと、スキャン中にWindowsの [セキュリティ]ウィンドウのプロンプトが表示されるたびに、パスワードまたはPINを入力することが必要になります。

> 重要! {/b}デフォルトでは、OpenText DASTはOpenSSLを使用します。OpenSSLではなく特定のSSL/TLSプロトコルを使用している場合、スキャン設定のProfiler部分はパスワードで保護されている証明書で動作しない場合があります。

e. [**テスト(Test)**]をクリックします。

4. プロキシサーバ経由でターゲットサイトにアクセスする必要がある場合は、メイン画面の左下にある [**プロキシ(Proxy)**]をクリックして [プロキシ設定(Proxy Settings)]エリアを表示し、 [プロキシ設定(Proxy Settings)]リストからオプションを選択します。

- **直接接続(プロキシ無効)(Direct Connection (proxy disabled))**
- **プロキシ設定の自動検出(Auto detect proxy settings)**: WPAD (Web Proxy Autodiscovery Protocol)を使用してプロキシ自動設定ファイルを見つけ、このファイルを使用してブラウザのWebプロキシ設定を行います。
- **システムのプロキシ設定を使用する(Use System proxy settings)**: ローカルマシンからプロキシサーバ情報をインポートします。
- **Firefoxプロキシ設定を使用する(Use Firefox proxy settings)**: Firefoxからプロキシサーバ情報をインポートします。
- **PACファイルを使用してプロキシ設定を行う(Configure proxy settings using a PAC File)**: PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。

このオプションを選択した場合は、[編集(Edit)]をクリックしてPACの場所(URL)を入力します。

- **プロキシを明示的に設定する(Explicitly configure proxy settings)**: 指示に従ってプロキシサーバ設定を指定します。このオプションを選択した場合は、表示されるフィールドにプロキシ情報を入力します。

重要! {/b}Socks4プロキシサーバは認証に対応しません。認証が必要なSocksプロキシサーバを使用する場合は、Socks5プロキシを使用する必要があります。

注記: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が[プロキシーを使用しない]に設定されている場合、またはWindowsの[LANにプロキシサーバを使用する]設定が選択されていない場合、プロキシサーバは使用されません。

Webサイトまたはディレクトリ構造のスクリーンショットが表示されたら、開始URLへの接続の検証が正常に完了しています。

5. [次へ(Next)]をクリックします。
[スキャンタイプの選択(Choose Scan Type)]ウィンドウが表示されます。

スキャンタイプの選択

1. [スキャン名(Scan Name)]ボックスにスキャンの名前を入力します。
2. 次のいずれかのスキャンタイプを選択します。
   - **標準(Standard)**: OpenText DASTおよびFortify WebInspect Enterpriseは自動分析を実行し、ターゲットURLから開始します。これは標準的なスキャン開始方法です。
   - **ワークフロー(Workflows)**: このオプションを選択すると、ガイド付きスキャンにワークフローステージが追加されます。
3. [スキャン方法(Scan Method)]エリアで、次のいずれかのスキャン方法を選択します。
   - **Web探索のみ(Crawl Only)**: このオプションを選択すると、サイトの階層データ構造が完全にマッピングされます。Web探索が完了したら、[監査(Audit)]をクリックしてアプリケーションの脆弱性を評価できます。
   - **Web探索および監査(Crawl and Audit)**: OpenText DASTおよびFortify WebInspect Enterpriseは、サイトの階層データ構造をマッピングし、各リソース(ページ)を監査します。選択したデフォルト設定に応じて、各リソースの検出時またはサイト全体のWeb探索後に監査を実行できます。Web探索および監査の同時実行と順次実行の詳細については、「"Web探索および監査モード(Crawl and audit mode)" ページ403」を参照してください。
   - **監査のみ(Audit Only)**: OpenText DASTおよびFortify WebInspect Enterpriseは、選択されたポリシーの手法を適用して脆弱性リスクを判断しますが、WebサイトのWeb探索は行いません。サイト上のリンクをたどることも評価することもありません。
4. [ポリシー(Policy)]エリアの[ポリシー(Policy)]リストからポリシーを選択します。ポリシーの管理の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイ*

ド』の「Policy Manager」の章を参照してください。

5. [Web探索のカバレッジ(Crawl Coverage)]エリアで、**[Web探索のカバレッジ(Crawl Coverage)]**スライダを使用してカバレッジのレベルを選択します。Web探索のカバレッジレベルの詳細については、"Web検索範囲と徹底性の設定" ページ208を参照してください。
6. **[シングルページアプリケーション(Single-Page Applications)]**エリアで、SPA (single-page application)のWeb探索および監査のオプションを選択します。有効にすると、DOMスクリプトエンジンは、Web探索中に、JavaScriptインクルード、フレームとiframeのインクルード、CSSファイルインクルード、およびAJAX呼び出しを検索してから、それらのイベントによって生成されたすべてのトラフィックを監査します。 **[シングルページアプリケーション(Single-Page Applications)]**のオプションは次のとおりです。
   - **自動(Automatic)** - OpenText DASTがSPAフレームワークを検出すると、自動的にSPAサポートモードに切り替わります。
   - **有効(Enabled)** - SPAフレームワークがターゲットアプリケーションで使用されていることを示します。

     注意! {/b}SPAサポートは、シングルページアプリケーションに対してのみ有効にするべきです。SPAサポートを有効にしてSPA以外のWebサイトをスキャンすると、スキャンが遅くなります。
   - **無効(Disabled)** - SPAフレームワークがターゲットアプリケーションで使用されていないことを示します。

   詳細については、「"シングルページアプリケーションスキャンについて" ページ235」を参照してください。
7. **[次へ(Next)]**ボタンをクリックします。

   ログインステージが表示され、左側のペインでネットワーク認証が強調表示されます。

ネットワーク認証の設定

ネットワークでユーザ認証が必要な場合は、ここで設定できます。ネットワークでユーザ認証が不要な場合は、 **[次へ(Next)]**ナビゲーションボタン、またはガイド付きスキャンツリーの次の該当ステップをクリックして続行します。

ネットワーク認証を設定するには:

1. **[ネットワーク認証(Network Authentication)]**チェックボックスをクリックします。
2. 認証メソッドのドロップダウンリストから、**メソッド**を選択します。認証メソッドは次のとおりです。
   - **ADFS CBT**
   - **自動**
   - **基本**
   - **ダイジェスト**

- **Kerberos**
- **ネゴシエート(Negotiate)**
- **NT LAN Manager (NTLM)**
- **OAuth 2.0 Bearer**

3. 次のいずれかを実行します。
   - OAuth 2.0 Bearer以外のすべての認証方法では、 **[ユーザ名(User name)]**ボックスにユーザIDを入力し、 **[パスワード(Password)]**ボックスにユーザのパスワードを入力します。
   - OAuth 2.0 Bearerメソッドの場合は、 **[設定(Configure)]**をクリックし、"OAuth 2.0のBearer資格情報の設定" ページ447の手順に従います。

クライアント証明書の使用

ネットワーク認証にクライアント証明書を使用するには:

1. ネットワーク認証にクライアント証明書を使用するには、 **[クライアント証明書(Client Certificate)]**を選択します。

   注記: クライアント証明書をWindowsフォンに追加できますが、後でその証明書を削除するには、Windowsフォンをデフォルト設定に戻すしかありません。

2. **[証明書ストア(Certificate Store)]**エリアで、次のいずれかを選択してから、 **[マイ(My)]**または **[ルート(Root)]**ラジオボタンを選択します。
   - **[ローカルマシン(Local Machine)]**。OpenText DASTは、 **[証明書ストア(Certificate Store)]**エリアで選択した内容に基づいて、ローカルマシン上の証明書を使用します。
   - **[現在のユーザ(Current User)]**。OpenText DASTは、 **[証明書ストア(Certificate Store)]**エリアで選択した内容に基づいて、現在のユーザの証明書を使用します。
3. **[証明書情報(Certificate Information)]**エリアに証明書の詳細を表示するには、証明書を選択します。
4. **[次へ(Next)]**ボタンをクリックします。
   [アプリケーション認証(Application Authentication)]ページが表示されます。

アプリケーション認証の設定

サイトで認証が必要な場合は、このステップを使用してログインマクロを作成、選択、または編集することにより、ログインプロセスを自動化してサイトのカバレッジを拡大できます。ログインマクロは、アプリケーションにアクセスしてログインするために必要なアクティビティの記録です。通常は、ユーザ名とパスワードを入力し、 **[ログイン]**や **[ログオン]**などのボタンをクリックします。

ログインマクロを使用するスキャンの **[スキャン設定: 認証(Scan Settings: Authentication)]**で **[マクロ検証を有効にする(Enable macro validation)]**が選択されている場合、OpenText

DASTはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

注記: マクロテストは、2要素認証を含むマクロに対してはサポートされていません。

重要! {/b}2要素認証を含むマクロを使用する場合は、スキャンを開始する前に、2要素認証アプリケーションの設定を行う必要があります。詳細については、「"アプリケーション設定: 2要素認証" ページ491」を参照してください。

ログインマクロでは、次のオプションを使用できます。

- "権限のエスカレーションなしでログインマクロを使用する" 下
- "権限のエスカレーションのためにログインマクロを使用する" 次のページ
- "Fortify WebInspect Enterpriseに接続しているときにログインマクロを使用する" ページ139

マスクされた値のサポート

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、OpenText DASTでガイド付きスキャンを設定するときにも、それらの値はマスクされます。

権限のエスカレーションなしでログインマクロを使用する

ログインマクロを使用するには:

1. [**このサイトでログインマクロを使用する(Use a login macro for this site)**]チェックボックスをオンにします。
2. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
   - [ログインマクロ(Login Macro)]フィールドに表示されている既存のログインマクロを編集するには、 [**編集(Edit)**]をクリックします。
   - 新しいマクロを記録するには、 [**作成(Create)**]をクリックします。

   新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。
3. [**次へ(Next)**]ボタンをクリックします。

   標準スキャンを選択した場合は、 [最適化タスク(Optimization Tasks)]ページが表示されます。ワークフロースキャンを選択した場合は、 [ワークフローの管理(Manage Workflows)]ページが表示されます。

権限のエスカレーションのためにログインマクロを使用する

権限のエスカレーションポリシーか、有効な権限のエスカレーションチェックを含む別のポリシーを選択した場合、高い権限を持つユーザアカウント用のログインマクロが少なくとも1つ必要です。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。

ログインマクロを使用するには:

1. **[高い権限のユーザアカウントログインマクロ(High-Privilege User Account Login Macro)]** チェックボックスをオンにします。このログインマクロは、サイト管理者やモデレータアカウントなど、より高い権限を持つユーザアカウント用です。
2. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン([..])をクリックして、保存されているマクロを参照します。
   - **[ログインマクロ(Login Macro)]** フィールドに表示されている既存のログインマクロを編集するには、 **[編集(Edit)]** をクリックします。
   - 新しいマクロを記録するには、 **[作成(Create)]** をクリックします。

   新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。

   最初のマクロを記録または選択して **[次へ(Next)]** の矢印をクリックすると、 **[低い権限のログインマクロを設定する(Configure Low Privilege Login Macro)]** プロンプトが表示されます。
3. 次のいずれかを実行します。
   - 認証モードでスキャンを実行するには、 **[はい(Yes)]** をクリックします。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。

     ガイド付きスキャンが **[ログインマクロの選択(Select Login Macro)]** ウィンドウに戻り、低い権限のログインマクロを作成または選択できるようになります。ステップ4に進みます。
   - スキャンを非認証モードで実行するには、 **[いいえ(No)]** をクリックします。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。

     アプリケーション認証のステップが完了しました。標準スキャンを選択した場合は、 **[最適化タスク(Optimization Tasks)]** ページが表示されます。ワークフロースキャンを選択した場合は、 **[ワークフローの管理(Manage Workflows)]** ページが表示されます。
4. **[低い権限のユーザアカウントログインマクロ(Low-Privilege User Account Login Macro)]** チェックボックスをオンにします。このログインマクロは、サイトコンテンツのビューアやコンシューマなど、低い権限のユーザアカウント用です。
5. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン([..])をクリックして、保存されているマクロを参照します。

- [ログインマクロ(Login Macro)]フィールドに表示されている既存のログインマクロを編集するには、 **[編集(Edit)]**をクリックします。
- 新しいマクロを記録するには、 **[作成(Create)]**をクリックします。

新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。

6. 2つ目のマクロを記録または選択した後、 **[次へ(Next)]**ボタンをクリックします。

標準スキャンを選択した場合は、 [最適化タスク(Optimization Tasks)]ページが表示されます。ワークフロースキャンを選択した場合は、 [ワークフローの管理(Manage Workflows)]ページが表示されます。

Fortify WebInspect Enterpriseに接続しているときにログインマクロを使用する

Fortify WebInspect Enterpriseに接続されているOpenText DASTの場合は、Fortify WebInspect Enterpriseマクロリポジトリからログインマクロをダウンロードして使用できます。

マクロをダウンロードするには:

1. **[このサイトでログインマクロを使用する(Use a login macro for this site)]**チェックボックスをオンにします。
2. **[ダウンロード(Download)]**をクリックします。

[Fortify WebInspect Enterpriseからマクロをダウンロードする(Download a Macro from Fortify WebInspect Enterprise)]ウィンドウが表示されます。

3. ドロップダウンリストから **[アプリケーション(Application)]**と **[バージョン(Version)]**を選択します。
4. **[マクロ(Macro)]**ドロップダウンリストからリポジトリマクロを選択します。
5. **[OK]**をクリックします。

注記: リポジトリマクロを選択すると、 [最終確認(Final Review)]ページの **[自動でスキャンをWIEにアップロードする(Automatically Upload Scan to WIE)]**の **[アプリケーション(Application)]**と **[バージョン(Version)]**が自動的に同期されます。

ログインマクロを自動的に作成する

ユーザ名とパスワードを入力して、OpenText DASTでログインマクロを自動的に作成できます。

注記: 権限のエスカレーションおよびマルチユーザログインスキャンに対して、また、セッションベースのレンダリングエンジンを使用するスキャンに対して自動でログインマクロを作成することはできません。

ログインマクロを自動的に作成するには:

1. [**ログインマクロの自動生成(Auto-gen Login Macro)**]を選択します。
2. [**ユーザ名(Username)**]フィールドにユーザ名を入力します。
3. [**パスワード(Password)**]フィールドにパスワードを入力します。

オプションで、[**テスト(Test)**]をクリックして、ログインフォームの検索、マクロの生成、マクロ検証テストの実行を行ってから、ガイド付きスキャンウィザードの次のステージに進みます。完了前に検証テストをキャンセルする必要がある場合は、[**キャンセル(Cancel)**]をクリックします。

マクロが無効で、アプリケーションへのログインが失敗すると、エラーメッセージが表示されます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

ワークフローステージについて

ワークフローステージは、サイトステージで[**スキャンタイプ(Scan Type)**]として[**ワークフロー(Workflows)**]を選択した場合にのみ表示されます。[**標準(Standard)**]を選択した場合、ワークフローステージは表示されません。

ワークフローマクロを作成すると、マクロで指定したページをOpenText DASTで確実に監査できます。OpenText DASTはマクロに含まれているURLのみを監査し、監査中に検出されたハイパーリンクはたどりません。

複数のワークフローマクロを、サイト上のユースケースごとに1つずつ作成できます。ログアウト署名は不要です。この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。複数のマクロを選択すると、すべてのマクロが同一スキャンに含まれます。複数のマクロを選択できることに加えて、Burp Proxyキャプチャと`.har`ファイルをインポートしてスキャンに追加することもできます。

> 重要! {/b}ログインマクロをワークフローマクロと起動マクロのどちらかまたはその両方と組み合わせて使用する場合は、すべてのマクロが同じタイプでなければなりません。すべてが`.webmacro`ファイル、すべてがBurp Proxyキャプチャ、またはすべてが`.har`ファイルのいずれかです。同じスキャンで異なる種類のマクロを使用することはできません。

ワークフローの設定を完了するには、[**ワークフロー(Workflow)**]テーブルで次のいずれかをクリックします。

- [**記録(Record)**]。Web Macro Recorderが開き、マクロを作成できます。
- [**編集(Edit)**]。Web Macro Recorderが開き、選択したマクロがロードされます。
- [**削除(Delete)**]。選択したマクロが削除されます(ただしディスクからは削除されません)。
- [**インポート(Import)**]。標準のファイル選択ウィンドウが開き、過去に記録された`.webmacro`ファイル、Burp Proxyキャプチャ、または`.har`ファイルを選択できます。

  > **注記:** コンピュータにOpenText UFT One (Unified Functional Testing)がインストールされている場合は、OpenText DASTがこれを自動的に検出し、UFT `.usr`ファイルをインポートするためのオプションを表示します。

詳細については、「"ガイド付きスキャンでの機能テストファイルのインポート" ページ162」を参照してください。

- 記録したマクロを**エクスポート**します。マクロを選択または記録した後で、許可ホストを必要に応じて指定できます。標準のファイル選択ウィンドウが開き、記録したマクロを保存できます。

ワークフローマクロを指定して再生すると、[ワークフロー(Workflows)]テーブルにそのマクロが表示され、許可ホストが**[ガイド付きスキャン(Guided Scan)] > [ワークフロー(Workflows)] > [ワークフロー(Workflows)] > [マネージャワークフロー(Manager Workflow)]**ページに追加されます。特定のホストへのアクセスを有効または無効にできます。詳細については、「"スキャン設定:許可ホスト" ページ421」を参照してください。

Burp Proxy結果の追加

Burp Proxyセキュリティテストを実行した場合、テスト中に収集されたトラフィックをワークフローマクロにインポートできます。これにより、同じエリアの再スキャンにかかる時間が短縮されます。

ワークフローマクロにBurp Proxy結果を追加するには:

1. [ワークフロー(Workflows)]画面が表示されていない場合は、[ガイド付きスキャン(Guided Scan)]ツリーの**[ワークフローの管理(Manage Workflows)]**ステップをクリックします。
2. **[インポート(Import)]**ボタンをクリックします。
   [マクロのインポート(Import Macro)]ファイルセレクタが表示されます。
3. ファイルの種類ボックスのフィルタを**[Webマクロ(*.webmacro)(Web Macro (*.webmacro))]**から**[Burp Proxy (*.*)]**に変更します。
4. Burp Proxyファイルに移動し、目的のファイルを選択します。
5. **[開く(Open)]**をクリックします。

Profilerの使用

OpenText DAST Profilerは、ターゲットWebサイトの事前テストを実行し、特定の設定を変更すべきかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Profilerは、サイトに入るために権限付与が必要であるものの、有効なユーザ名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Profilerの提案に従って、続行する前に必要な情報を設定することができます。

同様に、設定では、OpenText DASTが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが

含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにOpenText DAST設定を変更することを推奨します。

Profilerを起動するには:

1. [**プロファイル(Profile)**]をクリックします。
   Profilerが実行されます。詳細については、「"Server Profiler" ページ283」を参照してください。
   結果は、[**設定(Settings)**]セクションの[**スキャンの最適化(Optimize scan for)**]ボックスに表示されます。
2. 必要に応じて、要求された情報を入力します。
3. [**次へ(Next)**]ボタンをクリックします。

Profilerを実行していない場合でも、いくつかのオプションが表示されることがあります。これについては、以降のセクションで説明します。

Webフォームの自動入力(Autofill web forms)

OpenText DASTがターゲットサイトのスキャン中に検出されるフォームの入力コントロールの値を送信するようにするには、[**Web探索時のWebフォームの自動入力(Auto-fill Web forms during crawl)**]を選択します。OpenText DASTは、事前パッケージ化されたデフォルトファイル、またはWeb Form Editorを使用して作成したファイルから値を抽出します。『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Web Form Editor」に関する章を参照してください。以下を実行できます。

1. ブラウザボタンをクリックして、ファイルを見つけてロードします。
2. [**編集(Edit)**]をクリックして、選択したファイル(またはデフォルト値)をWeb Form Editorで編集します。
3. [**作成(Create)**]をクリックしてWeb Form Editorを開き、ファイルを作成します。

許可ホストを追加する

[**許可ホスト(Allowed Host)**]設定は、Web探索して監査するドメインを追加する場合に使用します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここに追加します。詳細については、「"スキャン設定:許可ホスト" ページ421」を参照してください。

許可するドメインを追加するには:

1. [**追加(Add)**]をクリックします。
2. [**許可ホストの指定(Specify Allowed Host)**]ウィンドウで、URL(またはURLを表す正規表現)を入力し、[**OK**]をクリックします。

識別された抑制された検出事項を再利用する

以前のスキャンで誤検出に変更された、または無視された脆弱性をインポートできます。これらの誤検出または無視された項目が現在のスキャンで検出された脆弱性と一致する場合、その脆弱性は誤検出に変更されるか、無視されます。既存のスキャンまたは抑制された検出事項ファイルから、抑制された検出事項をインポートできます。詳細については、「"抑制された検出事項" ページ83」を参照してください。

識別された抑制された検出事項を再利用するには:

1. [**抑制された検出事項のインポート(Import Suppressed Findings)**]を選択します。
2. 次の表に従って続行します。

使用する情報...	その場合...
既存のスキャン	a. [**抑制された検出事項をスキャンからインポートするには、ここをクリックします(Click here to import suppressed findings from scans)**]をクリックします。 [スキャンを選択して、抑制された検出事項をインポートする(Select a Scan to Import Suppressed Findings)]ダイアログが開きます。 b. 現在スキャンしている同じサイトからの、抑制された検出事項を含むスキャンを1つ以上選択します。 c. [OK]をクリックします。
抑制された検出事項ファイル	a. [**抑制された検出事項をファイルからインポートするには、ここをクリックします(Click here to import suppressed findings from a file)**]をクリックします。 標準のWindowsファイル選択ダイアログボックスが開きます。 b. インポートするファイルを選択し、[**開く(Open)**]をクリックします。 c. 必要に応じて、ステップaとbを繰り返して追加のファイルを選択します。

サンプルマクロの適用

OpenTextのサンプルバンキングアプリケーション(zero.webappsecurity.com)では、Webフォームログインが使用されています。このサイトをスキャンする場合は、[**サンプルマクロの適用(Apply sample macro)**]を選択して、ログインスクリプトを含む事前パッケージ化されたマクロを実行します。

トラフィック分析

Web Proxyツールを使用してOpenText DASTにより発行されたHTTP要求とターゲットサーバから返された応答を検査するには、[**Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)**]を選択します。

OpenText DASTはWebサイトのスキャン中に、Webサイトの階層構造を明らかにするセッションと、脆弱性が検出されたセッションのみをナビゲーションペインに表示します。ただし[**Traffic Monitorを有効にする(Enable Traffic Monitor)**]を選択すると、OpenText DASTでは[Traffic Monitor]ボタンが[スキャン情報(Scan Info)]パネルに追加されます。これにより、OpenText DASTが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。

メッセージ

Profilerが変更を推奨しない場合は、ガイド付きスキャンウィザードに「設定の変更は推奨されません。現在のスキャン設定はこのサイトに最適です。(No settings changes are recommended. Your current scan settings are optimal for this site.)」というメッセージが表示されます。

[**次へ(Next)**]をクリックします。

[最終確認(Final Review)]ページが表示され、左側のペインで [**詳細オプションの設定(Configure Detailed Options)**]が強調表示されます。

追加オプションの設定

詳細オプションを設定するには、次の設定を指定します。

識別された誤検出を再利用する(Reuse Identified False Positives)

OpenText DASTによってすでに識別されている誤検出を再利用するには、 [**誤検出(False Positives)**]ボックスをオンにします。

トラフィック分析

1. Web Proxyツールを使用するには、 [Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)]を選択して、OpenText DASTが発行したHTTP要求と、ターゲットサーバから返された応答を調べます。

   Web Proxyはスタンドアロンの自己完結型プロキシサーバであり、デスクトップ上で設定および実行できます。Web Proxyを使用すると、スキャナ、Webブラウザ、またはHTTP要求を送信してサーバから応答を受信するその他のツールからのトラフィックを監視できます。Web Proxyは、デバッグと侵入スキャンのためのツールです。サイトのブラウズ中に、すべての要求とサーバの応答を確認できます。
2. OpenText DASTによって送信された各HTTP要求と、サーバから受信した関連HTTP応答を表示および確認するには、 [**Traffic Monitor**]ボックスを選択します。

   OpenText DASTはWebサイトのスキャン中に、Webサイトの階層構造を明らかにしたセッションと、脆弱性が検出されたセッションのみを表示します。ただし [**Traffic Monitorを有効にする(Enable Traffic Monitor)**]を選択すると、OpenText DASTではOpenText DASTが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。
3. [**次へ(Next)**]をクリックします。

   [設定の検証とスキャンの開始(Validate Settings and Start Scan)]ページが表示され、左側のペインで [**詳細オプションの設定(Configure Detailed Options)**]が強調表示されます。

設定の検証とスキャンの開始

このページのオプションを使用すると、現在のスキャン設定を保存することができます。また、OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、Fortify WebInspect Enterpriseとやり取りすることができます。

1. スキャン設定をXMLファイルとして保存するには、 **[ここをクリックして設定を保存する(Click here to save settings)]**を選択します。標準の **[名前を付けて保存(Save as)]** ウィンドウを使用して、ファイルに名前を付けて保存します。
2. OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、ツールバーに **[テンプレート(Templates)]** セクションが表示されます。次の表に従って続行します。

目的の作業	その場合の手順
現在のスキャン設定をテンプレートとしてFortify WebInspect Enterpriseデータベースに保存する **注記:** 既存のテンプレートを編集する場合、 **[保存(Save)]** を実行すると、実際には更新が行われます。設定の編集を保存したり、テンプレート名を変更したりすることができます。ただし、アプリケーション、バージョン、またはグローバルテンプレートの設定は変更できません。	a. 次のいずれかを実行します。 ◦ ツールバーの **[テンプレート(Templates)]** セクションで **[保存(Save)]** をクリックします。 ◦ **[ここをクリックしてテンプレートを保存する(Click here to save template)]** を選択します。 **[テンプレートの保存(Save Template)]** ウィンドウが表示されます。 b. **[アプリケーション(Application)]** ドロップダウンリストからアプリケーションを選択します。 c. **[バージョン(Version)]** ドロップダウンリストからアプリケーションバージョンを選択します。 d. **[テンプレート(Template)]** フィールドに名前を入力します。
テンプレートからスキャン設定をロードする	a. ツールバーの **[テンプレート(Templates)]** セクションで **[ロード(Load)]** をクリックします。 現在のスキャン設定が失われるという確認メッセージが表示されます。 b. **[Yes]** をクリックします。 **[テンプレートのロード(Load Template)]** ウィンドウが表示されます。 c. **[アプリケーション(Application)]** ドロップダウンリストからアプリケーションを選択します。

目的の作業	その場合の手順
	d. [バージョン(Version)]ドロップダウンリストからアプリケーションバージョンを選択します。 e. [テンプレート(Template)]ドロップダウンリストからテンプレートを選択します。 f. [ロード(Load)]をクリックします。 ガイド付きスキャンがサイトステージに戻り、Webサイトの検証と、テンプレートからのステップごとの設定の実行が行えるようになります。

3. OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、このページに [Fortify WebInspect Enterprise]セクションが表示されます。Fortify WebInspect Enterpriseを操作するには、次のようにします。
   a. [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。
   b. [バージョン(Version)]ドロップダウンリストからアプリケーションバージョンを選択します。
   c. 次の表に従って続行します。

スキャンの実行方法	その場合の手順
Fortify WebInspect Enterpriseでセンサを使用する	i. [WebInspect Enterpriseで実行(Run in WebInspect Enterprise)]を選択します。 ii. [センサ(Sensor)]ドロップダウンリストからセンサを選択します。 iii. スキャンの [優先度(Priority)]を選択します。
OpenText DASTを使用する	i. [DASTで実行(Run in DAST)]を選択します。 ii. スキャン結果をFortify WebInspect Enterpriseの指定したアプリケーションおよびバージョンに自動的にアップロードする場合は、 [WebInspect Enterpriseへの自動アップロード(Auto Upload to WebInspect Enterprise)]を選択します。 **注記:** スキャンが正常に完了しない場

スキャンの実行方法	その場合の手順
	合、Fortify WebInspect Enterpriseにはアップロードされません。

4. [今すぐスキャン(Scan Now)]エリアでスキャン設定を見直し、[スキャンの開始(Start Scan)]をクリックしてスキャンを開始します。

参照情報

"ガイド付きスキャンの概要" ページ111

ネイティブスキャンテンプレートの使用

OpenText DASTおよびFortify WebInspect Enterpriseを使用すると、AndroidまたはiOSのアプリまたはサービスで生成されたバックエンドトラフィックをスキャンできます。トラフィックは、Android、Windows、またはiOSデバイス上でアプリケーションを実行するか、Androidまたは iOSエミュレータを介してソフトウェアを実行することで生成できます。

ガイド付きスキャンウィザードでは、アプリケーションのバックエンドトラフィックのスキャンに必要なステージとステップを順に実行します。前のステップまたはステージに戻る必要がある場合は、[戻る]ナビゲーションボタンをクリックするか、ガイド付きスキャンツリー内のステップをクリックして、そこに直接移動します。

推奨

OpenTextでは、スキャンを一度に1回だけ実行することをお勧めします。SQL Expressを使用する場合は特に、サイトのサイズによっては、同時(または並行)スキャンを実行すると、OpenText DASTホスト上のRAM、CPU、およびディスクリソースの使用率が高くなる場合があります。

モバイルデバイスのセットアップ

ネイティブスキャンの実行では、セキュリティ保護されたプロキシと連動するようにモバイルデバイスを設定する必要があります。この設定を行うには、以下の手順を実行する必要があります。

- モバイルデバイス/エミュレータプロキシを設定する("モバイルデバイスのプロキシアドレスの設定" ページ150を参照してください)
- 信頼された証明書をインストールする("信頼された証明書の追加" ページ151を参照してください)

ガイド付きスキャンのステージについて

ネイティブのモバイルテンプレートを使用したガイド付きスキャンは、4つのステージで構成され、各ステージには1つ以上のステップが含まれています。これらのステージは次のとおりです。

ネイティブモバイル: デバイスまたはエミュレータを選択し、デバイスまたはエミュレータのプロキシを設定し、実行するスキャンのタイプを選択します。

ログイン: モバイルアプリケーションのバックエンドで必要な場合に認証のタイプを定義します。

アプリケーション: アプリを実行し、Webトラフィックを記録し、スキャンに含めるホストとRESTfulエンドポイントを特定します。

設定: 選択内容を確認して検証し、スキャンを実行します。

サポートされるデバイス

OpenText DASTおよびFortify WebInspect Enterpriseは、次の表で説明するように、Android、Windows、およびiOSデバイス上のバックエンドトラフィックのスキャンをサポートしています。

OS	サポートされるデバイス
Android	Androidベースの携帯電話やタブレットなど、あらゆるAndroidデバイス
Windows	WindowsフォンやSurfaceタブレットなど、あらゆるWindowsデバイス
iOS	iPhoneやiPadなど、最新バージョンのiOSを実行しているあらゆるiOSデバイス

サポートされる開発エミュレータ

AndroidおよびiOSデバイスのサポートに加えて、お使いの開発環境でAndroidまたはiOSエミュレータを介してアプリケーションを実行できます。デバイスエミュレータを介して生成されたトラフィックをスキャンする場合、開発マシンがOpenText DASTまたはFortify WebInspect Enterpriseと同じネットワーク上に存在し、OpenText DASTまたはFortify WebInspect Enterpriseと開発マシンの間にプロキシが設定されていることを確認する必要があります。

ネイティブスキャンの起動

ネイティブスキャンを起動するには、デバイスまたはエミュレータがOpenText DASTと同じネットワーク上にあることを確認する必要があります。また、プロキシ接続を正常に作成するために、OpenText DASTを実行しているマシン上のポートに対する権限とアクセスが必要になります。

ネイティブスキャンを起動するには:

1. OpenText DASTまたはFortify WebInspect Enterpriseを開きます。
2. ガイド付きスキャンを開始します。
   - OpenText DASTの場合は、OpenText DASTの [開始ページ(Start page)] で、 **[ガイド付きスキャンの開始(Start a Guided Scan)]** をクリックします。
   - Fortify WebInspect Enterpriseの場合は、Webコンソールの [アクション(Actions)] で **[ガイド付きスキャン(Guided Scan)]** をクリックします。
3. [モバイルテンプレート(Mobile Templates)] セクションで **[ネイティブスキャン(Native Scan)]** を選択します。
   ガイド付きスキャンウィザードに、ネイティブモバイルステージの最初のステップである [デバイス/エミュレータの選択(Choose Device/Emulator)] が表示されます。

デバイス/エミュレータタイプの選択

ガイド付きスキャンを起動すると、次の表で説明するオプションが表示されます。

オプション	説明
プロファイル(Profile)	スキャンするデバイスまたはエミュレータのタイプ。ドロップダウンメニューからタイプを選択します。詳細については、「"プロファイルの選択" 下」を参照してください。
モバイルデバイス/エミュレータプロキシ(Mobile Device/Emulator Proxy)	デバイスまたはエミュレータとテスト対象のWebサービスまたはアプリケーション間のトラフィックをリスンするために、OpenText DASTまたはFortify WebInspect Enterpriseが作成するプロキシのIPアドレスとポート番号。IPアドレスまたはポート(あるいはその両方)が他のアクティビティ用に予約されていない限り、デフォルト設定を使用します。詳細については、「"モバイルデバイスのプロキシアドレスの設定" 次のページ」を参照してください。
信頼された証明書(Trusted Certificate)	デバイスまたはエミュレータのクライアント証明書を取得するためのポートとURL。デバイスまたはエミュレータに証明書をダウンロードしてインストールするには、"信頼された証明書の追加" ページ151を参照してください。

プロファイルの選択

デバイスプロファイルを設定するには、 **[プロファイル]** ドロップダウンテキストボックスから次のいずれかを選択します。

- iOSデバイス(iOS Device) -最新バージョンのiOSを実行しているiPadまたはiPhone。
- iOSシミュレータ(iOS Simulator) - iOS SDKの一部であるiOSエミュレータ。

- Androidデバイス(Android Device) - Androidオペレーティングシステムを実行している携帯電話またはタブレット。
- Androidエミュレータ(Android Emulator) - Android SDKの一部であるAndroidエミュレータ。
- Windowsデバイス(Windows Device) - WindowsフォンまたはSurfaceタブレット。

モバイルデバイスのプロキシアドレスの設定

[モバイルデバイス/エミュレータプロキシ(Mobile Device/Emulator Proxy)]セクションには、デバイスまたはエミュレータとOpenText DASTまたはFortify WebInspect Enterprise間のプロキシ接続を確立するために使用されるホストIPアドレスとポート番号が一覧表示されます。システムでIPアドレスまたはポート番号が使用できない場合を除き、推奨される設定を使用します。

注記: プロキシの設定後にサーバに接続できなかったりインターネットにアクセスできなかったりする場合は、ネイティブモバイルステージで指定されたファイアウォールのポートを開くか変更する必要がある場合があります。それでも機能しない場合は、別のIPアドレスの選択が必要になる可能性があります。OpenText DASTまたはFortify WebInspect Enterpriseインターフェイスに表示されるIPアドレスでは、アドレスをクリックすることで、ドロップダウンリストから代替アドレスを選択できます。

iOSデバイスでプロキシを設定するには:

1. [**設定(Settings)**]アプリケーションを実行します。
2. [**Wi-Fi**]を選択します。
3. OpenText DASTまたはFortify WebInspect Enterpriseへの接続に使用しているWi-Fiネットワークを選択します。
4. [HTTPプロキシ(HTTP Proxy)]セクションまでスクロールダウンして、[**手動(Manual)**]を選択します。

   この画面には、デバイスが接続されているネットワークのネットワーク設定オプションが表示されます。
5. さらに下にスクロールし、OpenText DASTまたはFortify WebInspect Enterpriseによって提供されるサーバのIPアドレスとポート番号を入力します。この情報が表示されない場合は、"デバイス/エミュレータタイプの選択" 前のページを参照してください。
6. OpenText DASTまたはFortify WebInspect Enterpriseで、[信頼された証明書(Trusted Certificate)]セクションの[**検証(Verify)**]ボタンをクリックし、接続が適切に動作していることを確認します。

   [検証(Verify)]アクティビティの進行状況バーが表示されます。
7. デバイスでデフォルトのブラウザを起動して任意のサイトにアクセスし、OpenText DASTまたはFortify WebInspect Enterpriseがバックエンドトラフィックを認識できることを確認します。

   すべてが正しく設定されている場合、しばらくすると、[検証(Verify)]アクティビティの進行状況バーにトラフィックが正常に検証されたことが示されます。
8. [**OK**]をクリックして検証の進行状況バーを閉じ、[**次へ(Next)**]をクリックしてスキャンタイプを選択します。

AndroidまたはWindowsデバイスでプロキシを設定するには、オペレータの指示に従ってください。

信頼された証明書の追加

サイトで安全な接続が必要な場合、スキャンを実行するたびに、OpenText DASTまたはFortify WebInspect Enterpriseはお使いのデバイスまたはエミュレータ用に固有のクライアント証明書を生成します。デバイス(またはエミュレータ)の証明書リポジトリに証明書をインストールする必要があります。

注記: クライアント証明書をWindowsフォンに追加できますが、後でその証明書を削除するには、Windowsフォンをデフォルト設定に戻すしかありません。

証明書を追加するには、次の3つの方法があります。

- ガイド付きスキャンの [信頼された証明書(Trusted Certificate)] セクションからQRコードをスキャンします(QRリーダソフトウェアが必要になります)。
- デバイスまたはデバイスエミュレータの組み込みブラウザにアドレスを入力します。
- 後で適用するために証明書をシステムクリップボードにコピーします(デバイスエミュレータでスキャンする場合に使用されます)。

ニーズに最適なオプションを選択します。

注記: スキャンの完了後、デバイスのリポジトリから証明書を削除する必要があります。「"スキャン後のステップ" ページ161」を参照してください。

iOSデバイスまたはエミュレータに証明書を追加するには:

1. QRコードをスキャンするか、提供されたURLをブラウザに入力すると、 [プロファイルのインストール(Install Profile)] ページが表示されます。

   注記: OpenText DASTルートの証明書のステータスは、これをルートチェーンに追加するまで、「信頼されていない(Not Trusted)」と表示されます。

2. [**インストール(Install)**] ボタンをタップします。
   証明書が信頼されていないことを示す警告画面が表示されます。デバイスまたはエミュレータの証明書リポジトリに証明書を追加すると、警告は表示されなくなります。
3. 警告(Warning)] 画面で [**インストール(Install)**] をタップします。
   表示が変更され、デバイスまたはエミュレータが接続されている現在のネットワークが表示されます。OpenText DASTまたはFortify WebInspect Enterpriseと同じネットワークに接続されていることを確認します。

スキャンタイプの選択

ネイティブモバイルステージの最初の部分でOpenText DASTまたはFortify WebInspect Enterpriseで動作するデバイスまたはエミュレータを設定したら、実行するスキャンのタイプを選択する必要があります。

次の表の説明に従ってオプションを設定します。

オプション	説明
スキャン名(Scan Name)	後で[スキャンの管理(Manage Scans)]ページでスキャンを識別できるように、スキャンの名前を入力します。
スキャン方法(Scan Method)	次のリストから目的のスキャンのタイプを選択します。 • **Web探索のみ(Crawl Only)**: 指定したワークフローの攻撃露呈部分をマッピングします。 • **Web探索および監査(Crawl and Audit)**:指定したワークフローの攻撃露呈部分をマッピングし、脆弱性をスキャンします。 • **監査のみ(Audit Only)**: 指定したワークフローの攻撃のみ行います。
ポリシー	ドロップダウンメニューからスキャンのポリシーを選択します。ポリシーの詳細については、「"OpenText DAST ポリシー" ページ509」を参照してください。ポリシーの作成と編集の詳細については、『OpenText™ Dynamic Application Security Testingツールガイド』の「Policy Manager」の章を参照してください。
Web探索のカバレッジ	[Web探索のカバレッジ(Crawl Coverage)]スライダを使用して、カバレッジのレベルを選択します。

ネットワーク認証の設定

ネットワークでユーザ認証が必要な場合は、ここで設定できます。ネットワークでユーザ認証が不要な場合は、[次へ(Next)]ナビゲーションボタン、またはガイド付きスキャンツリーの次の該当ステップをクリックして続行します。

ネットワーク認証を設定するには:

1. [**ネットワーク認証(Network Authentication)**]チェックボックスをクリックします。
2. 認証メソッドのドロップダウンリストから、**メソッド**を選択します。認証メソッドは次のとおりです。
   - **ADFS CBT**
   - **自動**
   - **基本**
   - **ダイジェスト**
   - **Kerberos**
   - **ネゴシエート(Negotiate)**

- **NT LAN Manager (NTLM)**
- **OAuth 2.0 Bearer**

3. 次のいずれかを実行します。
   - OAuth 2.0 Bearer以外のすべての認証方法では、 **[ユーザ名(User Name)]**ボックスにユーザIDを入力し、 **[パスワード(Password)]**ボックスにユーザのパスワードを入力します。
   - OAuth 2.0 Bearerメソッドの場合は、 **[設定(Configure)]**をクリックし、"OAuth 2.0のBearer資格情報の設定" ページ447の手順に従います。

クライアント証明書の使用

ネットワーク認証にクライアント証明書を使用するには:

1. **[クライアント証明書(Client Certificate)]**チェックボックスを選択します。
2. 次のいずれかを実行します。
   - コンピュータにとってローカルで、コンピュータ上のすべてのユーザにとってグローバルな証明書を使用するには、 **[ローカルマシン(Local Machine)]**を選択します。
   - コンピュータ上のユーザアカウントにとってローカルな証明書を使用するには、 **[現在のユーザ(Current User)]**を選択します。

   注記: 共通アクセスカード(CAC)リーダで使用される証明書はユーザ証明書であり、 **[現在のユーザ(Current User)]**に保管されます。

3. 次のいずれかを実行します。
   - 「個人」(「マイ」)証明書ストアから証明書を選択するには、ドロップダウンリストから **[マイ(My)]**を選択します。
   - 信頼されたルート証明書を選択するには、ドロップダウンリストで **[ルート(Root)]**を選択します。
4. Webサイトでは、共通アクセスカード(CAC)リーダまたはパスワードで保護された証明書を使用していますか。
   - 「はい」の場合は、次の手順を実行します。
     i. **[証明書(Certificate)]**リストから、「(Protected)」というプレフィクスが付いた証明書を選択します。

     選択した証明書に関する情報と **[パスワード/PIN (Password/PIN)]**フィールドが **[証明書情報(Certificate Information)]**エリアに表示されます。
     ii. パスワードまたはPINが必要な場合は、 **[パスワード/PIN (Password/PIN)]**フィールドに入力します。

     注記: PINが必要な場合に、この時点でPINを入力しないと、スキャン中にPINの入力を求められるたびに、Windowsの **[セキュリティ]**ウィンドウにPINを入力する必要があります。

重要! {/b}デフォルトでは、OpenText DASTはOpenSSLを使用します。OpenSSLではなく特定のSSL/TLSプロトコルを使用している場合、スキャン設定のProfiler部分はパスワードで保護されている証明書で動作しない場合があります。

iii. **テスト(Test)**]をクリックします。
正しいパスワードまたはPINを入力した場合は、成功メッセージが表示されます。

- 「いいえ」の場合は、 **証明書(Certificate)**]リストから証明書を選択します。
選択した証明書に関する情報が 証明書(Certificate)]リストの下に表示されます。

アプリケーション認証の設定

サイトで認証が必要な場合は、このステップを使用してログインマクロを作成、選択、または編集することにより、ログインプロセスを自動化してサイトのカバレッジを拡大できます。ログインマクロは、アプリケーションにアクセスしてログインするために必要なアクティビティの記録です。通常は、ユーザ名とパスワードを入力し、 ログイン]や ログオン]などのボタンをクリックします。

ログインマクロを使用するスキャンの スキャン設定:認証(Scan Settings: Authentication)]で **マクロ検証を有効にする(Enable macro validation)**]が選択されている場合、OpenText DASTはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

注記: マクロテストは、2要素認証を含むマクロに対してはサポートされていません。

重要! {/b}2要素認証を含むマクロを使用する場合は、スキャンを開始する前に、2要素認証アプリケーションの設定を行う必要があります。詳細については、「"アプリケーション設定:2要素認証" ページ491」を参照してください。

ログインマクロでは、次のオプションを使用できます。

- "権限のエスカレーションなしでログインマクロを使用する" 次のページ
- "権限のエスカレーションのためにログインマクロを使用する" 次のページ
- "Fortify WebInspect Enterpriseに接続しているときにログインマクロを使用する" ページ156
- "マクロのテスト" ページ157

マスクされた値のサポート

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、OpenText DASTでガイド付きスキャンを設定するときにも、それらの値はマスクされます。

権限のエスカレーションなしでログインマクロを使用する

ログインマクロを使用するには:

1. [**このサイトでログインマクロを使用する(Use a login macro for this site)**]チェックボックスをオンにします。
2. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
   - [ログインマクロ(Login Macro)]フィールドに表示されている既存のログインマクロを編集するには、 [**編集(Edit)**]をクリックします。
   - 新しいマクロを記録するには、 [**作成(Create)**]をクリックします。

   新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。
3. [**次へ(Next)**]ボタンをクリックします。

   アプリケーション認証のステップが完了しました。アプリケーションステージに進み、アプリケーションを実行します。

権限のエスカレーションのためにログインマクロを使用する

権限のエスカレーションポリシーか、有効な権限のエスカレーションチェックを含む別のポリシーを選択した場合、高い権限を持つユーザアカウント用のログインマクロが少なくとも1つ必要です。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。ログインマクロを使用するには:

1. [**高い権限のユーザアカウントログインマクロ(High-Privilege User Account Login Macro)**]チェックボックスをオンにします。このログインマクロは、サイト管理者やモデレータアカウントなど、より高い権限を持つユーザアカウント用です。
2. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン([...])をクリックして、保存されているマクロを参照します。
   - [ログインマクロ(Login Macro)]フィールドに表示されている既存のログインマクロを編集するには、 [**編集(Edit)**]をクリックします。
   - 新しいマクロを記録するには、 [**作成(Create)**]をクリックします。

   新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。

   最初のマクロを記録または選択して [次へ(Next)]の矢印をクリックすると、 [低い権限のログインマクロを設定する(Configure Low Privilege Login Macro)]プロンプトが表示されます。

3. 次のいずれかを実行します。
   - 認証モードでスキャンを実行するには、 **[はい(Yes)]**をクリックします。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。

     ガイド付きスキャンが **[ログインマクロの選択(Select Login Macro)]**ウィンドウに戻り、低い権限のログインマクロを作成または選択できるようになります。ステップ4に進みます。
   - スキャンを非認証モードで実行するには、 **[いいえ(No)]**をクリックします。詳細については、「"権限のエスカレーションスキャンについて" ページ232」を参照してください。

     アプリケーション認証のステップが完了しました。アプリケーションステージに進みます。
4. **[低い権限のユーザアカウントログインマクロ(Low-Privilege User Account Login Macro)]**チェックボックスをオンにします。このログインマクロは、サイトコンテンツのビューアやコンシューマなど、低い権限のユーザアカウント用です。
5. 次のいずれかを実行します。
   - 事前に記録されたログインマクロを使用するには、省略記号ボタン(**[..]**)をクリックして、保存されているマクロを参照します。
   - **[ログインマクロ(Login Macro)]**フィールドに表示されている既存のログインマクロを編集するには、 **[編集(Edit)]**をクリックします。
   - 新しいマクロを記録するには、 **[作成(Create)]**をクリックします。

   新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章を参照してください。
6. 2つ目のマクロを記録または選択した後、 **[次へ(Next)]**ボタンをクリックします。

   アプリケーション認証のステップが完了しました。アプリケーションステージに進み、アプリケーションを実行します。

Fortify WebInspect Enterpriseに接続しているときにログインマクロを使用する

Fortify WebInspect Enterpriseに接続されているOpenText DASTの場合は、Fortify WebInspect Enterpriseマクロリポジトリからログインマクロをダウンロードして使用できます。

1. **[このサイトでログインマクロを使用する(Use a login macro for this site)]**チェックボックスをオンにします。
2. **[ダウンロード(Download)]**をクリックします。

   [Fortify WebInspect Enterpriseからマクロをダウンロードする(Download a Macro from Fortify WebInspect Enterprise)]ウィンドウが表示されます。
3. ドロップダウンリストから **[アプリケーション(Application)]**と **[バージョン(Version)]**を選択します。
4. **[マクロ(Macro)]**ドロップダウンリストからリポジトリマクロを選択します。
5. **[OK]**をクリックします。

注記: リポジトリマクロを選択すると、 最終確認(Final Review)]ページの **自動でスキャンをWIEにアップロードする(Automatically Upload Scan to WIE)**]の **アプリケーション(Application)**]と **バージョン(Version)**]が自動的に同期されます。

マクロのテスト

オプションで、 **テスト(Test)**]をクリックして、ログインフォームの検索とマクロ検証テストの実行を行ってから、ガイド付きスキャンウィザードの次のステージに進みます。完了前に検証テストをキャンセルする必要がある場合は、 **キャンセル(Cancel)**]をクリックします。

マクロが無効で、アプリケーションへのログインが失敗すると、エラーメッセージが表示されます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

アプリケーションの実行

アプリケーションを実行してWebトラフィックを生成および収集するには:

1. **記録(Record)**]ボタンをクリックします。
2. アプリケーションを実行し、顧客が行うようにインタフェースを移動します。
3. 十分なトラフィックが生成されたら、 **停止(Stop)**]ボタンをクリックします。
4. ワークフローを確認するには、 **再生(Play)**]をクリックします。

許可ホストとRESTfulエンドポイントの最終決定

アプリケーションを実行してWebトラフィックを収集すると、許可ホストと潜在的なRESTfulエンドポイントのリストが生成されます。

監査に含めるホストを選択するには、 **許可ホスト(Allowed Hosts)**]テーブルの **有効(Enabled)**]列のチェックボックスをクリックします。

RESTfulエンドポイントのリストは、RESTfulエンドポイントになる可能性のあるすべての組み合わせを一覧表示することで生成されます。 **有効(Enabled)**]チェックボックスを選択して、リストから実際のRESTfulエンドポイントを選択します。より可能性の高いサブセットだけを示すようリストを縮小するには、 **検出(Detect)**]ボタンをクリックします。ヒューリスティックが適用され、可能性の低い結果の一部がフィルタで除外されます。結果のリストで **有効(Enabled)**]チェックボックスを選択します。

OpenText DASTまたはFortify WebInspect Enterpriseですべ てのRESTfulエンドポイントが見つからなかった場合は、手動で追加できます。

新しいRESTfulエンドポイントルールを設定するには:

1. **新規ルール(New Rule)**]ボタンをクリックします。
   RESTfulエンドポイントテーブルに新しいルール入力ボックスが表示されます。
2. 入力ボックスのサンプルフォーマットに従って、RESTfulエンドポイントを入力します。

RESTfulエンドポイントのリストをインポートするには:

1. [**インポート(Import)**]ボタンをクリックします。
   ファイルセレクタが表示されます。
2. Webアプリケーション記述言語(.wadl)ファイルを選択します。
3. [**OK**]をクリックします。

設定の確認

最終ステージでは、収集したトラフィックの監査方法に影響を与えるいくつかのオプションを設定できます。使用可能なオプションは、選択した内容によって異なります。

詳細オプションの設定

詳細オプションの設定ステップでは、詳細オプションを設定できます。これらのオプションは、ガイド付きスキャンウィザードでの選択内容に依存するため、スキャンごとに変わります。次のようなオプションがあります。

識別された抑制された検出事項を再利用する

以前のスキャンで誤検出に変更された、または無視された脆弱性をインポートできます。これらの誤検出または無視された項目が現在のスキャンで検出された脆弱性と一致する場合、その脆弱性は誤検出に変更されるか、無視されます。既存のスキャンまたは抑制された検出事項ファイルから、抑制された検出事項をインポートできます。詳細については、「"抑制された検出事項" ページ83」を参照してください。

識別された抑制された検出事項を再利用するには:

1. [**抑制された検出事項のインポート(Import Suppressed Findings)**]を選択します。
2. 次の表に従って続行します。

使用する情報...	**その場合...**
既存のスキャン	a. [**抑制された検出事項をスキャンからインポートするには、ここをクリックします(Click here to import suppressed findings from scans)**]をクリックします。 [スキャンを選択して、抑制された検出事項をインポートする(Select a Scan to Import Suppressed Findings)]ダイアログが開きます。 b. 現在スキャンしている同じサイトからの、抑制された検出事項を含むスキャンを1つ以上選択します。 c. [**OK**]をクリックします。
抑制された検出事項ファイル	a. [**抑制された検出事項をファイルからインポートするには、ここをクリックします(Click here to import suppressed findings from a**

使用する情報...	その場合...
	file)]をクリックします。 標準のWindowsファイル選択ダイアログボックスが開きます。 b. インポートするファイルを選択し、[開く(Open)]をクリックします。 c. 必要に応じて、ステップaとbを繰り返して追加のファイルを選択します。

トラフィック分析

自己完結型のプロキシサーバをデスクトップで使用できます。これを使用すると、サーバとの間でHTTP要求の送信と応答の受信を行うスキャナ、ブラウザ、または他のツールからのトラフィックを監視できます。Traffic Monitorを有効にし、OpenText DASTナビゲーションペインにWebサイトまたはWebサービスの階層構造を表示することもできます。これにより、OpenText DASTによって送信されたすべてのHTTP要求と、サーバから受信した関連するHTTP応答を表示および確認できます。

スキャンモード(Scan mode)

検出(パスの切り捨て)の設定を可能にするWeb探索専用機能です。パスの切り捨てにより、ファイル名のない既知のディレクトリに対して要求を行うことができます。これにより、ディレクトリー覧を表示できます。また、[パッシブ分析(キーワード検索)(Passive Analysis (Keyword Search))]オプションを選択して、Webサーバからのすべての応答(エラーメッセージ、ディレクトリリスト、クレジットカード番号など)について、Webサイトで適切に保護されていないかどうかを調べることもできます。

設定の検証とスキャンの開始

このページのオプションを使用すると、現在のスキャン設定を保存することができます。また、OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、Fortify WebInspect Enterpriseとやり取りすることができます。

1. スキャン設定をXMLファイルとして保存するには、[**ここをクリックして設定を保存する(Click here to save settings)**]を選択します。標準の[名前を付けて保存(Save as)]ウィンドウを使用して、ファイルに名前を付けて保存します。
2. OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、ツールバーに[テンプレート(Templates)]セクションが表示されます。次の表に従って続行します。

目的の作業	その場合の手順
現在のスキャン設定をテンプレートとしてFortify WebInspect Enterpriseデータベースに保存する	a. 次のいずれかを実行します。 ◦ ツールバーの[テンプレート(Templates)]セクションで[保存

目的の作業	その場合の手順
注記: 既存のテンプレートを編集する場合、[保存(Save)]を実行すると、実際には更新が行われます。設定の編集を保存したり、テンプレート名を変更したりすることができます。ただし、アプリケーション、バージョン、またはグローバルテンプレートの設定は変更できません。	[保存(Save)]をクリックします。 ◦ [ここをクリックしてテンプレートを保存する(Click here to save template)]を選択します。 [テンプレートの保存(Save Template)]ウィンドウが表示されます。 b. [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。 c. [バージョン(Version)]ドロップダウンリストからアプリケーションバージョンを選択します。 d. [テンプレート(Template)]フィールドに名前を入力します。
テンプレートからスキャン設定をロードする	a. ツールバーの[テンプレート(Templates)]セクションで[ロード(Load)]をクリックします。 現在のスキャン設定が失われるという確認メッセージが表示されます。 b. [Yes]をクリックします。 [テンプレートのロード(Load Template)]ウィンドウが表示されます。 c. [アプリケーション(Application)]ドロップダウンリストからアプリケーションを選択します。 d. [バージョン(Version)]ドロップダウンリストからアプリケーションバージョンを選択します。 e. [テンプレート(Template)]ドロップダウンリストからテンプレートを選択します。 f. [ロード(Load)]をクリックします。 ガイド付きスキャンがサイトステージに戻り、Webサイトの検証と、テンプレートから

目的の作業	その場合の手順
	のステップごとの設定の実行が行えるようになります。

3. OpenText DASTがFortify WebInspect Enterpriseと統合されている場合は、このページに [Fortify WebInspect Enterprise] セクションが表示されます。Fortify WebInspect Enterpriseを操作するには、次のようにします。
   a. [**アプリケーション(Application)**] ドロップダウンリストからアプリケーションを選択します。
   b. [**バージョン(Version)**] ドロップダウンリストからアプリケーションバージョンを選択します。
   c. 次の表に従って続行します。

スキャンの実行方法	その場合の手順
Fortify WebInspect Enterpriseでセンサを使用する	i. [**WebInspect Enterpriseで実行(Run in WebInspect Enterprise)**] を選択します。 ii. [**センサ(Sensor)**] ドロップダウンリストからセンサを選択します。 iii. スキャンの [**優先度(Priority)**] を選択します。
OpenText DASTを使用する	i. [**DASTで実行(Run in DAST)**] を選択します。 ii. スキャン結果をFortify WebInspect Enterpriseの指定したアプリケーションおよびバージョンに自動的にアップロードする場合は、 [**WebInspect Enterpriseへの自動アップロード(Auto Upload to WebInspect Enterprise)**] を選択します。 **注記:** スキャンが正常に完了しない場合、Fortify WebInspect Enterpriseにはアップロードされません。

4. [**今すぐスキャン(Scan Now)**] エリアでスキャン設定を見直し、 [**スキャンの開始(Start Scan)**] をクリックしてスキャンを開始します。

スキャン後のステップ

スキャンを完了してOpenText DASTまたはFortify WebInspect Enterpriseを実行したら、Android、Windows、またはiOSデバイスまたはエミュレータを以前の状態にリセットする必要

があります。次のステップは、iOSデバイスを開始前の状態にリセットする方法を示しています。他のデバイスおよびエミュレータのステップは類似していますが、実行しているOSのバージョンによって異なります。

iOSデバイスでFortify証明書を削除するには:

[設定(Settings)]アプリケーションを実行します。

1. [設定(Settings)]列から[全般(General)]を選択します。
2. リストの一番下までスクロールして、[プロファイルWebInspectルート(Profile WebInspect Root)]を選択します。
3. [削除(Remove)]ボタンをタップします。

iOSデバイスのプロキシ設定を削除するには:

1. [設定(Settings)]アプリケーションを実行します。
2. [設定(Settings)]列から[Wi-Fi]を選択します。
3. [ネットワーク(Network)]の名前をタップします。

サーバのIPアドレスとポート番号を削除します。

参照情報

"ガイド付きスキャンの概要" ページ111

ガイド付きスキャンでの機能テストファイルのインポート

OpenText™ Functional Testingアプリケーションがインストールされている場合、OpenText DASTがこのアプリケーションを検出し、ワークフロースキャンに機能テストファイル(.usr)をインポートして、スキャンの完全性と攻撃露呈部分を改善できるようにします。詳細については、OpenText WebサイトのFunctional Testingに関するページを参照してください。

機能テスト(`.usr`)ファイルをOpenText DASTガイド付きスキャンにインポートするには:

1. ガイド付きスキャンを起動し、[スキャンタイプ(Scan Type)]として[ワークフロースキャン(Workflows Scan)]を選択します。[ワークフロースキャン(Workflows Scan)]オプションの下に追加のテキストが表示されます。

   OpenText Functional Testingが検出されました。スクリプトをインポートして、セキュリティテストの完全性を強化できます。
2. [次へ(Next)]ボタンをクリックします。
3. [認証(Authentication)]セクションで、[アプリケーション認証(Application Authentication)]が自動的に選択されます。指示に従ってフィールドに入力します。

4. [ワークフローの管理(Manage Workflows)]画面で[インポート(Import)]をクリックします。 [スクリプトのインポート(Import Scripts)]ダイアログボックスが表示されます。 [スクリプトのインポート(Import Scripts)]ダイアログボックスでは、次の操作を実行できます。
   - ファイル名を入力します。
   - クリックしてファイルを参照し、拡張子が.usrのファイルを探します。ファイルタイプのドロップダウンから[VuGenスクリプトファイル(VuGen script file)]を選択し、ファイルに移動します。
   - [編集(Edit)]をクリックして、OpenText Functional Testingアプリケーションを起動します。
5. (オプション) [スクリプトのインポート(Import Scripts)]ダイアログボックスでは、次のいずれかのオプションを選択できます。
   - **インポート時にOpenText Functional Testing UIを表示する(Show OpenText Functional Testing UI during import)**
   - **インポート後にスクリプトの結果を開く(Open script result after import)**
6. インポートするファイルを選択し、[インポート(Import)]をクリックします。ファイルが正常にインポートされると、そのファイルが[ワークフロー(Workflows)]テーブルに表示されます。
7. [ワークフロー(Workflows)]テーブルから次のいずれかを選択します。
   - **記録(Record)** - Web Macro Recorderを起動します。詳細については、『OpenText™ Dynamic Application Security Testingツールガイド』の「Webマクロレコーダ」の章を参照してください。
   - **編集(Edit)** - Webマクロレコーダを使用してファイルを変更できます。『OpenText™ Dynamic Application Security Testingツールガイド』の「Webマクロレコーダ」の章を参照してください。
   - **削除(Delete)** - [ワークフロー(Workflows)]テーブルからスクリプトを削除します。
   - **インポート(Import)** -別のファイルをインポートします。
   - **エクスポート(Export)** -指定した名前と場所を使用して.webmacro形式でファイルを保存します。
8. [次へ(Next)]ボタンをクリックします。

   最初の.usrスクリプトファイルをリストに追加すると、その名前(またはデフォルトの名前)が[ワークフロー(Workflows)]テーブルに表示され、[許可ホスト(Allowed Hosts)]テーブルがペインに追加されます。

   別の.usrスクリプトファイルを追加すると、許可ホストをさらに追加できます。有効になっているホストは、追加の対象であるworkflow.usrファイルだけでなく、一覧表示されたすべてのワークフロー.usrスクリプトファイルで使用できます。ガイド付きスキャンでは、対応するチェックボックスがオンであるかどうかに関係なく、一覧にされているすべてのワークフローファイルが再生され、一覧にされているすべての許可ホストに対して要求が行われます。許可ホストのチェックボックスがオンになっている場合、OpenText DASTはそのホストからの応答をWeb探索または監査します。チェックボックスがオフの場合、OpenText DASTは、そのホストからの応答をWeb探索または監査しません。加えて、特定のワークフロー.usrスクリプトでパラメータが使用されている場合は、そのワークフローマクロがリストで

選択されたときに [マクロパラメータ(Macro Parameters)] テーブルが表示されます。必要に応じてパラメータの値を編集します。

9. [ワークフロー(Workflows)] テーブルの変更または追加が完了したら、ガイド付きスキャンウィザードで次に進み、設定を完了してスキャンを実行します。新しいログインマクロの記録や既存のログインマクロの使用の詳細については、『OpenText™ Dynamic Application Security Testingツールガイド』の「Webマクロレコーダ」の章を参照してください。

APIまたはWebサービススキャンの実行

ターゲットアプリケーションで使用されるRESTアプリケーションプログラミングインタフェース(API)またはWebサービスのスキャンを実行できます。OpenText DASTは、次のAPIまたはWebサービステクノロジのスキャンの実行をサポートしています。

- GraphQL
- gRPC
- OData
- Postman
- SOAP
- Swagger (Open APIとも呼ばれる)

SOAP Webサービススキャンに関する重要な情報

従来のSOAP Webサービススキャン機能は今後のリリースで削除される予定です。
OpenTextでは、できるだけ早く新しいSOAP向けAPIスキャンに移行することをお勧めします。

gRPC protoファイルに関する重要な情報

すべてのgRPC protoファイルは、自己完結型である必要があります。インポートは、ユーザ生成ファイルに対してではなく、内部で認識されるリソースに対して行う必要があります。
OpenText DASTは、インポートされたprotoファイルのファイルパスを識別できません。このようなファイルを使用した場合、スキャンはクライアントの生成に失敗し、中断されます。追加のインポートが必要な場合は、プライマリprotoファイルと組み合わせて「マスタ」protoファイルにする必要があります。

gRPCスキャンの既知の制限

gRPCスキャンに関連する次の既知の制限に注意してください。

- gRPC APIのスキャンを実行するには、Windows 11にインストールされたOpenText DASTか、LinuxバージョンのOpenText DASTが必要です。
- 暗号化されていないHTTP/2 (H2C)を使用してサーバ上で実行されているgRPC APIのスキャンを実行するには、LinuxバージョンのOpenText DASTを使用する必要があります。

Linuxバージョンの詳細については、*OpenText™ Dynamic Application Security TestingおよびOAST on Dockerユーザガイド*を参照してください。

スキャンを実行するためのオプション

APIとWebサービスのスキャンは、OpenText DASTユーザインタフェースまたはCLIを使用して実行できます。詳細については、次のトピックを参照してください。

- "APIスキャンウィザードの使用" 下
- "wi.exeを使用したAPIのスキャン" ページ186

ODataおよびSwagger (Open API)タイプの場合、`WISwag.exe`ツールをwi.exeまたはOpenText DAST REST APIと組み合わせて使用することでスキャンを実行できます。詳細については、「"WISwag.exeツールの使用" ページ349」を参照してください。

APIスキャンウィザードの使用

OpenText DASTユーザインタフェース内で、APIスキャンウィザードを使用して、APIスキャンまたはWebサービススキャンの設定を行うことができます。

APIスキャン

Swagger、OData、Postmanスキャンの場合、OpenText DASTはREST API定義からマクロを作成し、自動分析を実行します。GraphQL、gRPC、SOAPスキャンでは、従来のスキャン方法が使用されます。

重要! {/b}Postman APIスキャンを設定する場合は、次に進む前に前提条件のソフトウェアがインストールされていることを確認してください。ダイナミックトークンを使用したダイナミック認証の設定など、Postmanコレクションファイルの使用に関する詳細については、「"Postmanコレクションによるスキャン" ページ364」を参照してください。

Webサービススキャン(Web Service Scan)

従来のWebサービススキャンの場合、OpenText DASTはWSDLサイトをWeb探索し、検出した各操作の各パラメータに値を送信します。これらの値はファイルから抽出されますが、そのファイルはWeb Service Test Designerを使用して作成する必要があります。次に、OpenText DASTは、SQLインジェクションなどの脆弱性を検出するために各パラメータを攻撃して、サイトを監査します。

Webサービス脆弱性スキャンとその他のタイプのスキャンアクションの違いについては、「"Webサービスの監査" ページ293」を参照してください。

推奨

OpenTextでは、スキャンを一度に1回だけ実行することをお勧めします。SQL Expressを使用する場合は特に、サイトのサイズによっては、同時(または並行)スキャンを実行すると、OpenText DASTホスト上のRAM、CPU、およびディスクリソースの使用率が高くなる場合があります。

APIスキャンウィザードの開始

APIスキャンまたはWebサービススキャンの設定を開始するには:

1. OpenText DASTの **[開始ページ(Start Page)]** で **[APIスキャンの開始(Start an API Scan)]** をクリックします。
   APIスキャンウィザードが開きます。
2. オプションで、 **[スキャン名(Scan Name)]** ボックスにスキャンの名前を入力します。

ヒント: APIスキャンウィザードで表示される任意のウィンドウで、(ウィンドウの下部にある) **[設定(Settings)]** をクリックして、デフォルトの設定を変更するか、または以前に保存した設定ファイルをロードすることができます。変更はすべてこのスキャンにのみ適用され、デフォルト設定ファイルに保持されることはありません。変更を行い、デフォルト設定として維持するには、OpenText DASTの **[編集(Edit)]** メニューをクリックし、 **[デフォルトのスキャン設定(Default Scan Settings)]** を選択します。

次に行う作業

次のいずれかを実行します。

- APIスキャンを設定するには、"APIスキャンの設定" 下に進んでください。
- WEBサービス定義言語(WSDL)ファイルを使用して従来のWebサービススキャンを設定するには、"WSDLファイルを使用したWebサービススキャンの設定" ページ169に進みます。
- WEBサービステスト設計(WSD)ファイルを使用して従来のWebサービススキャンを設定するには、"既存のWSDファイルを使用したWebサービススキャンの設定" ページ170に進みます。

APIスキャンの設定

APIスキャンの設定は、**APIスキャンウィザード**の **[APIスキャン(API Scan)]** ページで開始できます。

APIスキャンを設定するには:

1. **[APIスキャン(API Scan)]** を選択します。
2. **[APIタイプ(API Type)]** リストでスキャンするAPIタイプを選択します。オプションは次のとおりです。
   - **GraphQL**
   - **gRPC**

     注記: SOCKSプロキシを使用するWindows上のOpenText DASTはgRPC APIをスキャンできません。
   - **OData**
   - **Postman**

- SOAP
- Swagger (Open APIとも呼ばれる)

3. 次の表に従って続行します。

APIのタイプ...	操作手順
GraphQL gRPC OData Swagger	次のいずれかを実行します。 • [API定義/設定(API Definition/Config)]ボックスに、API定義ファイルのURLを次の例に示すように指定します。 `http://172.16.81.36/v1` `http://myapi/protos/client.proto` `http://myapi/graphql/` • ...をクリックして、環境設定ファイルまたは定義ファイルをインポートします。 **ヒント:** または、ローカルマシンに保存されているファイルへのフルパスを貼り付けることもできます。 [スキャン名(Scan Name)]ボックスに名前を入力しなかった場合は、定義ファイルが解析され、URLが[スキャン名(Scan Name)]ボックスに追加されます。
Postman	次のいずれかを実行します。 • ワークフローコレクションをインポートするには、...をクリックし、ドロップダウンリストから[ワークフロー(Workflow)]を選択して、Postmanワークフローコレクションファイルをインポートします。 • 認証コレクションをインポートするには、...をクリックし、ドロップダウンリストから[認証(Authentication)]を選択し、Postman認証コレクションファイルをインポートします。 • 環境ファイルをインポートするには、...をクリックし、ドロップダウンリストから[環境(Environment)]を選択し、Postman環境ファイルをインポートします。 • グローバル変数を含むファイルをインポートするには、...をクリックし、ドロップダウンリストから[グローバル(Globals)]を選択して、Postmanグローバル変数ファイルをインポートします。 ファイルは、Postmanファイルのリストに追加されます。追加のファイルをインポートするには、このステップを繰り返します。

APIのタイプ...	操作手順
	重要! {/b}ワークフローコレクションファイルは複数インポートできます。インポートできる認証コレクションファイル、環境ファイル、グローバル変数ファイルはそれぞれ1つのみです。環境変数ファイルとグローバル変数ファイルの両方で同じ変数が定義されている場合、環境ファイルがグローバルファイルを上書きします。
SOAP	a. 次のいずれかを実行します。 ◦ [API定義/設定(API Definition/Config)]ボックスに、API定義ファイルのURLを次の例に示すように指定します。 `http://172.16.81.36/web-services/infoService?wsdl` ◦ ...をクリックして、環境設定ファイルまたは定義ファイルをインポートします。 **ヒント:** または、ローカルマシンに保存されているファイルへのフルパスを貼り付けることもできます。 [スキャン名(Scan Name)]ボックスに名前を入力しなかった場合は、定義ファイルが解析され、URLが[スキャン名(Scan Name)]ボックスに追加されます。 b. [バージョン(Version)]リストで、特定のバージョンに基づく操作のフィルタリングを許可するバージョンを選択します。オプションは次のとおりです。 ◦ **従来(Legacy)** - サポートされている最下位バージョンに対してフィルタが適用されます。 ◦ **混合(Mixed)** - 使用できるものに応じて、従来と最新の組み合わせを使用します。 ◦ **最新(Newest)** - デフォルト設定です。最新バージョンに対してフィルタが適用されます。

4. の場合、スキーム、ホスト、またはサービスパスが指定されている定義ファイルまたは環境設定ファイルがインポートされると、[APIの場所はAPI定義の場所と異なる(API location is different from API definition location)]オプションが選択されます。次の項目を指定します。
   - [APIスキームのタイプ(API Scheme Type)]リストで、タイプを選択します。オプションは、[HTTP]、[HTTPS]、[HTTPおよびHTTPS (HTTP and HTTPS)]です。
   - [APIホスト(API Host)]ボックスに、URLまたはホスト名を入力します。
   - [APIサービスパス(API Service Path)]ボックスに、APIサービスのディレクトリパスを入力します。

注記: GraphQLサービスの場所は、常に定義場所と同じです。gRPCサービスの場所は、常に定義場所とは異なります。

注記: SOAPの場合、クエリ文字列「?wsdl」値が削除されると、SOAPサービスの場所が定義場所と同じになる場合と異なる場合があります。また、定義済みのサービスホストまたはパスのないWSDLを提供する場合は、 **[APIの場所とAPI定義の場所が異なっている(API location is different from API definition location)]**を選択し、 **[APIホスト(API Host)]**ボックスと **[APIサービスパス(API Service Path)]**ボックスを空のままにする必要があります。OpenText DASTは、SOAPポートバインディング場所を使用して要求を送信します。

注記: Swaggerスキャンに対してサービスパスが定義されていない場合、OpenText DASTはSwagger定義の内容で定義されているbasePathを使用します。Swaggerスキャンの場合、サービスがSwaggerのdocsフォルダと同じ場所で明示的に実行されていない限り、 **[APIの場所はAPI定義の場所と異なる(API location is different from API definition location)]**を選択します。オプションで、サービスパスがbasePathと異なる場合は、そのパスを定義することもできます。

5. **[次へ(Next)]**をクリックし、"APIスキャンの認証とコネクティビティの設定" 次のページに進みます。

WSDLファイルを使用したWebサービススキャンの設定

APIスキャンウィザードの **[APIスキャン(API Scan)]**ページで、Webサービス定義言語(WSDL)ファイルを使用して、従来のWebサービススキャンの設定を開始できます。

WSDLファイルを使用して設定を行うには:

1. **[SOAP Webサービススキャンの設定(Configure a SOAP Web Service Scan)]**を選択します。
2. 次のいずれかを実行します。
   - WSDLファイルのフルパスと名前を入力または選択します。
   - ...をクリックして標準のファイル選択ダイアログボックスを開き、WSDLファイルを選択します。

注記: この時点でWSDLファイルをインポートし、後でWeb Service Test Designerを起動して、サービスの各操作の値を含むファイルを設定します。

3. **[次へ(Next)]**をクリックし、"APIスキャンの認証とコネクティビティの設定" 次のページに進みます。

既存のWSDファイルを使用したWebサービススキャンの設定

APIスキャンウィザードの **APIスキャン(API Scan)**]ページで、既存のWebサービステスト設計(WSD)ファイルを使用して、従来のWebサービススキャンの設定を開始できます。

既存のWSDファイルを使用して設定を行うには:

1. **既存のデザインファイルを使用してスキャンする(Scan with Existing Design File)**]を選択します。
2. ...をクリックして標準のファイル選択ダイアログボックスを開き、Web Service Test Designerを使用して以前に作成したWSDファイルを選択します。

   注記: 選択したファイルには、サービスの各操作の値が含まれています。

3. **次へ(Next)**]をクリックし、"APIスキャンの認証とコネクティビティの設定" 下に進みます。

APIスキャンの認証とコネクティビティの設定

プロキシ設定、ネットワーク認証、サイト認証は、**APIスキャンウィザード**の **認証とコネクティビティ(Authentication and Connectivity)**]ページで設定できます。認証を設定するためのオプションには、次のものがあります。

- "APIスキャンおよびWebサービススキャンのプロキシの設定" 下
- "APIスキャンおよびWebサービススキャンのネットワーク認証の設定" 次のページ
- "クライアント証明書の使用" ページ173
- "カスタムヘッダの使用" ページ174
- "SOAP認証の設定" ページ175

注記: このトピックの一部のオプションは、Webサービス定義言語(WSDL)ファイルまたは既存のWebサービステスト設計(WSD)ファイルを使用する、従来のWebサービススキャンには適用されません。

APIスキャンおよびWebサービススキャンのプロキシの設定

プロキシサーバ経由でターゲットサイトにアクセスする必要がある場合は、**APIスキャンウィザード**の **認証とコネクティビティ(Authentication and Connectivity)**]ページでプロキシを設定できます。

プロキシ設定を行うには:

- **ネットワークプロキシ(Network Proxy)**]を選択し、**プロキシプロファイル(Proxy Profile)**]リストからオプションを選択します。
  - **自動検出(Auto Detect)**]: WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、これを使用してブラウザのWebプロキシ設定を行います。
  - **システムプロキシを使用(Use System Proxy)**]: ローカルマシンからプロキシサーバ情報をインポートします。

- **[PACファイルを使用(Use PAC File)]**: PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。このオプションを選択した場合は、**[編集(Edit)]**をクリックしてPACの場所(URL)を入力します。
- **[明示的なプロキシ設定を使用(Use Explicit Proxy Settings)]**: プロキシサーバ設定を指定します。このオプションを選択した場合は、**[編集(Edit)]**をクリックしてプロキシ情報を入力します。
- **[Mozilla Firefoxを使用(Use Mozilla Firefox)]**: Firefoxからプロキシサーバ情報をインポートします。

重要! {/b}Socks4プロキシサーバは認証に対応しません。認証が必要なSocksプロキシサーバを使用する場合は、Socks5プロキシを使用する必要があります。

注記: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が**[プロキシーを使用しない]**に設定されている場合、またはInternet Explorerの**[LANにプロキシサーバを使用する]**設定が選択されていない場合、プロキシサーバは使用されません。

APIスキャンおよびWebサービススキャンのネットワーク認証の設定

Webサーバにアクセスするためのネットワーク認証は、**APIスキャンウィザード**の**[認証とコネクティビティ(Authentication and Connectivity)]**ページで設定できます。

Webサーバのネットワーク認証を設定するには:

1. **[ネットワーク認証(Network Authentication)]**を選択します。
2. **[メソッド(Method)]**ドロップダウンリストで、認証メソッドを選択します。APIタイプによって、使用可能な認証メソッドが決まります。すべてのメソッドのリストを以下に示します。
   - ADFS CBT
   - 自動
   - 基本
   - Bearer
   - カスタム(Custom)
   - ダイジェスト
   - Kerberos
   - ネゴシエート(Negotiate)
   - NT LAN Manager (NTLM)
   - OAuth 2.0 Bearer

   注記: ADFS CBT、自動、Kerberos、ネゴシエートのメソッドは、AuthProvidersを使用するスキャンでは使用できません。
3. 次の表に従って続行します。

認証のタイプ	操作手順
ADFS CBT 自動 基本 ダイジェスト Kerberos ネゴシエート (Negotiate) NTLM	a. [ユーザ名(Username)]ボックスに認証ユーザ名を入力します。 b. [パスワード(Password)]ボックスに認証パスワードを入力します。
カスタム (Custom)	a. [スキーム(Scheme)]ボックスにカスタムヘッダ名またはトークン名を入力します。 b. [パラメータ(Parameter)]ボックスにトークン値を入力します。 カスタムを使用する場合、ワークフローマクロに対する応答から生成されるトークンをフェッチし、そのトークンを使用して状態を適用できます。詳細については、「"トークン値のフェッチ" 下」を参照してください。
Bearer	[パラメータ(Parameter)]ボックスにトークン値を入力します。 Bearerを使用する場合、ワークフローマクロに対する応答から生成されるトークンをフェッチし、そのトークンを使用して状態を適用できます。詳細については、「"トークン値のフェッチ" 下」を参照してください。
OAuth 2.0 Bearer	[設定(Configure)]をクリックし、"OAuth 2.0のBearer資格情報の設定" ページ447に進みます。

トークン値のフェッチ

カスタム正規表現を使用して、ログインマクロまたはワークフローマクロからトークン値をフェッチできます。応答内で正規表現との一致が検出されると、その値がフェッチされ、Bearerトークンとして使用されます。正規表現に括弧が含まれている場合は、括弧内の値が抽出され、Bearerトークンとして使用されます。括弧内の最初の値だけが使用されます。

注記: トークン値のフェッチは、ODataまたはSwagger定義タイプには適用されません。

トークン値をフェッチするには:

1. [**マクロからトークンをフェッチする(Fetch Token From Macro)**]を選択します。
2. 次のいずれかを実行します。
   - 既存のマクロをインポートするには、...をクリックして、インポートするファイルを探して選択します。
   - マクロを記録するには、Record...をクリックします。
3. [**トークンフェッチの検索パターン(Fetch Token Search Pattern)**]ボックスにパターンマッチングの正規表現を入力します。
4. 次のいずれかを実行します。
   - 各スキャンスレッドに独自のフェッチマクロを再生させ、Bearerトークン値をそのスレッドに適用するには、[**状態を分離する(Isolate State)**]チェックボックスを選択します。
   - すべてのスキャンスレッドに対して1つのフェッチマクロのみを再生し、単一の共有Bearerトークン値をすべてのスレッドに適用するには、[**状態を分離する(Isolate State)**]チェックボックスをオフにします。

クライアント証明書の使用

クライアント証明書認証を使用すると、ユーザはサイト認証のためにユーザ名とパスワードを入力するのではなく、クライアント証明書を提示することができます。証明書の使用を有効にしてから、証明書をスキャン設定にインポートできます。

注記: クライアント証明書は、ODataまたはSwagger定義タイプには適用されません。

クライアント証明書を使用するには:

1. [**クライアント証明書(Client Certificate)**]を選択します。
2. ...をクリックします。
   標準のWindowsファイル選択ダイアログボックスが開きます。
3. 証明書ファイルを探して選択し、[**開く(Open)**]をクリックします。
   その証明書ファイルが[クライアント証明書(Client Certificate)]ボックスに追加されます。
4. [**クライアント証明書のパスワード(Client Certificate Password)**]ボックスにパスワードを入力します。

複合スキャン設定での証明書の更新

複合スキャン設定には、暗号化された証明書データを格納するBINファイルが含まれています。複合スキャン設定でクライアント証明書を置換または更新する必要がある場合は、更新したPFXファイルまたはP12ファイルを、複合設定のZIPファイル内のcertificatesディレクトリに配置できます。OpenText DASTで設定を開くと、まずPFXファイルとP12ファイルの有無がチェックされます。どちらも存在しない場合、BINファイルが復号化されて使用されます。複合設定の詳細については、"アプリケーション設定: 全般" ページ480を参照してください。

クライアント証明書を置換または更新するには、次の手順を実行します。

1. 複合スキャン設定のZIP内のcertificatesディレクトリで、暗号化されたBINファイルを見つけます。ファイル名はGUIDで、次のようになります。

   `<your-scansettings.zip>\certificates\0b627638-efda-4d01-a83e-80ee3a79b4cf.bin`

   注記: Windowsにおけるデフォルトの設定ファイルの場所は、`C:\ProgramData\HP\HP WebInspect\Settings\`です。

2. 更新したPFXファイルまたはP12ファイルを同じディレクトリに配置します。
3. PFXファイルまたはP12ファイルの名前をBINファイルと同じ名前に変更します。前の例を使用すると、ファイル名は次のようになります。

   `0b627638-efda-4d01-a83e-80ee3a79b4cf.pfx`

   – または –

   `0b627638-efda-4d01-a83e-80ee3a79b4cf.p12`

   重要! {/b}必ず元のファイル拡張子を保持してください。

4. 必要に応じて、暗号化された証明書を設定に保持する場合は、設定を再度保存します。BINファイルには、更新されたPFX証明書またはP12証明書が反映されます。PFX証明書またはP12証明書がZIPから削除されます。

ヒント: PFX証明書およびP12証明書では、多くの場合、パスワードが必要です。次のいずれかのオプションを使用して、設定のパスワードを指定します。

- PFX証明書またはP12証明書を作成するときに空のパスワードを設定し、それを設定のZIPファイルに配置します。
- PFX証明書またはP12証明書のパスワードを保持し、`settings.json`ファイルを編集して、次のようにCertificatePinの値としてパスワードを設定します。

  `"CertificatePin": "<password>"`

カスタムヘッダの使用

認証のために追加のヘッダまたは別のヘッダが必要な場合は、その情報をカスタムヘッダとして追加する必要があります。

複数のカスタムヘッダを設定できます。

重要! {/b}同じHTTPヘッダ名を使用して複数のカスタムヘッダを設定することはできません。

カスタムヘッダを追加するには:

1. **[カスタムヘッダ(Custom Headers)]**を選択します。
2. **[追加...(Add...)]**をクリックします。
3. **[名前(Name)]**ボックスに、カスタムHTTPヘッダ名を入力します。たとえば、`X-MyCustomAuth`になります。

   重要! {/b}ヘッダは固有でなければならず、`Authorization`にすることはできません。

4. [スキーム(Scheme)]ボックスに、ヘッダ値のプレフィクス名を入力します。たとえば、CustomTokenになります。
5. [パラメータ(Parameter)]ボックスに、カスタムヘッダ値を入力します。
6. [OK]をクリックします。
   カスタムヘッダがリストに追加されます。

カスタムヘッダを編集するには:

1. [カスタムヘッダ(Custom Headers)]リストで、編集するカスタムヘッダを選択します。
2. [編集...(Edit...)]をクリックします。
3. "カスタムヘッダを追加するには:" 前のページの手順3から6に従います。

カスタムヘッダを削除するには:

1. [カスタムヘッダ(Custom Headers)]リストで、削除するカスタムヘッダを選択します。
2. [削除(Remove)]をクリックします。

SOAP認証の設定

SOAPスキャンのためのメッセージベースの認証を設定できます。

SOAP認証を設定するには:

1. [SOAP認証(SOAP Authentication)]を選択します。
2. [SOAPメソッド(SOAP Method)]リストから、使用する認証メソッドを選択します。オプションは、 [ユーザ名トークン(Username Token)]と [証明書ペア(Certificate Pair)]です。
3. 次の表に従って続行します。

SOAPメソッド	操作手順
ユーザ名トークン(Username Token)	a. [ユーザ名(Username)]ボックスに、資格情報をSOAPサービスへのアクセスに使用するユーザ名を入力します。 b. [パスワード(Password)]ボックスに、ユーザ名のパスワードを入力します。 c. [ユーザ名トークンタイプ(Username Token Type)]リストで、トークンのタイプを選択します。オプションは、 [テキスト(Text)]と [ハッシュ(Hash)]です。 d. [タイムスタンプ(Timestamp)]リストで、ユーザ名トークンの作成日時と有効期限のオプションを選択します。オプションは、 [作成済み(Created)]、 [フル(Full)]、 [なし(None)]です。 e. トークンに対してnonceが有効になっている場合は、 [nonceを含める(Include nonce)]を選択します。

SOAPメソッド	操作手順
	重要! {/b}nonceはハッシュトークンに必要です。これは、サーバがハッシュを再計算して、クライアントから送信されたデータと比較できるようにするためです。
証明書ペア	a. [クライアント証明書(Client Certificate)]ボックスの右側にある...をクリックします。 標準のWindowsファイル選択ダイアログボックスが開きます。 b. 証明書ファイルを探して選択し、[開く(Open)]をクリックします。 その証明書ファイルが[クライアント証明書(Client Certificate)]ボックスに追加されます。 c. [クライアント証明書のパスワード(Client Certificate Password)]ボックスにパスワードを入力します。 d. [サーバ証明書(Server Certificate)]ボックスの右側にある...をクリックします。 標準のWindowsファイル選択ダイアログボックスが開きます。 e. 証明書ファイルを探して選択し、[開く(Open)]をクリックします。 その証明書ファイルが[サーバ証明書(Server Certificate)]ボックスに追加されます。 f. [サーバ証明書のパスワード(Server Certificate Password)]ボックスにパスワードを入力します。

4. または、SOAPサービスが使用するWebサービスアドレス指定(WS-Addressing)スキーマバージョンを識別するために、[WS Addressing]を選択して、次を行います。
   a. [スキーマバージョン(Schema Version)]リストでバージョンを選択します。オプションは、[なし(NONE)]、[WSA0408]、[WSA0508]です。
   b. [WSA: 宛先(WSA: To)]ボックスに、Webサービスホストの URL上書きを入力します。

   注記: SOAPサービスは、ロードバランサまたはリバースプロキシによって公開される場合があります。この設定により、センサが内部Webサービスのホスト名に関する正しい情報を取得できなくなる場合があります。[WSA: 宛先(WSA: To)]のURL上書きにより、WS Addressingに正しいアドレスを指定できます。

   URL上書きでは、次のフォーマットが使用されます。

   ```
   https://<host_name><service_path>/<port_name>
   ```

次に行う作業

次のいずれかを実行します。

- WEBサービス定義言語(WSDL)ファイルまたは既存のWebサービステスト設計(WSD)ファイルを使用して従来のWebサービススキャンを設定する場合は、 **次へ(Next)**]をクリックして、"APIおよびWebサービススキャンのスキャン詳細の設定" ページ183に進みます。
- 他のすべてのAPIスキャンの場合は、 **次へ(Next)**]をクリックして、"APIコンテンツおよびフィルタの設定" 下に進みます。

APIコンテンツおよびフィルタの設定

APIスキャンを設定する場合、**APIスキャンウィザード**の **コンテンツおよびフィルタ(Content and Filters)**]ページを使用して、優先コンテンツタイプと、スキャン中にインクルードまたは除外する操作、パラメータ名、パラメータタイプを設定できます。Postman APIスキャンを実行する場合、以前に選択したコレクションファイルがスキャンウィザードによって検証され、このページにPostman環境設定が表示されます。設定を確認し、必要に応じて調整できます。

Postman環境設定の表示および調整

注記: Postman環境設定は、Postman APIスキャンを実行する場合にのみ使用できます。

Postmanコレクションファイルの検証が正常に完了すると、コレクションファイルに含まれるセッションのリストが **Postman設定(Postman Configuration)**]エリアに表示されます。認証セッションが指定されている場合、それらのセッションは**認証(Auth)**セッションとして事前に選択されます。その他のすべてのセッションは、**監査(Audit)**セッションとして事前に選択されます。また、検出された認証のタイプが**トークン戦略(Token Strategy)**として一覧にされ、オプションとして **なし(None)**]、 **スタティック(Static)**]、または **ダイナミック(Dynamic)**]があります。

注記: 認証(Auth)セッションは、スキャンの認証に使用されます。**監査(Audit)**セッションは、スキャンで監査されます。

必要に応じて設定を調整します。

1. 必要に応じてセッションのタイプを変更するには、 **認証(Auth)**]または **監査(Audit)**]チェックボックスをオンにします。
2. Postman認証設定を次のように変更します。
   - **スタティック(Static)**認証の場合は、 **カスタムヘッダトークン(Custom Header Token)**]ボックスにトークンを入力します。
   - **ダイナミック(Dynamic)**認証の場合は、次の手順を実行します。
     - **応答トークン(Response Token)**]ボックスの右側にある **正規表現(カスタム)(Regex (Custom))**]オプションを選択して、 **応答トークン名(Response Token Name)**]ボックスにカスタム正規表現を入力します。
     - **要求トークン名(Request Token Name)**]ボックスの右側にある **正規表現(カスタム)(Regex (Custom))**]オプションを選択して、 **要求トークン名(Request Token Name)**]ボックスにカスタム正規表現を入力します。

- [**ログアウト条件(Logout Condition)**]ボックスの右側にある[**自動検出を使用する(Use Auto Detect)**]オプションをオフにして、[**ログアウト条件(Logout Condition)**]ボックスに新しいログアウト条件文字列を入力します。

Postmanの動的認証の詳細については、「"ダイナミックトークン用のPostmanログインの手動設定" ページ368」を参照してください。

重要! {/b}Postman認証設定を変更する場合、**APIスキャンウィザード**の[**APIスキャン(API Scan)**]ページに戻り、[**次へ(Next)**]をもう一度クリックしないと、これらの変更は検証されません。

優先コンテンツタイプの指定

優先コンテンツタイプの設定では、要求ペイロードの優先コンテンツタイプを指定します。操作でサポートされているコンテンツタイプのリストに優先コンテンツタイプがある場合、生成される要求ペイロードはそのタイプになります。ない場合は、操作で最初に一覧指定されているコンテンツタイプが使用されます。優先コンテンツタイプの例: `application/json`。

重要! {/b} [**優先コンテンツタイプ(Preferred Content Type)**]設定は、GraphQL、SOAP、gRPC、PostmanなどのスキーマベースのAPIでは機能しません。

優先タイプを指定するには:

- [**優先コンテンツタイプ(Preferred Content Type)**]ボックスに優先コンテンツタイプを入力します。

包含する特定の操作の定義

包含機能は、出力に包含する必要がある操作IDの許可リストを定義します。

包含する特定の操作を定義するには:

1. [**特定の操作(Specific Operations)**]を選択します。
2. [**包含(Include)**]を選択します。
3. [**追加(Add)**]をクリックします。
   [操作の指定(Specify Operation)]ダイアログボックスが開きます。
4. [**操作(Operation)**]ボックスに操作IDを入力します。
5. [**OK**]をクリックします。
   操作IDが許可リストに追加されます。

除外する特定の操作の定義

除外機能は、出力から除外する必要がある操作IDの拒否リストを定義します。

除外する特定の操作を定義するには:

1. [**特定の操作(Specific Operations)**]を選択します。
2. [**除外(Exclude)**]を選択します。

3. [追加(Add)]をクリックします。
   [操作の指定(Specify Operation)]ダイアログボックスが開きます。
4. [操作(Operation)]ボックスに操作IDを入力します。
5. [OK]をクリックします。
   操作IDが拒否リストに追加されます。

特定の操作の編集

許可リストまたは拒否リストの特定の操作を編集するには:

1. 次のいずれかを実行します。
   - 許可リストで操作を編集するには、 [包含(Include)]を選択します。
   - 拒否リストで操作を編集するには、 [除外(Exclude)]を選択します。
2. 編集する操作IDを選択します。
3. [編集(Edit)]をクリックします。

特定の操作の削除

許可リストまたは拒否リストから特定の操作を削除するには:

1. 次のいずれかを実行します。
   - 許可リストで操作を削除するには、 [包含(Include)]を選択します。
   - 拒否リストで操作を削除するには、 [除外(Exclude)]を選択します。
2. 削除する操作IDを選択します。
3. [削除(Remove)]をクリックします。

パラメータルールの定義

パラメータルールは、パラメータ名とタイプが検出された場合にパラメータに使用するデフォルト値を定義します。また、操作を指定して、特定のパラメータルールをそれらの操作に適用するかどうかを決定することもできます。

重要! {/b}パラメータルールを設定してから、パラメータルールタイプが無効になるAPI定義タイプを変更すると、無効なパラメータルールタイプが [任意(Any)]に変更され、警告メッセージがリストの下に表示されます。

パラメータルールを追加するには:

1. [パラメータルール(Parameter Rules)]を選択します。
2. [追加(Add)]をクリックします。
   [パラメータルール(Parameter Rules)]ダイアログボックスが開きます。
3. [パラメータルール名(Parameter Rule Name)]ボックスに、ルールの名前を入力します。

4. **[パラメータルールタイプ(Parameter Rule Type)]**リストでタイプを選択します。使用可能なオプションはAPIタイプによって異なり、次のオプションが含まれる場合があります。
   - **任意**
   - **Boolean**
   - **Date**
   - **ファイル**
   - **Guid**
   - **Number**
   - **String**

   APIタイプに基づくパラメータルールタイプとその対応関係の詳細については、「"パラメータタイプの一致について" 次のページ」を参照してください。
5. 次の表の説明に従って操作を進めます。

ルールタイプ	**[パラメータルール値(Parameter Rule Value)]**ボックスで実行する操作
任意	任意の値を入力します。
Boolean	「**true**」または「**false**」を入力します。
Date	文字列値を入力するには: • 次の例に示すように、MM/DD/YYYY形式で日付と時刻の文字列を入力します。 `2025年5月10日 11:00 AM` カレンダを使用して日付と時刻を選択するには: a. カレンダアイコン( )をクリックします。 b. 日付と時刻を選択します。 c. **[閉じる(Close)]**をクリックします。
ファイル	a. ...をクリックして参照し、スキャン設定に追加するファイルを探します。 b. **[開く(Open)]**をクリックします。
Guid	GUIDを入力します。
Number	数値を入力します。
String	任意の値を入力します。

6. ODataおよびSwagger (Open API)スキャンの場合は、 [**パラメータルールの場所 (Parameter Rule Location)**]リストで、そのパラメータがある要求内の場所を選択します。オプションは次のとおりです。
   - **任意**
   - **本文(Body)**
   - **ヘッダ**
   - **パス**
   - **クエリ(Query)**
7. オプションで、このパラメータルールを適用する、または適用しない操作を指定するには、 [**特定の操作(Specific Operations)**]を選択し、"包含する特定の操作の定義" ページ178または"除外する特定の操作の定義" ページ178の手順2から5を実行します。
8. オプションで [**パラメータの挿入(Inject Parameter)**]を選択して、定義されたパラメータを要求に含めます。

   重要! {/b} [**パラメータの挿入(Inject Parameter)**]オプションは、SOAP、gRPC、PostmanなどのスキーマベースのAPIでは機能しません。これらのAPIタイプは強制パラメータを受け付けません。GraphQLの場合、 [**パラメータの挿入(Inject Parameter)**]は、プロパティがクエリスキーマ内にある場合にのみ、クエリ操作で機能します。

9. [**OK**]をクリックします。
   ルールが [パラメータルール(Parameter Rules)]リストに追加されます。

パラメータルールの編集

[パラメータルール(Parameter Rules)]リストでルールを編集するには:

- 編集するルールのチェックボックスをオンにして、 [**編集(Edit)**]をクリックします。
  [パラメータルール(Parameter Rules)]ダイアログボックスが開きます。このダイアログボックスの使用の詳細については、「"パラメータルールの定義" ページ179」を参照してください。

パラメータルールの削除

[パラメータルール(Parameter Rules)]リストからルールを削除するには:

- 削除するルールのチェックボックスをオンにして、 [**削除(Remove)**]をクリックします。

次に行う作業

監査範囲と徹底性を設定するには、 [**次へ(Next)**]をクリックし、"API監査範囲と徹底性の設定" ページ183に進みます。

パラメータタイプの一致について

次の表に、パラメータルールタイプの対応関係をAPIタイプごとに示します。

OpenText DASTパラメータルールタイプ	対応するもの				
	Open API (Swagger)	OData	GraphQL	gRPC	SOAP
任意	All	All	All	All	All
Boolean	boolean	Edm.Boolean	boolean	bool	boolean
Date	date (Open API 2.0) string (Open API 3.0)[1]	Edm.Date Edm.DateTime Edm.DateTimeOffset Edm.Duration Edm.Time Edm.TimeOfDay	N/A	N/A	date
ファイル	file (Open API 2.0)[2]	Edm.Binary	N/A	bytes	N/A
GUID	N/A	Edm.Guid	N/A	N/A	N/A
Number	number integer	Edm.Byte Edm.Decimal Edm.Double Edm.Int16 Edm.Int32 Edm.Int64 Edm.SByte Edm.Single	int float	double enum fixed32 fixed64 float int32 int64 sfixed32 sfixed64 sint32 sint64 uint32 uint64	base64Binary byte decimal double float hexBinary hexint int integer long signedInt short unsignedByte unsignedInt unsignedLong unsignedShort
String	string	Edm.GeographyCollection Edm.GeographyLineString Edm.GeographyMultiLineString Edm.GeographyMultiPoint Edm.GeographyMultiPolygon Edm.GeographyPoint Edm.GeographyPolygon Edm.GeometryCollection Edm.GeometryLineString Edm.GeometryMultiLineString Edm.GeometryMultiPoint Edm.GeometryMultiPolygon Edm.GeometryPoint	id string	string	string

[1]Open API 3.0の実装は日付文字列フォーマットで修飾されます。
[2]Open API 3.0の実装はバイナリまたはバイト文字列フォーマットで修飾されます。

OpenText DASTパラメータルールタイプ	対応するもの				
	Open API (Swagger)	OData	GraphQL	gRPC	SOAP
		Edm.GeometryPolygon Edm.String			

API監査範囲と徹底性の設定

APIスキャンおよびWebサービススキャンのデフォルトポリシーはAPIポリシーです。**APIスキャンウィザード**の **詳細スキャン設定(Detailed Scan Configuration)**]ページで、別のポリシーを選択し、スキャンの他のオプションを選択できます。複数のポリシーを選択した場合、センサはスキャン中に複数のポリシーを集約します。

APIスキャン用の1つ以上のポリシーの選択

別のポリシーを選択するには:

1. **監査の深度(ポリシー) (Audit Depth (Policy))**]リストで、**API**のトグルを無効の位置にスライドします。
2. 目的のポリシーのトグルを有効の位置にスライドします。
   選択したポリシーが[有効化されたスキャンポリシー(ENABLED SCAN POLICIES)]リストに表示されます。ポリシーの詳細については、「"OpenText DAST ポリシー" ページ509」を参照してください。
3. **次へ(Next)**]をクリックします。

追加のポリシーを選択するには、次の方法を実行します。

1. **監査の深度(ポリシー) (Audit Depth (Policy))**]リストで、使用するポリシーのトグルを有効の位置にスライドします。
   選択したポリシーが[有効化されたスキャンポリシー(ENABLED SCAN POLICIES)]リストに表示されます。ポリシーの詳細については、「"OpenText DAST ポリシー" ページ509」を参照してください。
2. **次へ(Next)**]をクリックします。

次に行う作業

スキャンの詳細を設定するには、 **次へ(Next)**]をクリックし、"APIおよびWebサービススキャンのスキャン詳細の設定" 下に進みます。

APIおよびWebサービススキャンのスキャン詳細の設定

APIスキャンウィザードの **詳細スキャン設定(Detailed Scan Configuration)**]ページで、Web Service Test Designerを起動するかスキャンの他の設定ンを構成できます。

Web Service Test Designerの起動

Webサービススキャンを設定する場合は、Web Service Test Designerを起動して、インポートされたWSDまたはWSDLファイルの意図した動作が正しいかどうかを確認できます。

Web Service Test Designerを起動するには::

1. [**デザイン(Design)**]をクリックします。
   Web Service Test Designerが開き、インポートされたWSDLが表示されます。
2. 必要に応じてファイルを編集します。
   詳細については、Web Service Test Designerのヘルプまたは『*OpenText™ Dynamic Application Security Testingツールガイド*』を参照してください。
3. Web Service Test DesignerでWSDファイルを保存します。
4. "APIスキャンおよびWebサービススキャンの追加の設定" 下に進みます。

APIスキャンおよびWebサービススキャンの追加の設定

必要に応じて、次の表の説明に従って [**設定(Settings)**]セクションで追加設定を選択または設定できます。

目的の作業...	その場合...
スタンドアロンプロキシサーバの使用	[**Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)**]を選択します。 **注記:** このオプションは、スキャンをスケジュールしている場合は使用できません。
スキャン中にOpenText DASTから送信されたすべてのHTTP要求をキャプチャして表示する	[**Traffic Monitorを有効にする(Enable Traffic Monitor)**]を選択します。
既存のスキャンから抑制された検出事項をインポートする	1. [**抑制された検出事項のインポート(Import Suppressed Findings)**]を選択します。 2. [**スキャンの選択(select scans)**]をクリックします。 [スキャンを選択して、抑制された検出事項をインポートする(Select a Scan to Import Suppressed Findings)]ダイアログが開きます。 3. 現在スキャンしている同じサイトからの、抑制された検出事項を含むスキャンを1つ以上選択します。

目的の作業...	その場合...
	4. [OK]をクリックします。
抑制された検出事項ファイルから抑制された検出事項をインポートする	1. [抑制された検出事項のインポート(Import Suppressed Findings)]を選択します。 2. [ファイルの選択(select file)]をクリックします。 標準のWindowsファイル選択ダイアログボックスが開きます。 3. インポートするファイルを選択し、[開く(Open)]をクリックします。 4. 必要に応じて、ステップ1と2を繰り返して追加のファイルを選択します。
許可ホストを追加する	1. [許可ホストの追加(Add Allowed Hosts)]セクションで[追加(Add)]をクリックします。 2. [許可ホストの指定(Specify Allowed Host)]ダイアログボックスで、URL(またはURLを表す正規表現)を入力します。 **注記:** URLを指定する場合は、プロトコル指定子(http://やhttps://など)を含めないでください。 3. 許可ホストの正規表現を入力した場合は、[正規表現を使用する(Use Regular Expression)]を選択します。 **ヒント:** 正規表現の作成のヒントについては、  ([許可ホスト(Allowed Host)]ボックスの右側)をクリックします。 4. [OK]をクリックします。 URLが[許可ホスト(Allowed Hosts)]リストに追加されます。

次に行う作業

設定の保存、スキャンの実行、スキャンのスケジュールを行うには、[次へ(Next)]をクリックして"設定の保存またはAPIスキャンの開始" 次のページに進みます。

設定の保存またはAPIスキャンの開始

APIスキャンウィザードの **[その後の作業(Congratulations)]**ページでは、設定を保存するか、設定を使用してスキャンを実行できます。

設定の保存

このスキャンを再度実行する予定の場合は、設定をXMLファイルに保存できます。

設定を保存するには:

- **[保存(Save)]**ハイパーリンクをクリックして、ファイルに名前を付けて保存します。
  APIスキャンウィザードでスキャンを開始するときに、 **[設定(Settings)]**(ウィンドウ下部にある)をクリックしてこの設定ファイルをロードできます。

スキャンの開始

設定を使用してスキャンを開始するには:

- **[スキャン(Scan)]**をクリックします。

wi.exeを使用したAPIのスキャン

コマンドラインインタフェース(CLI)からwi.exeを使用して次のAPIタイプをスキャンできます。

- GraphQL
- gRPC

  注記: SOCKSプロキシを使用するWindows上のOpenText DASTはgRPC APIをスキャンできません。
- OData
- SOAP
- Swagger

コマンドでは、サービスの定義ファイルまたはエンドポイントを指すことができます。必要に応じて、認証やプロキシ設定などの追加情報を含めたスキャン環境設定ファイルを作成し、コマンドでその設定ファイルを指すことができます。

プロセスの概要

次の表で、wi.exeを使用してAPIをスキャンするプロセスについて説明します。

ステージ	説明
1.	必要に応じて、APIスキャン環境設定ファイル(JSON)を作成します。詳細につい

ステージ	説明
	ては、「"APIスキャン環境設定ファイルについて" 次のページ」を参照してください。 **ヒント:** 認証、プロキシ、URLとは異なるサービスパスなどのカスタム設定が必要ない場合は、スキャン環境設定ファイルを作成する必要がありません。
2.	CLIを開いて、次の例に示すように、`wi.exe`を使用し、オプション`-api`を指定して、スキャンを実行します。 `wi.exe -xd -api SOAP -u "D:\Development\soapConfig.json"` `wi.exe -api GraphQL -u "http://localhost:5013/graphql" -tm -pc "C:\ProgramData\hp\HP WebInspect\Policies\<custom_policy>.policy"` wi.exeのオプションの詳細については、"wi.exeの使用" ページ329を参照してください。
3.	結果を表示するには、OpenText DASTでスキャンを開きます。スキャン名は`API Assessment <API_Type> <Service_URL>`になります。 **注記:** スキャンが完了するまでは、OpenText DASTでスキャンを表示できません。

定義ファイルに関する重要な考慮事項

スキャン設定ファイルを設定したり、CLIコマンドを作成したりする場合は、次の点を考慮してください。

- OpenText DASTは、CLIコマンドで指定されたURLから定義を生成しようとします。また、APIエンドポイントは同じURLであるもののファイル名が含まれていないと見なします。サービスが定義ファイルと同じ場所にある場合(GraphQLでは一般にこれが当てはまる)は、URLを指定すると役に立ちます。ただし、SOAPとgRPCの場合は、定義が別の場所にある可能性があります。
- GraphQL APIでは、スキャンのスキーマコンテンツをダウンロードするために、イントロスペクションが有効になっている必要があります。イントロスペクションを有効にしない場合は、完全なスキーマクエリ(イントロスペクションクエリ)を実行できます。その後で、JSONファイル内のAPIDefinition設定に応答を配置できます。

推奨事項

wi.exeを使用してAPIスキャンを実行する場合は、次の推奨事項に従ってください。

- APIスキャンでは、使用されるポリシーに関係なく、API検出エンジンが使用されます。ただし、ポリシーでAPI検出チェックが有効になっていない場合は、それが検出事項に表示されません。そのため、OpenTextでは、API検出チェックが有効になっているポリシーを使用する

ようにお勧めします。

- OpenTextでは、スキャンを一度に1回だけ実行することをお勧めします。SQL Expressを使用する場合は特に、サイトのサイズによっては、同時(または並行)スキャンを実行すると、OpenText DASTホスト上のRAM、CPU、およびディスクリソースの使用率が高くなる場合があります。

APIスキャン環境設定ファイルについて

次の表で、JSON環境設定ファイルで使用可能なパラメータについて説明します。

重要! {/b}JSONファイルでは二重引用符内のすべての二重引用符をエスケープする必要があります。エスケープするには、各引用符の前に1つのバックスラッシュ(\)を付けます。例:

```
"Setting": "Value \"Value Text Inside Quotes\""
```

パラメータ	説明
`APIDefinition`	特定のURLであるサービス定義の場所を指します。各APIサービスでは、次のように、特定のタイプのファイルが使用されます。 • SOAPでは、WSDL (Web Service Definition Language)ファイルが使用されます。 • gRPCでは、`.proto`ファイルが使用されます。 • GraphQLでは、`introspection-query.graphql`などのイントロスペクションクエリまたはエンドポイントが使用されます。 `APIDefinition`をURLにする必要はありません。URLにすることも、API定義の内容にすることもできます。たとえば、ローカルマシン上の定義ファイルへのファイルパスを指定できます。定義の場所がHTTP URLまたはディレクトリパスを指している場合は、OpenText DASTがコンテンツをダウンロードして、URLまたはパスをそのコンテンツに置き換えます。その結果、定義ファイル全体が設定内に保存されます。
`Type`	スキャン対象のAPIサービスのタイプを示します。可能性がある値は次のとおりです。 • `GraphQL` • `gRPC` • `SOAP`
`Schemes`	サービスで使用されるプロトコル(`http`と`https`のどちらかまたはその両方)を示します。

パラメータ	説明
	重要! {/b}スキームは、1つまたは複数の値が使用されるかどうかに関係なく、JSON配列として定義する必要があります。配列の例を次に示します。 `[ "http" ],[ "http", "https" ]`
`Host`	サービスが実行されているホスト名またはURLを示します。 **ヒント:** これはほとんどの場合、API定義のルートURLと同じです。
`APIVersion`	主にSOAPに使用され、特定のバージョンによる操作のフィルタリングが可能です。可能性がある値は次のとおりです。 • `Legacy` - サポートされている最下位バージョンに対してフィルタが適用されます。 • `Mixed` - 使用できるものに応じて、`Legacy`と`Newest`の組み合わせを使用します。 • `Newest` - デフォルト設定です。最新バージョンに対してフィルタが適用されます。
`ServicePath`	サービスへのディレクトリパスを指定します。
`AuthProviders`	オプションで、トランスポートBearerトークンなどの認証タイプを識別します。`AuthProviders`パラメータの詳細については"API AuthProvidersの設定について" ページ193を参照してください。
`Proxy`	オプションで、プロキシ設定を指定します。`Proxy`には、次のパラメータが必要です。 • `Host` - プロキシが実行されているホスト名またはURLを示します • `Port` - プロキシサーバで使用されるポート番号を示します • `UserName` - オプションで、プロキシサーバにアクセスするためのユーザアカウントを識別します • `Password` - オプションで、ユーザプロファイルのパスワードを指定します 重要! {/b}現時点でサポートされているのは基本認証のみです。

パラメータ	説明
preferredContentType	オプションで、要求ペイロードの優先コンテンツタイプを設定します。 操作でサポートされているコンテンツタイプのリストに preferredContentTypeがある場合、生成される要求ペイロードは、そのタイプになります。ない場合は、操作で最初に一覧指定されているコンテンツタイプが使用されます。
excludeOperations	オプションで、出力から除外する操作IDの拒否リストを定義します。操作IDの配列で表現します。 **例:** `[ 'operation1', 'operation2', 'operationN' ]`
includeOperations	オプションで、出力に含める操作IDの許可リストを定義します。操作IDの配列で表現します。 **例:** `[ 'operation1', 'operation2', 'operationN' ]`
parameterRules	オプションで、デフォルト値が適切ではない場合、またはパラメータがAPI定義で定義されていない場合に、パラメータの特定の値を定義します。 **例:** API定義で定義されていない権限付与ヘッダなどのパラメータは、要求ごとに挿入する必要があります。 このプロパティは、「parameterRule」オブジェクトのアレイで表現されます。「parameterRule」オブジェクトについては、"パラメータルールオブジェクトについて" 次のページを参照してください。

JSON環境設定ファイルのサンプルについては、"APIスキャン環境設定ファイルのサンプル" ページ198を参照してください。

パラメータルールオブジェクトについて

次の表で、「parameterRule」オブジェクトについて説明します。

オブジェクト	必須/オプション	説明
`name`	Required	照合するパラメータ名を指定します。 名前の競合が発生した場合にプロパティを上書きするには、API定義のオブジェクトタイプをパラメータ名の前に指定し、「*<type_of_object>/<parameter_name>*」の形式でスラッシュで区切ります。 たとえば、「name」という名前のパラメータと、同じく「name」という名前のネストされたパラメータがある場合は、次に示すように、ネストされたパラメータのオブジェクトタイプを指定する必要があります。 `{ name : 'name', value : 'Romeo', location : 'body', type : 'string', includeOperations : [ 'addPet'] }, { name : 'tag/name', value : 'Juliet', location : 'body', type : 'string', includeOperations : [ 'addPet'] },`
`value`	Required	置き換えまたは挿入するパラメータ値を指定します。
`location`	オプション	照合するパラメータの場所を指定します。オプションは次のとおりです。 • `'body'` • `'header'` • `'path'` • `'query'` • `'any'`

オブジェクト	必須/オプション	説明
		デフォルトは「any」で、すべての場所に一致します。
type	オプション	照合するパラメータタイプを指定します。オプションは次のとおりです。 • 'number' • 'boolean' • 'string' • 'file' (以下のfilenameを参照してください)。 • 'date' • 'any' デフォルトは「any」で、すべてのタイプに一致します。
filename	オプション	一致するマルチパートまたはフォームファイル項目のファイル名属性を置換します。typeが'file'の場合のみ有効です。
inject	オプション	パラメータ値を置換します。オプションは次のとおりです。 • true - 一致する名前またはタイプが検出されたかどうかに関係なく、指定した場所にパラメータが挿入されます。 • false -指定した名前、場所、およびタイプに一致するパラメータ値のみを置換します。 デフォルトはfalseです。
base64Decode	オプション	'value'がbase64エンコードバイナリデータかどうかを指定します。オプションは次のとおりです。 • true - 'value'はbase64エンコードバイナリデータと見なされ、生成されるHTTP要求に挿入される際にバイトの配列にデコードされます。 • false - 'value'はbase64エンコードバイナリデータではありません。 デフォルトはfalseです。
includeOperations	オプション	このパラメータルールをリスト内の操作IDに適用しま

オブジェクト	必須/オプション	説明
		す。操作IDのアレイで表現します。 **例:** `[ 'operation1', 'operation2', 'operationN' ]`
`excludeOperations`	オプション	このパラメータルールをリスト内の操作IDに適用しません。操作IDのアレイで表現します。 **例:** `[ 'operation1', 'operation2', 'operationN' ]`

API AuthProvidersの設定について

環境設定ファイルで、AuthProvidersの次のカテゴリを設定できます。

- クライアント証明書(Client certificate)
- メッセージベース(Message-based)
- トランスポート(権限付与、基本、Bearer、ダイジェスト、NTLM) (Transport (Authorization, Basic, Bearer, Digest, and NTLM))
- トランスポートカスタムヘッダ(Transport custom header)

必要に応じてAuthProviderタイプを組み合わせて、ネットワークとAPI定義ファイルまたはAPIエンドポイントにアクセスできます。ただし、トランスポートカスタムヘッダを除き、各カテゴリのAuthProviderは1つしか使用できません。

クライアント証明書(Client certificate)

次の表で、スキャン環境設定ファイルで設定できるAuthProvidersのクライアント証明書カテゴリについて説明します。

Type	説明
`TRANSPORT_CERTIFICATE`	認証に証明書設定を使用します。`TRANSPORT_CERTIFICATE`には、次のパラメータが必要です。 • `ClientCertificate` - 証明書情報を指定します。次のパラメータを含みます。 • `Data` -パスワードで保護されたBase 64エンコード`*.pfx`証明書を指定します。

Type	説明
	ヒント: 次のopensslコマンドを使用して、Dataの値として使用する証明書のテキストバージョンを取得できます。 `openssl base64 -A -in d:\dump\cert.pfx -out d:\dump\cert.pfx.base64` • Password -証明書のパスワードを指定します。 次のサンプルは、これらのパラメータの構文を示しています。 `{ "Type": "TRANSPORT_CERTIFICATE", "ClientCertificate": { "Data": "<64-base_encoded_certificate>", "Password": "<Password>" }, }`

メッセージベース(Message based)

次の表で、スキャン環境設定ファイルで設定できるAuthProvidersのメッセージベースカテゴリについて説明します。

Type	説明
MESSAGE_CERTIFICATE	認証に証明書設定を使用します。MESSAGE_CERTIFICATEには、次のパラメータが必要です。 • ClientCertificate - 証明書情報を指定します。クライアントのために行い、次のパラメータを含みます。 • Data -パスワードで保護されたBase 64エンコード*.pfx証明書を指定します。 **ヒント:** 次のopensslコマンドを使用して、Dataの値として使用する証明書のテキストバージョンを取得できます。 `openssl base64 -A -in d:\dump\cert.pfx -out d:\dump\cert.pfx.base64` • Password -証明書のパスワードを指定します。 • ServerCertificate -証明書情報の指定をサーバのために行い、次のパラメータを含みます。 • Data -パスワードで保護されたBase 64エンコード*.pfx証明書を指定します。 次のサンプルは、これらのパラメータの構文を示しています。 `{ "Type": "MESSAGE_CERTIFICATE", "ClientCertificate": { "Data":`

Type	説明
	`"<64-base_encoded_certificate>" "Password": "<Password>" }, "ServerCertificate": { "Data": "<64-base_encoded_certificate>" } }`
MESSAGE_USERNAMETOKEN	ユーザ名とトークンを使用して、SOAPサービスに対する認証を行います。MESSAGE_USERNAMETOKENには、次のパラメータが必要です。 • Username -資格情報をSOAPサービスへのアクセスに使用するユーザ名を指定します。 • Password -ユーザ名のパスワードを指定します。 • UsernameToken - SOAPのにメッセージレベルの認証を提供し、次のパラメータを含みます。 • Type -トークンのタイプを指定します。オプションはTEXTとHASHです。 • TimeStamp -オプションで、usernameTokenの作成日時と失効日時を示します。TimeStampは、Created、Full、またはNoneを受け入れます。 • IncludeNonce - nonceが有効かどうかを示します。nonceはHASHトークンに必要です。これは、サーバがハッシュを再計算して、クライアントから送信されたデータと比較できるようにするためです。オプションはtrueまたはfalseです。 • WSAddressing - オプションで、SOAPサービスが使用するWebサービスアドレス指定(WS-Addressing)スキーマバージョンを識別します。オプションは、NONE、WSA_0408、WSA_0508です。 • To - オプションで、Webサービスホストの URLを識別します。 **注記:** SOAPサービスは、ロードバランサまたはリバースプロキシによって公開される場合があります。この設定により、センサが内部Webサービスのホスト名に関する正しい情報を取得できなくなる場合があります。To URL上書きにより、WS Addressingに正しいアドレスを指定できます。 次のサンプルは、これらのパラメータの構文を示しています。 `{ "Type": "MESSAGE_USERNAMETOKEN", "Username": "<username>", "Password": "<password>", "UsernameToken": { "Type": "TEXT", "TimeStamp": "Created", "IncludeNonce": true }, "WSAddressing": { "Version": "WSA_0408", "To": "http://webservice/wcf/service.svc/CustomSoapEndpoint" } }`

トランスポート(Transport)

次の表で、スキャン環境設定ファイルで設定できるAuthProvidersのトランスポートカテゴリについて説明します。

Type	説明
TRANSPORT_AUTHORIZATION	認証トークンを使用します。TRANSPORT_AUTHORIZATIONには、次のパラメータが含まれます。 • Name - トークン名を示します。 • Value - トークン値を指定します。 次のサンプルは、これらのパラメータの構文を示しています。 `{ "Type": "TRANSPORT_AUTHORIZATION", "Name": "<token_name>", "Value": "<token_value>", }` TRANSPORT_AUTHORIZATIONでは、Fetchパラメータを使用することもできます。詳細については、「"トークン値のフェッチ" ページ198」を参照してください。
TRANSPORT_BASIC	認証に基本設定を使用します。TRANSPORT_BASICには、次のパラメータが必要です。 • Username - 資格情報をAPIサービスへのアクセスに使用するユーザ名を指定します。 • Password - ユーザ名のパスワードを指定します。 次のサンプルは、これらのパラメータの構文を示しています。 `{ "Type": "TRANSPORT_BASIC", "Username": "<UserName>", "Password": "<Password>", }`
TRANSPORT_BEARER	認証にBearerトークン設定を使用します。TRANSPORT_BEARERには、次のパラメータが必要です。 • Value - JSONトークン(通常はログインフォームへの応答からのもの)を指定します。 • Header - オプションで、カスタムヘッダ名を識別します。 次のサンプルは、このパラメータの構文を示しています。 `{ "Type": "TRANSPORT_BEARER", "Value":"<token>" }` TRANSPORT_BEARERでは、Fetchパラメータを使用することもできます。詳細につ

Type	説明
	いては、「"トークン値のフェッチ" 次のページ」を参照してください。
TRANSPORT_DIGEST	ダイジェスト認証を使用します。TRANSPORT_DIGESTには、次のパラメータが必要です。 • Username - 資格情報をAPIサービスへのアクセスに使用する、ホスト名とユーザ名の組み合わせを指定します。 • Password -ユーザ名のパスワードを指定します。 次のサンプルは、これらのパラメータの構文を示しています。 `{ "Type": "TRANSPORT_DIGEST", "Username": "<host_name>\\<username>", "Password": "<password>", }`
TRANSPORT_NTLM	認証にNTLM設定を使用します。TRANSPORT_NTLMには、次のパラメータが必要です。 • Username - 資格情報をAPIサービスへのアクセスに使用する、ホスト名とユーザ名の組み合わせを指定します。 • Password -ユーザ名のパスワードを指定します。 次のサンプルは、これらのパラメータの構文を示しています。 `{ "Type": "TRANSPORT_NTLM", "Username": "<host_name>\\<username>", "Password": "<password>", }`

トランスポートカスタム(Transport custom)

次の表で、スキャン環境設定ファイルで設定できるAuthProvidersのトランスポートカスタムカテゴリについて説明します。

重要! {/b}OpenTextでは、同じHTTPヘッダ名を使用して複数のカスタムヘッダを設定しないことをお勧めします。

Type	説明
TRANSPORT_CUSTOM_HEADER	このタイプを使用して、複数のカスタムヘッダを設定できます。TRANSPORT_CUSTOM_HEADERには、次のパラメータが含まれます。 • Header - HTTPヘッダ名を識別します。ヘッダは固有でなければならず、Authorizationにすることはできません。 • Name - オプションで、ヘッダ値のプレフィクス名を指定します。 • Value - ヘッダ値を指定します。

Type	説明
	次のサンプルは、これらのパラメータの構文を示しています。 `{ "Type": "TRANSPORT_CUSTOM_HEADER", "Header": "<header_name>", "Name": "<prefix_header_name>", "Value": "<header_value>" }` 次の例は、カスタム認証トークンを使用して"X-MyCustomAuth: CustomToken value" HTTPカスタムヘッダを設定するための構文を示しています。 `{ "Type": "TRANSPORT_CUSTOM_HEADER", "Header": "X-MyCustomAuth", "Name": "CustomToken", "Value": "<token_value>" }`

トークン値のフェッチ

TRANSPORT_AUTHORIZATIONおよびTRANSPORT_BEARER AuthProviderはフェッチパラメータを使用できます。これは、ワークフローマクロから応答を生成し、正規表現を使用してトークンをキャプチャして、状態の適用に使用できるようにします。Fetchは、次のパラメータを受け入れます。

- Macro - マクロのBase 64エンコードテキストキャプチャをインポートします。マクロには、ログインWebフォームと、JSON Webトークンが指定された応答を含める必要があります。

  ヒント: マクロファイルをテキストエディタで開いてから、テキストをコピーしてMacroフィールドに貼り付けることができます。

- Search - カスタム正規表現を使用したトークン値のフェッチを可能にします。応答内で正規表現との一致が検出されると、その値がフェッチされ、Bearerトークンとして使用されます。正規表現に括弧が含まれている場合は、括弧内の値が抽出され、Bearerトークンとして使用されます。括弧内の最初の値だけが使用されます。

  重要! {/b}Searchパラメータは、JSONファイル内でMacroパラメータの後ろに指定する必要があります。

- IsolatedState - オプションで、フェッチマクロの再生の適用方法を決定します。trueに設定すると、各スキャンスレッドは独自のフェッチマクロを再生し、そのスレッドにBearerトークン値を適用します。falseに設定すると、すべてのスキャンスレッドに対して1つのフェッチマクロのみを再生し、単一の共有Bearerトークン値がすべてのスレッドに適用されます。デフォルト設定はfalseです。

次のサンプルは、これらのパラメータの構文を示しています。

```
{ "Type": "TRANSPORT_BEARER", "Fetch": { "Macro": "<base-64_encoded_text>", "Search": "<regular_expression>", "IsolatedState": "true" }, }
```

APIスキャン環境設定ファイルのサンプル

以降の段落では、API環境設定ファイルのJSONサンプルを示します。

GraphQL環境設定ファイルのサンプル

次のサンプルは、認証なしのGraphQL環境設定ファイルを示しています。

```
{ "APIDefinition": "http://<ip_address>:<port>/graphql/", "Schemes": [
"http" ], "Host": "<ip_address>:<port>", "ServicePath": "/graphql/",
"Type": "GraphQL", "Proxy": { "Host": "<ip_address>", "Port": "<port>",
"UserName": "<username>", "Password": "<password>" } }
```

gRPC環境設定ファイルのサンプル

次のサンプルは、TRANSPORT_BEARER AuthProviderタイプを、明示的に設定されたトークン値とともに使用するgRPC環境設定ファイルを示しています。

```
{ "APIDefinition": "https://<host_name>:<port>/protos/client.proto",
"Type": "gRPC", "Schemes": [ "https" ], "Host": "<host_name>:<port>",
"ServicePath" : "/", "AuthProviders": [ { "Type": "TRANSPORT_BEARER",
"Value":"<token>" } ] }
```

SOAP環境設定ファイルのサンプル

次のサンプルは、TRANSPORT_NTLMおよびMESSAGE_USERNAMETOKEN AuthProviderタイプを使用するSOAP環境設定ファイルを示しています。

```
{ "APIDefinition": "https://<host_name>:<port>/wcf/service.svc?singleWsdl",
"Type": "SOAP", "Schemes": [ "https" ], "Host": "<host_name>:<port>",
"APIVersion": "Mixed", "AuthProviders": [ { "Type": "TRANSPORT_NTLM",
"Username": "<host_name>\\<username>", "Password": "<password>", }, {
"Type": "MESSAGE_USERNAMETOKEN", "Username": "<username>", "Password":
"<password>", "UsernameToken": { "Type": "TEXT", "TimeStamp": "Created",
"IncludeNonce": true },  } ] }
```

基本スキャンの実行(Webサイトスキャン)

このウィンドウおよびそれ以降のウィンドウにデフォルトで表示されるオプションは、OpenText DASTのデフォルト設定から抽出されます。行う変更はすべて、このスキャンにのみ使用されます。ウィンドウ下部の **設定(デフォルト)(Settings (Default))**]をクリックしてOpenText DASTの全設定にアクセスする場合も、選択する内容はすべて一時的なものになります。デフォルト設定を変更するには、 **編集(Edit)**]メニューから **デフォルトのスキャン設定(Default Scan Settings)**]を選択する必要があります。詳細については、「"デフォルトのスキャン設定" ページ 402」を参照してください。

推奨

OpenTextでは、スキャンを一度に1回だけ実行することをお勧めします。SQL Expressを使用する場合は特に、サイトのサイズによっては、同時(または並行)スキャンを実行すると、OpenText DASTホスト上のRAM、CPU、およびディスクリソースの使用率が高くなる場合があります。

基本スキャンのオプションの設定

1. [**スキャン名(Scan Name)**]ボックスに、スキャンの名前または簡単な説明を入力します。
2. 次のいずれかのスキャンモードを選択します。
   - **Web探索のみ(Crawl Only)**: サイトの階層データ構造が完全にマッピングされます。Web探索が完了したら、 [**監査(Audit)**]をクリックしてアプリケーションの脆弱性を評価できます。
   - **Web探索および監査(Crawl and Audit)**: サイトの階層データ構造がマッピングされ、各リソース(ページ)が監査されます。選択したデフォルト設定に応じて、各リソースの検出時またはサイト全体のWeb探索後に監査を実行できます。Web探索および監査の同時実行と順次実行の詳細については、「"Web探索および監査モード(Crawl and audit mode)" ページ403」を参照してください。
   - **監査のみ(Audit Only)**: 選択されているポリシーの手法を適用して脆弱性リスクを判断しますが、Webサイトのweb探索は実行されません。サイト上のリンクをたどることも評価することもありません。
   - **手動(Manual)**: アクセス先として選んだのがアプリケーションのどのセクションであれ、FirefoxによるTruClientを使用してそこに手動で移動できます。OpenText DASTはサイト全体のWeb探索を実行せず、サイト内を手動で移動中に検出したリソースに関する情報のみを記録します。この機能は、Webフォームのログオンページからサイトに入る場合、または調査するアプリケーションの個別のサブセットまたは部分を定義する場合に最もよく使用されます。サイト内を移動し終わったら、結果を監査して、記録したサイトのその部分に関連するセキュリティ脆弱性を評価できます。

     注記: スキャンをスケジュールするときには、手動モードは使用できません。
3. [**レンダリングエンジン(Rendering Engine)**]ドロップダウンリストからレンダリングエンジンを選択します。選択するレンダリングエンジンによって、スキャンの設定時に新しいマクロの記録または既存のマクロの編集を行うときに開かれるWeb Macro Recorderが決まります。オプションは次のとおりです。
   - **イベントベース(Event-based) (優先)** -このオプションを選択すると、イベントベースのWebマクロレコーダが指定されます。これはTruClientとFirefoxテクノロジを使用します。
   - **セッションベース(Session-based)** -このオプションを選択すると、セッションベースのWeb Macro Recorderが指定されます。これはInternet Explorerブラウザテクノロジを使用します。

注記: 手動モードでレンダリングエンジンを設定することはできません。手動モードでは、TruClientとFirefoxテクノロジを使用します。

4. 次のいずれかのスキャンタイプを選択します。
   - **標準スキャン(Standard Scan)**: ターゲットURLから始めて、自動分析を実行します。これは標準的なスキャン開始方法です。
   - **手動スキャン(Manual Scan)**: (ステップモードとも呼ばれます)アクセス先として選んだのがアプリケーションのどのセクションであれ、FirefoxによるTruClientを使用してそこに手動で移動できます。この選択項目は、手動スキャンモードを選択している場合にのみ表示されます。
   - **リストドリブンスキャン(List-Driven Scan)**: スキャン対象URLのリストを使用してスキャンを実行します。各URLは完全修飾であり、プロトコル(http://またはhttps://など)が含まれている必要があります。カンマ区切りリスト形式または1行に1つずつURLを指定したテキストファイルを使用できます。
     - リストをインポートするには、[**インポート(Import)**]をクリックします。
     - Site List Editorを使用してリストを作成または編集するには、[**管理(Manage)**]をクリックします。詳細については、「"Site List Editorの使用" ページ215」を参照してください。
   - **ワークフロードリブンスキャン(Workflow-Driven Scan)**: 以前に記録したマクロに含まれているURLのみを監査し、監査中に検出されたハイパーリンクはたどりません。ログアウト署名は不要です。この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。複数のマクロを選択すると、すべてのマクロが同一スキャンに含まれます。`.webmacro`ファイル、Burp Proxyキャプチャ、または`.har`ファイルを使用できます。詳細については、「"ワークフローマクロの選択" ページ281」を参照してください。

     重要! {/b}ログインマクロをワークフローマクロと起動マクロのどちらかまたはその両方と組み合わせて使用する場合は、すべてのマクロが同じタイプでなければなりません。すべてが`.webmacro`ファイル、すべてがBurp Proxyキャプチャ、またはすべてが`.har`ファイルのいずれかです。同じスキャンで異なる種類のマクロを使用することはできません。

5. 次の表に従って続行します。

選択する項目...	行う手順...
標準スキャン(Standard Scan)	a. [**開始URL(Start URL)**]ボックスで、調査するサイトの完全なURLまたはIPアドレスを入力または選択します。 URLを入力する場合は、正確に入力する必要があります。たとえば「MYCOMPANY.COM」と入力すると、OpenText DASTはWWW.MYCOMPANY.COMなどのバリエーションはスキャンしません([**許可ホスト(Allowed Hosts)**]設定で代替URLを指定して

選択する項目...	行う手順...
	いる場合を除く)。 無効なURLまたはIPアドレスを指定すると、エラーが発生します。階層ツリー内の特定の位置からスキャンを実行する場合は、スキャンの開始点(http://www.myserver.com/myapplication/など)を追加します。 IPアドレスによるスキャンでは、(相対パスではなく)完全修飾URLを使用するリンクは追跡しません。 OpenText DASTでは、IPV4 (Internet Protocolバージョン4)とIPV6 (Internet Protocolバージョン6)の両方がサポートされています。IPV6アドレスは括弧で囲む必要があります。詳細については、「"Internet Protocolバージョン6" ページ401」を参照してください。 b. [フォルダに限定(Restrict to folder)]を選択した場合は、ドロップダウンリストから選択したエリアにスキャン範囲を制限できます。次の選択肢があります。 ◦ **ディレクトリのみ(Directory only)** - OpenText DASTは、指定されたURLだけをWeb探索または監査(またはその両方)します。たとえば、このオプションを選択してwww.mycompany/one/two/というURLを指定すると、OpenText DASTは「two」ディレクトリのみを評価します。 ◦ **ディレクトリおよびサブディレクトリ(Directory and subdirectories)** - OpenText DASTは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも上位のディレクトリにはアクセスしません。 ◦ **ディレクトリおよび親ディレクトリ(Directory and parent directories)** - OpenText DASTは、指定されたURLでWeb探索または監査(またはその両方)を開始しますが、ディレクトリツリーでそれよりも下位のディレクトリにはアクセスしません。 [フォルダに限定(Restrict to folder)]スキャンオプションの制限については、"「フォルダに限定」に関する制限" ページ227を参照してください。
手動スキャン(Manual Scan)	**開始URL**を入力し、必要に応じて**[フォルダに限定(Restrict to folder)]**を選択します。前に説明した「標準スキャン」を参照してください。

選択する項目...	行う手順...
	注記: 手動モードでレンダリングエンジンを設定することはできません。手動モードでは、TruClientとFirefoxテクノロジを使用します。
リストドリブンスキャン(List-Driven Scan)	次のいずれかを実行します。 • [**インポート(Import)**]をクリックし、スキャンするURLのリストを含むテキストファイルまたはXMLファイルを選択します。 • [**管理(Manage)**]をクリックし、URLのリストを作成または変更します。
ワークフロードリブンスキャン(Workflow-Driven Scan)	次のいずれかを実行します。 • [**管理(Manage)**]をクリックして、マクロを選択、編集、記録、インポート、エクスポート、または削除します。 • [**記録(Record)**]をクリックしてマクロを作成します。 **注記:** 複数のマクロを1つのスキャンに含めることができます。

6. [**次へ(Next)**]をクリックします。
[認証と接続(Authentication and Connectivity)]ページが表示されます。

ネットワーク認証と接続の設定

[認証と接続(Authentication and Connectivity)]ページでは、プロキシ、ネットワーク認証、サイト認証の設定を構成できます。

プロキシ設定の構成

プロキシサーバを介してターゲットWebサイトへのアクセスを設定するには、次の手順を実行します。

1. [**ネットワークプロキシ(Network Proxy)**]を選択します。
2. [**プロキシプロファイル(Proxy Profile)**]リストからプロファイルを選択します。プロファイルは次のとおりです。
   - **自動検出(Auto Detect)**: WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、これを使用してブラウザのWebプロキシ設定を行います。

- **[システムプロキシを使用(Use System Proxy)]**: ローカルマシンからプロキシサーバ情報をインポートします。
- **[PACファイルを使用(Use PAC File)]**: PAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。このオプションを選択した場合は、**[編集(Edit)]**をクリックしてPACの場所(URL)を入力します。詳細については、「"プロキシプロファイルの設定" ページ216」を参照してください。
- **[明示的なプロキシ設定を使用(Use Explicit Proxy Settings)]**: プロキシサーバ設定を指定します。このオプションを選択した場合は、**[編集(Edit)]**をクリックしてプロキシ情報を入力します。詳細については、「"プロキシプロファイルの設定" ページ216」を参照してください。
- **[Mozilla Firefoxを使用(Use Mozilla Firefox)]**: Firefoxからプロキシサーバ情報をインポートします。

注記: ブラウザのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が**[プロキシーを使用しない]**に設定されている場合、またはWindowsの**[LANにプロキシサーバを使用する]**設定が選択されていない場合、プロキシサーバは使用されません。

ネットワーク認証の設定

ターゲットWebサイトのネットワーク認証を設定するには:

1. **[ネットワーク認証(Network Authentication)]**を選択します。
2. 認証メソッドを選択し、ネットワーク資格情報を入力します。認証メソッドは次のとおりです。
   - ADFS CBT
   - **自動**
   - **基本**
   - **ダイジェスト**
   - Kerberos
   - **ネゴシエート(Negotiate)**
   - NT LAN Manager (NTLM)
   - OAuth 2.0 Bearer
3. 次のいずれかを実行します。
   - OAuth 2.0 Bearer以外のすべての認証方法では、**[ユーザ名(User name)]**ボックスにユーザIDを入力し、**[パスワード(Password)]**ボックスにユーザのパスワードを入力します。
   - OAuth 2.0 Bearerメソッドの場合は、**[設定(Configure)]**をクリックし、"OAuth 2.0のBearer資格情報の設定" ページ447の手順に従います。

クライアント証明書の使用

Webサイトのクライアント証明書を使用するには、**[設定(Settings)] > [認証(Authentication)]**をクリックし、次の手順に従って続行します。

1. **[クライアント証明書(Client Certificates)]**エリアで、**[有効化(Enable)]**チェックボックスをオンにします。
2. **[選択(Select)]**をクリックします。
   [クライアント証明書(Client Certificates)]ウィンドウが開きます。
3. 次のいずれかを実行します。
   - コンピュータにとってローカルで、コンピュータ上のすべてのユーザにとってグローバルな証明書を使用するには、**[ローカルマシン(Local Machine)]**を選択します。
   - コンピュータ上のユーザアカウントにとってローカルな証明書を使用するには、**[現在のユーザ(Current User)]**を選択します。

     注記: 共通アクセスカード(CAC)リーダで使用される証明書はユーザ証明書であり、**[現在のユーザ(Current User)]**に保管されます。
4. 次のいずれかを実行します。
   - 「個人」(「マイ」)証明書ストアから証明書を選択するには、ドロップダウンリストから**[マイ(My)]**を選択します。
   - 信頼されたルート証明書を選択するには、ドロップダウンリストで**[ルート(Root)]**を選択します。
5. Webサイトでは、CACリーダまたはパスワードで保護された証明書を使用していますか。
   - 「はい」の場合は、次の手順を実行します。
     i. **[証明書(Certificate)]**リストから、「(Protected)」というプレフィクスが付いた証明書を選択します。
     選択した証明書に関する情報と**[パスワード/PIN (Password/PIN)]**フィールドが**[証明書情報(Certificate Information)]**エリアに表示されます。
     ii. パスワードまたはPINが必要な場合は、**[パスワード/PIN (Password/PIN)]**フィールドに入力します。

     注記: パスワードまたはPINが必要であるのに、ここで入力していないと、スキャン中にWindowsの**[セキュリティ]**ウィンドウのプロンプトが表示されるたびに、パスワードまたはPINを入力することが必要になります。

     重要! {/b}デフォルトでは、OpenText DASTはOpenSSLを使用します。OpenSSLではなく特定のSSL/TLSプロトコルを使用している場合、スキャン設定のProfiler部分はパスワードで保護されている証明書で動作しない場合があります。

iii. [テスト(Test)]をクリックします。
正しいパスワードまたはPINを入力した場合は、成功メッセージが表示されます。

- 「いいえ」の場合は、[証明書(Certificate)]リストから証明書を選択します。
選択した証明書に関する情報が[証明書(Certificate)]リストの下に表示されます。

6. [OK]をクリックします。

複合スキャン設定での証明書の更新

複合スキャン設定には、暗号化された証明書データを格納するBINファイルが含まれています。複合スキャン設定でクライアント証明書を置換または更新する必要がある場合は、更新したPFXファイルまたはP12ファイルを、複合設定のZIPファイル内のcertificatesディレクトリに配置できます。OpenText DASTで設定を開くと、まずPFXファイルとP12ファイルの有無がチェックされます。どちらも存在しない場合、BINファイルが復号化されて使用されます。複合設定の詳細については、"アプリケーション設定: 全般" ページ480を参照してください。

クライアント証明書を置換または更新するには、次の手順を実行します。

1. 複合スキャン設定のZIP内のcertificatesディレクトリで、暗号化されたBINファイルを見つけます。ファイル名はGUIDで、次のようになります。

```
<your-scansettings.zip>\certificates\0b627638-efda-4d01-a83e-80ee3a79b4cf.bin
```

注記: Windowsにおけるデフォルトの設定ファイルの場所は、`C:\ProgramData\HP\HP WebInspect\Settings\`です。

2. 更新したPFXファイルまたはP12ファイルを同じディレクトリに配置します。
3. PFXファイルまたはP12ファイルの名前をBINファイルと同じ名前に変更します。前の例を使用すると、ファイル名は次のようになります。

```
0b627638-efda-4d01-a83e-80ee3a79b4cf.pfx
```

– または –

```
0b627638-efda-4d01-a83e-80ee3a79b4cf.p12
```

重要! {/b}必ず元のファイル拡張子を保持してください。

4. 必要に応じて、暗号化された証明書を設定に保持する場合は、設定を再度保存します。BINファイルには、更新されたPFX証明書またはP12証明書が反映されます。PFX証明書またはP12証明書がZIPから削除されます。

ヒント: PFX証明書およびP12証明書では、多くの場合、パスワードが必要です。次のいずれかのオプションを使用して、設定のパスワードを指定します。

- PFX証明書またはP12証明書を作成するときに空のパスワードを設定し、それを設定のZIPファイルに配置します。
- PFX証明書またはP12証明書のパスワードを保持し、`settings.json`ファイルを編集し

て、次のようにCertificatePinの値としてパスワードを設定します。

```
"CertificatePin": "<password>"
```

サイト認証の設定

サイト認証を設定するには:

1. ターゲットサイトにログインできる1つ以上のユーザ名とパスワードが含まれている記録済みマクロを使用するには、 **[サイト認証(Site Authentication)]**を選択します。そのマクロには「ログアウト条件」も含まれている必要があります。これは、予期せぬログアウトが発生した場合にそれを示し、OpenText DASTがこのマクロを再実行して再びログインできるようにするためのものです。

   Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、OpenText DASTで基本スキャンを設定するときにも、それらの値はマスクされます。

   ログインマクロを使用するスキャンの **[スキャン設定: 認証(Scan Settings: Authentication)]**で **[マクロ検証を有効にする(Enable macro validation)]**が選択されている場合、OpenText DASTはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

   注記: マクロテストは、2要素認証を含むマクロに対してはサポートされていません。

   重要! {/b}2要素認証を含むマクロを使用する場合は、スキャンを開始する前に、2要素認証アプリケーションの設定を行う必要があります。詳細については、「"アプリケーション設定: 2要素認証" ページ491」を参照してください。

   次の表に従って続行します。

目的...	その場合...
事前に記録されたWeb Macro Recorderマクロを使用する	省略記号ボタン(...)をクリックしてマクロを選択します。 マクロを選択した後で、Web Macro Recorderを使用してマクロを変更する場合は、 **[編集(Edit)]**をクリックします。 **ヒント:** マクロ名を消去するには、 **[サイト認証(Site Authentication)]**チェックボックスをオフにします。
新しいマクロを作成する	**[記録(Record)]**をクリックします。 Web Macro Recorderが開きます。

目的...	その場合...
	注記: Web Macro Recorderの使用法の詳細については、Web Macro Recorderのヘルプを参照してください。
ログインマクロを自動的に作成する **注記:** 権限のエスカレーションおよびマルチユーザログインスキャン用のログインマクロは自動的に作成できません。	a. [**ログインマクロの自動生成(Auto-gen Login Macro)**]を選択します。 b. [**ユーザ名(Username)**]フィールドにユーザ名を入力します。 c. [**パスワード(Password)**]フィールドにパスワードを入力します。 オプションで、[**テスト(Test)**]をクリックして、ログインフォームの検索、マクロの生成、マクロ検証テストの実行を行ってから、スキャンウィザードの次のステージに進みます。完了前に検証テストをキャンセルする必要がある場合は、[**キャンセル(Cancel)**]をクリックします。 マクロが無効で、アプリケーションへのログインが失敗すると、エラーメッセージが表示されます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

2. [**次へ(Next)**]をクリックします。
   [Web検索範囲と徹底性(Crawl Coverage and Thoroughness)]ページが表示されます。

Web検索範囲と徹底性の設定

効率と徹底性のバランスを設定するには、次の手順を行います。

1. Oracle Application Development Framework FacesのコンポーネントまたはIBM WebSphere Portalのいずれかを使用して構築されたアプリケーションの設定を最適化するには、[**フレームワーク(Framework)**]を選択し、[**スキャンの最適化対象(Optimize scan for)**]リストから[**Oracle ADF Faces**]または[**WebSphere Portal**]を選択します。Fortifyでは、他の設定オーバーレイを開発し、スマートアップデートを通じて提供することがあります。
   WebSphere Portalのスキャンの詳細については、「"WebSphere Portalに関するFAQ" ページ326」を参照してください。
2. [**Web探索範囲(CrawlCoverage)**]スライダを使用して、Web探索プログラム設定を指定します。

このスライダが使用可能かどうかは、選択したスキャンモードによって決まります。このスライダに関連付けられているラベルも、選択した内容に応じて異なります。このスライダが使用可能な場合、スライダではWeb探索の4つの位置から1つを選択できます。それぞれの位置は、特定の設定コレクションを表しており、次のラベルで示されています。

徹底(Thorough)

徹底Web探索とは、次の設定を使用する自動Web探索です。

- 冗長ページ検出(Redundant Page Detection): **オフ(OFF)**
- 単一URL最大ヒット数(Maximum Single URL Hits): **10**
- Webフォーム最大送信数(Maximum Web Form Submissions): **7**
- ページあたりの最大スクリプトイベント数(Maximum Script Events Per Page): **2000**
- セッションあたりの許容ダイナミックフォーム数(Number of Dynamic Forms Allowed Per Session): **無制限(Unlimited)**
- ヒット数にパラメータを含める(Include Parameters In Hit Count): **True**

デフォルト(Default)

デフォルトのWeb探索とは、次の(デフォルトスキャン)設定を使用する自動Web探索です。

- 冗長ページ検出(Redundant Page Detection): **オフ(OFF)**
- 単一URL最大ヒット数(Maximum Single URL Hits): **5**
- Webフォーム最大送信数(Maximum Web Form Submissions): **3**
- ページあたりの最大スクリプトイベント数(Maximum Script Events Per Page): **1000**
- セッションあたりの許容ダイナミックフォーム数(Number of Dynamic Forms Allowed Per Session): **無制限(Unlimited)**
- ヒット数にパラメータを含める(Include Parameters In Hit Count): **True**

中程度(Moderate)

標準的なWeb探索とは、次の設定を使用する自動Web探索です。

- 冗長ページ検出(Redundant Page Detection): **オフ(OFF)**
- 単一URL最大ヒット数(Maximum Single URL Hits): **5**
- Webフォーム最大送信数(Maximum Web Form Submissions): **2**
- ページあたりの最大スクリプトイベント数(Maximum Script Events Per Page): **300**
- セッションあたりの許容ダイナミックフォーム数(Number of Dynamic Forms Allowed Per Session): **1**
- ヒット数にパラメータを含める(Include Parameters In Hit Count): **False**

クイック(Quick)

クイックWeb探索では、次の設定が使用されます。

- 冗長ページ検出(Redundant Page Detection): **オン(ON)**
- 単一URL最大ヒット数(Maximum Single URL Hits): **3**
- Webフォーム最大送信数(Maximum Web Form Submissions): **1**
- ページあたりの最大スクリプトイベント数(Maximum Script Events Per Page): **100**
- セッションあたりの許容ダイナミックフォーム数(Number of Dynamic Forms Allowed Per Session): **0**
- ヒット数にパラメータを含める(Include Parameters In Hit Count): **False**

設定(Settings)]をクリックして(詳細設定(Advanced Settings)]ダイアログボックスを開き)、設定を変更して、スライダに4つある位置の1つで定められている設定と対立した場合、スライダには カスタマイズされたカバレッジ設定(Customized Coverage Settings)]という名前の5つ目の位置が作成されます。

3. **次へ(Next)**]をクリックします。
   [監査範囲と徹底性(Audit Coverage and Thoroughness)]ページが表示されます。

監査範囲と徹底性の設定

デフォルトの選択とは異なるポリシーを選択するか、より適切な範囲のために複数のポリシーを設定するか、または特定のタイプの脆弱性にさらに重点を置く必要があります。たとえば、標準ポリシーを使用してスキャンを実行するものの、SQLインジェクションにさらに重点を置きたい場合は、スキャンの標準ポリシーとSQLインジェクションポリシーを選択できます。センサは、選択したすべてのポリシーをスキャン中に集約します。

別のポリシーを選択するには:

1. **監査の深さ(ポリシー)**]リストで、選択したポリシーのトグルを無効の位置にスライドします。
2. 目的のポリシーのトグルを有効の位置にスライドします。
   選択したポリシーが[有効化されたスキャンポリシー(ENABLED SCAN POLICIES)]リストに表示されます。ポリシーの詳細については、「"OpenText DAST ポリシー" ページ509」を参照してください。
3. **次へ(Next)**]をクリックします。
   [スキャン詳細設定(Detailed Scan Configuration)]ページが表示されます。 プロファイラを自動的に実行する(Run Profiler Automatically)]オプションが選択されている場合は、「プロファイルサイト...(Profiling Site...)」メッセージが表示されます。

追加のポリシーを選択するには、次の方法を実行します。

1. **監査の深度(ポリシー) (Audit Depth (Policy))**]リストで、使用するポリシーのトグルを有効の位置にスライドします。

選択したポリシーが[有効化されたスキャンポリシー(ENABLED SCAN POLICIES)]リストに表示されます。ポリシーの詳細については、「"OpenText DAST ポリシー" ページ509」を参照してください。

2. **[次へ(Next)]**をクリックします。

[スキャン詳細設定(Detailed Scan Configuration)]ページが表示されます。 **[プロファイラを自動的に実行する(Run Profiler Automatically)]**オプションが選択されている場合は、「プロファイルサイト...(Profiling Site...)」メッセージが表示されます。

Profilerの使用

[スキャン詳細設定(Detailed Scan Configuration)]ページで、OpenText DASTは、ターゲットWebサイトの事前テストを実行し、特定の設定を変更すべきかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Server Profilerは、サイトに入るために権限付与が必要であるものの、有効なユーザ名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Server Profilerの提案に従って、続行する前に必要な情報を設定することができます。

同様に、設定では、OpenText DASTが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにOpenText DAST設定を変更することを推奨します。

このページにアクセスするたびにProfilerを起動するには、 **[Profilerを自動的に実行する(Run Profiler Automatically)]**を選択します。

Profilerを手動で起動するには、 **[プロファイル(Profile)]**をクリックします。詳細については、「"Server Profiler" ページ283」を参照してください。

結果が **[設定(Settings)]**セクションに表示されます。

Profilerが変更を推奨しない場合は、スキャンウィザードに「設定の変更は推奨されません。現在のスキャン設定はこのサイトに最適です。(No settings changes are recommended. Your current scan settings are optimal for this site.)」というメッセージが表示されます。

プロファイラの推奨設定の選択

[スキャン詳細設定(Detailed Scan Configuration)]ページの[設定(Settings)]領域で、提案された設定を受け入れるか拒否するか選択できます。

Profilerを実行しない場合でも、いくつかのオプションが表示されることがあります。以下のものが含まれます。

- Webフォームに自動入力する(「"Webフォームの自動入力(Auto fill Web forms)" 下」を参照してください)
- 許可されているホストを追加します(「"許可ホストを追加する" 下」を参照してください)
- 確認された非表示の結果を再使用する(「"識別された抑制された検出事項を再利用する" 次のページ」を参照してください)
- サンプルマクロを適用する(「"サンプルマクロ" 次のページ」を参照してください)
- トラフィック分析(「"トラフィック分析" ページ214」を参照してください)

プロファイラの提案を受諾または拒否します。

1. 提案を受諾または拒否します。
   - 設定を受け入れるには、対応するチェックボックスをオンにします。
   - 拒否するには、対応するチェックボックスをオフにします。
2. 必要に応じて、要求された情報を入力します。
3. **[次へ(Next)]**をクリックします。
   [おめでとうございます(Congratulations)]ウィンドウが表示されます。

Webフォームの自動入力(Auto fill Web forms)

OpenText DASTがターゲットサイトのスキャン中に検出されるフォームの入力コントロールの値を送信するようにするには、**[Web探索時のWebフォームの自動入力(Auto-fill Web forms during crawl)]**を選択します。OpenText DASTは、事前パッケージ化されたデフォルトファイル、またはWeb Form Editorを使用して作成したファイルから値を抽出します。以下を実行できます。

- 省略記号ボタン...をクリックして、ファイルを見つけてロードします。
- **[編集(Edit)]**をクリックして、選択したファイル(またはデフォルト値)をWeb Form Editorで編集します。
- **[作成(Create)]**をクリックしてWeb Form Editorを開き、ファイルを作成します。

許可ホストを追加する

[許可ホスト(Allowed Host)]設定は、Web探索して監査するドメインを追加する場合に使用します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここに追加します。詳細については、「"スキャン設定:許可ホスト" ページ421」を参照してください。

許可するドメインを追加するには:

1. **[追加(Add)]**をクリックします。
2. **[許可ホストの指定(Specify Allowed Host)]**ウィンドウで、URL(またはURLを表す正規表現)を入力し、**[OK]**をクリックします。

許可ホストの追加または編集の詳細については、「"許可ホストの指定" ページ217」を参照してください。

識別された抑制された検出事項を再利用する

以前のスキャンで誤検出に変更された、または無視された脆弱性をインポートできます。これらの誤検出または無視された項目が現在のスキャンで検出された脆弱性と一致する場合、その脆弱性は誤検出に変更されるか、無視されます。既存のスキャンまたは抑制された検出事項ファイルから、抑制された検出事項をインポートできます。詳細については、「"抑制された検出事項" ページ83」を参照してください。

識別された抑制された検出事項を再利用するには:

1. **[抑制された検出事項のインポート(Import Suppressed Findings)]**を選択します。
2. 次の表に従って続行します。

使用する情報...	**その場合...**
既存のスキャン	a. **[スキャンの選択(select scans)]**をクリックします。 [スキャンを選択して、抑制された検出事項をインポートする(Select a Scan to Import Suppressed Findings)]ダイアログが開きます。 b. 現在スキャンしている同じサイトからの、抑制された検出事項を含むスキャンを1つ以上選択します。 c. **[OK]**をクリックします。
抑制された検出事項ファイル	a. **[ファイルの選択(select file)]**をクリックします。 標準のWindowsファイル選択ダイアログボックスが開きます。 b. インポートするファイルを選択し、**[開く(Open)]**をクリックします。 c. 必要に応じて、ステップaとbを繰り返して追加のファイルを選択します。

注記: スキャンのスケジューリング時やエンタープライズスキャンの実行時には、抑制された検出事項をインポートできません。

サンプルマクロ

OpenText DASTのサンプルバンキングアプリケーション(zero.webappsecurity.com)では、Webフォームログインが使用されています。このサイトをスキャンする場合は、**[サンプルマクロの適用(Apply sample macro)]**を選択して、ログインスクリプトを含むサンプルマクロを実行します。

トラフィック分析

Web Proxyツールを使用してOpenText DASTにより発行されたHTTP要求とターゲットサーバから返された応答を検査するには、 **[Web Proxyの起動およびWeb Proxy経由でのトラフィックの送信(Launch and Direct Traffic through Web Proxy)]**を選択します。

OpenText DASTはWebサイトのスキャン中に、Webサイトの階層構造を明らかにするセッションと、脆弱性が検出されたセッションのみをナビゲーションペインに表示します。ただし **[Traffic Monitorを有効にする(Enable Traffic Monitor)]**を選択すると、OpenText DASTでは **[Traffic Monitor]**ボタンが **[スキャン情報(Scan Info)]**パネルに追加されます。これにより、OpenText DASTが送信した各HTTP要求と、サーバから受信した関連HTTP応答を表示して確認できます。

その後の作業(Congratulations)

[設定(Congratulations)]ウィンドウに表示される内容は、選択内容と設定によって異なります。

Fortify WebInspect Enterpriseスキャンテンプレートへのアップロード

エンタープライズサーバ(Fortify WebInspect Enterprise)に接続している場合、このスキャンの設定をFortify WebInspect Enterpriseに送信できます。これにより、スキャンテンプレートが作成されます。ただし、スキャンテンプレートを作成できる役割が自分に割り当てられている必要があります。

設定の保存

このスキャン用に設定した内容を保存しておき、将来のスキャンで設定を再利用できます。

レポートの生成

スキャンをスケジュールしている場合は、スキャン完了時にレポートを生成することをOpenText DASTに対して指示できます。

1. **[レポートの生成(Generate Reports)]**を選択します。
2. **[レポートの選択(Select reports)]**ハイパーリンクをクリックします。
3. (オプション) **[お気に入り(Favorites)]**リストからレポートを選択します。
   「お気に入り」は、1つ以上のレポートとその関連パラメータの単なる名前付きコレクションです。レポートおよびパラメータを選択した後でお気に入りを作成するには、 **[お気に入り(Favorites)]**リストをクリックして、 **[お気に入りに追加(Add to favorites)]**を選択します。
4. 1つ以上のレポートを選択します。

5. 要求できるパラメータの情報を入力します。必須のパラメータは赤で囲まれます。
6. [次へ(Next)]をクリックします。
7. [ファイル名の自動生成(Automatically Generate Filename)]を選択すると、レポートファイルの名前は*<reportname> <date/time>.<extension>*の形式になります。例えば、pdf形式でコンプライアンスレポートを作成し、そのレポートが4月5日の6:30に生成される場合、ファイル名は「Compliance Report 04_05_2022 06_30.pdf」になります。これは、反復スキャンの場合に便利です。

   レポートは、生成されるレポート用にアプリケーション設定で指定されたディレクトリに書き込まれます。
8. [ファイル名の自動生成(Automatically Generate Filename)]を選択しなかった場合は、[ファイル名(Filename)]ボックスにファイルの名前を入力します。
9. [エクスポート形式(Export Format)]リストからレポート形式を選択します。
10. 複数のレポートを選択した場合は、[レポートを1つに集約(Aggregate reports into one report)]を選択することで、すべてのレポートを1つに結合できます。
11. レポートに使用するヘッダとフッタを定義するテンプレートを選択し、必要に応じて要求されたパラメータを指定します。
12. [完了(Finished)]をクリックします。
13. [スケジュール(Schedule)]をクリックします。

Site List Editorの使用

基本スキャンウィザードを使用してリストドリブンスキャンを実行する場合、Site List Editorを使用してURLのリストを作成または編集できます。

Site List Editorにアクセスするには:

- 基本スキャンウィザードの[リストドリブンスキャン(List-Driven Scan)]オプションの下にある[管理(Manage)]をクリックします。

個々のURLを手動で追加するには:

1. [追加(Add)]をクリックします。
2. スキャンに追加するURLを入力します。プロトコルを指定しない場合、エディタによってURLの先頭に「http://」が追加されます。
3. 必要に応じて、操作を繰り返します。

テキストファイルまたはXMLファイルに指定されているURLを追加するには:

1. [インポート(Import)]をクリックします。
2. 標準のファイル選択ウィンドウを使用して、ファイルを見つけて[開く(Open)]をクリックします。
3. 必要に応じて、操作を繰り返します。

注記: エディタでは重複はチェックされません。2つのリストをインポートし、両方のリストに同じURLが含まれている場合、そのURLは2回リストに含められます。

> また、各URLにはプロトコル(http://またはhttps://など)が含まれている必要があります。手動での入力とは異なり、インポートされたURLの先頭にはプロトコルは自動的に追加されません。

エントリを編集するには:

- URLをクリックします。

エントリを削除するには:

- URLを選択し、 **削除(Delete)**]をクリックします。

参照情報

"基本スキャンの実行(Webサイトスキャン)" ページ199

プロキシプロファイルの設定

基本スキャンを実行し、PAC (Proxy Automatic Configuration)ファイルからプロキシ設定を使用するか、明示的なプロキシ設定(Explicit Proxy Settings)を指定する場合は、 [プロキシプロファイル(Proxy Profile)]ウィンドウでプロキシオプションを設定できます。

[プロキシプロファイル(Proxy Profile)]ウィンドウにアクセスするには:

- 基本スキャンウィザードの [ネットワークプロキシ(Network Proxy)]にある **編集(Edit)**]をクリックします。

PACファイルを使用してプロキシを設定する(Configure proxy using a PAC file)

プロキシ設定をPAC (Proxy Automatic Configuration)ファイルからロードします。 [**URL**]ボックスにファイルの場所を指定します。

プロキシを明示的に設定する(Explicitly configure proxy)

要求された情報を入力することによって、プロキシを設定します。

1. [**サーバ(Server)**]ボックスにプロキシサーバのURLまたはIPアドレスを入力し、続いて([**ポート(Port)**]ボックスに)ポート番号(8080など)を入力します。
2. [**タイプ(Type)**]リストから、プロキシサーバ経由のTCPトラフィックを処理するプロトコルを選択します。
   - **SOCKS4**
   - **SOCKS5**
   - **標準(Standard)**

3. 認証が必要な場合は、 **認証(Authentication)**]リストからタイプを選択します。
   - **自動**
   - **基本**
   - **ダイジェスト**
   - Kerberos
   - **ネゴシエート(Negotiate)**
   - NT LAN Manager (NTLM)

   重要! {/b}Socks4プロキシサーバは認証に対応しません。認証が必要なSocksプロキシサーバを使用する場合は、Socks5プロキシを使用する必要があります。
4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。
5. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、 **プロキシをバイパスするサイト(Bypass Proxy For)**]ボックスにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。

参照情報

"基本スキャンの実行(Webサイトスキャン)" ページ199

許可ホストの指定

Web探索するドメインを追加するには許可ホストを指定します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここに追加します。たとえば、「WIexample.com」をスキャンする場合、「WIexample2.com」と「WIexample3.com」がWebプレゼンスの一部であり、かつそれらをWeb探索または監査に含めたいのであれば、それらのドメインをここに追加する必要があります。

この機能を使用して、指定したテキストが名前に含まれているドメインをスキャンすることもできます。たとえば、スキャンターゲットとして「www.myco.com」を指定し、許可ホストとして「myco」と入力したとします。OpenText DASTは、ターゲットサイトをスキャンして「myco」を含むURLへのリンクを検出すると、そのリンクをたどってそのサイトのサーバをスキャンします。この処理は、すべてのリンク先のサイトがスキャンされるまで繰り返されます。この仮説例では、OpenText DASTによって次のドメインがスキャンされます。

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

ポート番号を指定する場合は、許可ホストが完全に一致する必要があることに注意してください。

許可ホストの指定

許可ホストを指定(追加)するには:

1. 基本スキャンウィザードの [詳細スキャン設定(Detailed Scan Configuration)] ページで、**[追加(Add)]** をクリックします。
2. [許可ホストの指定(Specify Allowed Host)] ダイアログボックスで、URL (またはURLを表す正規表現)を入力します。

   注記: URLを指定する場合は、プロトコル指定子(http://やhttps://など)を含めないでください。

3. 許可ホストの正規表現を入力した場合は、 **[正規表現を使用する(Use Regular Expression)]** を選択します。

   正規表現の作成のヒントについては、  (**[許可ホスト(Allowed Host)]** ボックスの右側)をクリックします。
4. [OK] をクリックします。

許可ホストの編集

許可ホストを編集するには:

1. 基本スキャンウィザードの [詳細スキャン設定(Detailed Scan Configuration)] ページでホストを選択し、 **[編集(Edit)]** をクリックします。
2. [許可ホストの編集(Edit Allowed Host)] ダイアログボックスで、URL (またはURLを表す正規表現)を編集します。

   注記: URLを編集する場合は、プロトコル指定子(http://やhttps://など)を含めないでください。

3. [OK] をクリックします。

参照情報

"基本スキャンの実行(Webサイトスキャン)" ページ199

マルチユーザログインスキャン

ユーザごとに1つのアクティブログインセッションのみを許可するアプリケーションでは、マルチスレッドスキャンができません。複数のログインが行われると、スレッドどうしによって相互の状態が無効にされ、スキャン時間が遅くなります。

この問題を解決するには、ログインマクロに記録された資格情報をパラメータに変換し、同じアプリケーション特権を持つ複数のログインアカウントを使用します。 [スキャンの設定: 認証(Scan Settings: Authentication)] ウィンドウの [マルチユーザログイン(Multi-user Login)] オプ

ションを使用すると、ログインマクロ内のユーザ名とパスワードをパラメータ化し、スキャンで使用する複数のユーザ名とパスワードのペアを定義できます。2要素認証が必要な場合は、電話番号、電子メール、および電子メールパスワードをパラメータ化することもできます。

このアプローチを使用すると、複数のスレッドでスキャンを実行できます。スレッドごとにログインセッションが異なるため、スキャン時間が短縮されます。

作業を開始する前に

マルチユーザログインスキャンを設定するには、パラメータ化されたログインマクロを使用する必要があります。詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章の「パラメータの使用」トピックを参照してください。

既知の制限事項

マルチユーザログイン機能には、次の既知の制限事項が適用されます。

- この機能を使用する場合、OpenText DASTはログイン関連の複数のSecurebaseチェックを検出しません。
- この機能は現在、共有リクエスタスレッドのみをサポートしています。Web探索と監査の別個のスレッドでデフォルトのスキャン設定を使用することは、サポートされていません。詳細については、「"スキャン設定:リクエスタ" ページ414」を参照してください。
- ログインしている複数のユーザ間でスキャンの作業が等しく分散されません。たとえば、1人の設定済みユーザがスキャンアクティビティの最大75%を使用し、他のすべてのユーザが残りの25%のスキャンアクティビティに割り当てられる場合があります。

プロセスの概要

マルチユーザログインスキャンを設定するには、次の表で説明されているプロセスを使用します。

ステージ	説明
1.	共有リクエスタを目的のユーザ数に設定します。詳細については、「"スキャン設定:リクエスタ" ページ414」を参照してください。 重要! {/b}共有リクエスタスレッドの数が、設定されたユーザの数を超えないようにする必要があります。有効なユーザを持たないリクエスタスレッドでは、スキャンの実行時間が長くなります。複数のユーザを設定する場合は、最初のユーザとして、パラメータ化されたマクロ内のオリジナルのユーザ名とパスワードをカウントすることを忘れないでください。
2.	パラメータ化されたユーザ名とパスワードを含むログインマクロを使用してください。2要素認証が必要な場合は、必要に応じて、電話番号、電子メール、および電

ステージ	説明
	子メールパスワードをパラメータ化します。詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Webマクロレコーダ」の章の「パラメータの使用」トピックを参照してください。
3.	基本スキャンウィザードまたはガイド付きスキャンウィザードで、「"マルチユーザログインスキャンの設定" 下」の説明に従って、マルチユーザのチェックボックスを有効にします。
4.	「"資格情報の追加" 次のページ」の説明に従って、複数のユーザの資格情報を追加します。
5.	通常どおりにスキャンウィザードを進め、スキャンを実行します。

マルチユーザログインスキャンの設定

マルチユーザログインスキャンを設定するには:

1. 次のいずれかを実行します。
   - 基本スキャンウィザードでは、 **編集(Edit)] > 現在のスキャン設定(Current Scan Settings)]** をクリックします。次に、 **[スキャン設定(Scan Settings)] > 認証(Authentication)]** を選択します。
   - ガイド付きスキャンウィザードでは、リボンの **詳細設定(Advanced)]** をクリックし、 **[スキャン設定(Scan Settings)] > 認証(Authentication)]** を選択します。
2. **[フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)]** チェックボックスを選択します。

   重要! {/b}マルチユーザログインオプションを有効にするには、このチェックボックスをオンにする必要があります。

3. 次のいずれかを実行します。
   - 新しいマクロを記録するには、通常どおり **記録(Record)]** をクリックしてログインマクロを記録します。

     注記: ガイド付きスキャンの場合は、ログインマクロを記録するための別のステージが含まれているため、 **記録(Record)]** ボタンを使用できません。マクロを記録した後、資格情報をパラメータ化する必要があります。

   - 既存のマクロを使用するには、 **[..]** をクリックして、すでにパラメータ化された資格情報を持つ保存済みマクロを選択します。
4. **[マルチユーザログイン(Multi-user Login)]** チェックボックスをオンにします。

注記: スキャンを実行する前に [マルチユーザログイン(Multi-user Login)] チェックボックスをオフにすると、スキャン中に追加の資格情報が使用されません。OpenText DASTは、ログインマクロに記録されたオリジナルの資格情報のみを使用します。

5. 次の手順に従います。
   - ユーザの資格情報を追加するには、「"資格情報の追加" 下」に進みます。
   - ユーザの資格情報を編集するには、「"資格情報の編集" 次のページ」に進みます。
   - ユーザの資格情報を削除するには、「"資格情報の削除" 次のページ」に進みます。
6. ユーザの資格情報を設定した後、通常どおりにスキャンウィザードを進め、スキャンを実行します。

資格情報の追加

資格情報を追加するには:

1. [**マルチユーザログイン(Multi-user Login)**] で、 [**追加(Add)**] をクリックします。
   [マルチユーザ資格情報入力(Multi-user Credential Input)] ダイアログボックスが表示されます。
2. [**ユーザ名(Username)**] ボックスに、ユーザ名を入力します。
3. [**パスワード(Password)**] ボックスに、対応するパスワードを入力します。
4. 2要素認証が必要な場合は、必要に応じて次の表の説明に従って操作を進めます。

この資格情報ボックスの場合...	これを入力...
電話番号(Phone Number)	ユーザ名に対応する電話番号(SMS応答を受信するため)
Email	ユーザ名に対応する電子メールアドレス(電子メール応答を受信するため)
電子メールパスワード(Email Password)	電子メールアドレスのパスワード(電子メール応答を受信するため)

5. [**OK**] をクリックします。
6. 追加するユーザログインごとにステップ1-5を繰り返します。

重要! {/b}共有リクエスタスレッドの数が、設定されたユーザの数を超えないようにする必要があります。有効なユーザを持たないリクエスタスレッドでは、スキャンの実行時間が長くなります。複数のユーザを設定する場合は、最初のユーザとして、パラメータ化されたマクロ内のオリジナルのユーザ名とパスワードをカウントすることを忘れないでください。詳細については、「"スキャン設定:リクエスタ" ページ414」を参照してください。

資格情報の編集

資格情報を編集するには:

1. [**マルチユーザログイン(Multi-user Login)**]で、テーブル内のエントリを選択し、 [**編集(Edit)**]をクリックします。
   [マルチユーザ資格情報入力(Multi-user Credential Input)]ダイアログボックスが表示されます。
2. 必要に応じて資格情報を編集します。
3. [**OK**]をクリックします。

資格情報の削除

資格情報を削除するには:

1. [マルチユーザログイン(Multi-user Login)]で、削除するテーブル内のエントリを選択します。
2. [**削除(Delete)**]をクリックします。

2要素認証の使用

2要素認証は、「自分が知っているもの」の要素として定義される通常のパスワードを、次のいずれかを使用して補います。

- SMSまたは電子メールで送信されるワンタイムパスコード(OTP)など、自分が所有しているもの
- 指紋、顔、または網膜など、自分の体の一部

この2つ目の認証要素はセキュリティを向上させますが、それを実装するWebアプリケーションの自動スキャンを行う際の複雑さが増大します。

OpenTextエンジニアは、OpenText DASTとイベントベースのWebマクロレコーダで、2要素認証の「自分が所有しているもの」の要素を自動化する方法とプロセスを開発しました。

2要素認証を使用するスキャンの仕組み

OpenText DASTにはNode.jsサーバが含まれており、これを設定して、アプリケーションサーバから受信するSMSおよび電子メールの応答をコントロールセンターで処理できます。また、SMS応答をコントロールセンターに転送するモバイルアプリケーションもあります。コントロールセンターは応答をキューに登録し、認証で必要になったら、適切なTruClientブラウザに転送します。

推奨

テスト用電話とテスト用電子メールアドレスのみを使用することを強くお勧めします。個人情報保護の観点から、個人の電話やメールアドレスは使用しないでください。

既知の制限事項

次の既知の制限事項は、2要素認証機能に適用されます。

- IMAPおよびPOP3サーバがサポートされています。ただし、固有のID一覧(UIDL)をサポートするPOP3サーバのみがサポートされます。
- 現在、電子メールを使用した2要素認証を備えたログインマクロは、IMAPまたはPOP3の基本認証方式のみをサポートしています。
- 現在、サポートされているのはAndroid携帯電話のみです。
- 携帯電話では、OpenText DASTがインストールされているサブネットと同じサブネット内のWi-Fiに接続する必要があります。

Gmailアカウントに関する考慮事項

Gmailアカウントに関連する次の点にご注意ください。

- Gmailアカウントの設定には、通常モードと最新モードが含まれます。Gmailアカウントを使用していて新しい受信メールで問題が発生した場合、最新モードを使用することでこの問題が解決する可能性があります。最新モードを有効にするには、POP3アカウント設定でアカウント名を次の形式で設定します。

  `recent:<email_address@gmail.com>`
- セキュリティの観点から、Googleは「Googleでログイン」を使用してGmailをユーザのGoogleアカウントに関連付けます。ユーザが作成したパスワードは受け付けません。Gmailアカウントを使用する場合、Googleアプリのパスワードを作成して使用する必要があります。詳細については、アプリパスワードの作成と使用に関するGoogleアカウントのマニュアルを参照してください。

プロセスについて

次の表では、2要素認証を使用してスキャンを実行するプロセスについて説明します。

ステージ	説明
1.	2要素認証のOpenText DASTアプリケーション設定で、次の操作を実行します。 • 2要素認証コントロールセンターを設定する • モバイルアプリケーションを設定する(SMS応答を使用する場合)

ステージ	説明
	詳細については、「"アプリケーション設定:2要素認証" ページ491」を参照してください。
2.	イベントベースのWebマクロレコーダでログインマクロを記録して、次のように変更します。 1. [2要素認証(Two-factor authentication)]グループステップを追加および設定します。 **注記:** [SMS]または[電子メール(email)]の応答のグループステップを設定する必要があります。グループステップには、[2FAを待機する(Wait for 2FA)]ステップが含まれます。このステップも設定する必要があります。 2. オプションで、ユーザ名、パスワード、電話番号、電子メール、および電子メールパスワードのパラメータを作成します。2要素認証のパラメータを使用すると、マルチユーザログインスキャンを実行できます。 3. [2FAを待機する(Wait for 2FA)]ステップを設定します。 4. [汎用オブジェクトアクション(Generic Object Action)]ステップを追加し、それを[タイプ(Type)]ステップとして設定します。 5. [汎用オブジェクトアクション(Generic Object Action)]ステップを追加し、それを[クリック(Click)]ステップとして設定します。 詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』を参照してください。
3.	Web Macro Recorderで、ログインマクロを再生します。
4.	オプションで、マルチユーザログインスキャンを実行する場合は、[スキャン設定:認証(Scan Settings: Authentication)]ウィンドウに、ユーザ名、パスワード、電話番号、電子メール、および電子メールパスワードの資格情報を追加します。詳細については、「"マルチユーザログインスキャン" ページ218」および「"スキャン設定:認証" ページ440」を参照してください。
5.	OpenText DASTで、マクロを使用してスキャンを実行します。

対話型スキャン

CAPTCHAなど、特定のタイプのアンチスキャンテクノロジを使用するWebアプリケーションでは、OpenText DASTで対話型のスキャン設定が必要になります。対話型スキャンでは、認証のためのユーザ入力を求めるブラウザウィンドウが表示されます。入力フィールドが検出され

た場合にのみ一時停止する自動対話型スキャンを設定できます。この一時停止は、入力フィールドが検出されたリクエスタスレッドにのみ影響します。残りのスレッドには影響しません。

対話型スキャン設定は、CAPTCHA、RSA IDトークンフィールド、仮想PINパッド、仮想キーボード、およびPINまたは入力がダイナミックで変化する共通アクセスカード(CAC)リーダに対して機能します。

ヒント: スタティックPINでCACリーダを使用するWebサイトでは、CAC証明書を使用するようにスキャンを設定できます。次のいずれかのトピックを参照してください。

- "スキャン設定: 認証" ページ440
- "基本スキャンの実行(Webサイトスキャン)" ページ199
- "ネイティブスキャンテンプレートの使用" ページ147
- "モバイルスキャンテンプレートの使用" ページ130
- "事前定義テンプレートの使用" ページ113

注記: 2要素認証では、対話型スキャンは不要です。2要素認証を使用して、完全に自動化されたスキャンを設定できます。詳細については、「"2要素認証の使用" ページ222」を参照してください。

対話型スキャンの設定

次の表で、対話型スキャンを設定するためのプロセスについて説明します。

ステージ	説明
1.	次のようにWebフォーム入力ファイルを準備します。 1. Web Form Editorツールにフィールド名を記録するか入力します。 2. フォーム名を右クリックし、 **[対話型としてマークする(Mark As Interactive)]** を選択します。 3. Webフォーム入力ファイルを保存します。 詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Web Form Editor」の章を参照してください。
2.	ダイナミックPINを必要とするクライアント側証明書を使用していますか。 • 「はい」の場合は、クライアント側の証明書がブラウザの証明書リストに一覧表示されていないことを確認するか、手動でインポートします。たとえば、Microsoft Edgeの **[プライバシー、検索、サービス]** 設定の **[証明書の管理]** ダイアログボックスにアクセスします。 この操作により、証明書が一時的にWindowsの証明書ストアにロードされます。

ステージ	説明
	注記: ハードウェアトークンに接続し、要求されたPINを入力すると、これが自動的に行われます。 • 「いいえ」の場合は、ステージ3にスキップします。
3.	対話型スキャンモードのスキャン方法を次のように設定します。 1. [スキャン設定: 方法(Scan Settings: Method)]ウィンドウを開きます。 2. [**Webフォームの自動入力(Auto fill web forms)**]フィールドで、ステージ1で作成したWebフォーム入力ファイルを指定します。 3. [**スキャン中にWebフォーム値の入力を要求する(対話型モード)(Prompt for web form values during scan (interactive mode))**]チェックボックスをオンにします。 4. [**タグ付けされた入力に対してのみプロンプトを表示する(Only prompt for tagged inputs)**]チェックボックスをオンにします。 **注記:** この最後のチェックボックスが選択されていない場合は、サイトで検出されたすべての入力に対してプロンプトが表示されます。
4.	動的なパスワードまたはPINを必要とするクライアント側証明書を使用していますか。 • 「はい」の場合は、次の手順に従って、クライアント側証明書を使用するように認証を設定します。 a. [スキャン設定: 認証(Scan Settings: Authentication)]ウィンドウを開きます。 b. [クライアント証明書(Client Certificates)]エリアで [**有効にする**]チェックボックスをオンにして、ユーザの証明書を参照して選択します。 OpenText DASTでは、この証明書がタイムアウトして、要求されたパスワードまたはPINの入力に失敗するまで、またはハードウェアトークンが削除され、Windowsで証明書がストアから削除されるまで、この証明書が使用されます。 • 「いいえ」の場合は、ステージ5にスキップします。
5.	スキャン設定を保存して、それらの設定をOpenText DASTスキャンで使用します。 重要! {/b}必要に応じて、ポップアップを確認してフォームの値を入力する必要があります。

「フォルダに限定」に関する制限

このトピックでは、JavaScriptのインクルードファイルが検出されるか、ログインマクロまたはワークフローマクロが使用される場合の、 [フォルダに限定(Restrict to folder)]スキャンオプションに関する制限について説明します。

JavaScriptインクルードファイル

スキャン中に、Web探索プログラムとJavaScriptエンジンは、外部のJavaScriptインクルードファイルにアクセスすることがあります。これらのファイルはアクティブに監査されないので、攻撃がHTTP経由で送信されることはありません。ただし、パッシブな調査によってJavaScriptインクルードファイルの問題が明らかになり、これらのファイルがサイトツリーに一覧表示されることがあります。

ログインマクロ

ログインマクロを使用する場合、そのマクロで要求されるセッションはサイトツリーに一覧表示されます。セッションはパッシブに監査されます。つまり、攻撃は送信されませんが、弱い暗号化、暗号化されないログインフォームなどの脆弱性が明らかになる可能性があります。

ワークフローマクロ

[Web探索および監査(Crawl and Audit)]スキャンまたは [Web探索のみ(Crawl Only)]スキャンでワークフローマクロを使用する場合、スキャンは [フォルダに限定(Restrict to folder)]オプションに違反する可能性があります。ワークフローマクロに含まれるURLにアクセスすることを希望していると見なされます。

エンタープライズスキャンの実行

エンタープライズスキャンは、Webプレゼンスの包括的な概観を企業ネットワークの観点から提供します。OpenText DASTを使用すると、ある範囲のIPアドレスで使用可能なすべてのポートが自動的に検出されます。その後、検出された全サーバから脆弱性を評価するサーバを選択できます。

エンタープライズスキャンを開始するには:

1. 次のいずれかを実行して、エンタープライズスキャンウィザードを起動します。
   - OpenText DASTの **[開始ページ(Start Page)]**で、 **[エンタープライズスキャンの開始(Start an Enterprise scan)]**をクリックします。
   - **[ファイル(File)] > [新規作成(New)] > [エンタープライズスキャン(Enterprise Scan)]**の順にクリックします。

- (ツールバーの) **[新規(New)]** アイコンでドロップダウン矢印をクリックし、 **[エンタープライズスキャン(Enterprise Scan)]** を選択します。
- OpenText DASTの **[開始ページ(Start Page)]** で、 **[スケジュールされたスキャンの管理(Manage Scheduled Scans)]** をクリックし、 **[追加(Add)]** をクリックしてから **[エンタープライズスキャン(Enterprise Scan)]** を選択します。

2. エンタープライズスキャンウィザードのステップ1で、スキャンを実行するタイミングを指定します。次の選択肢があります。
   - **即時(Immediately)**: スケジュールされたスキャンウィザードを終了するとすぐにスキャンが実行されます。
   - **日時指定で1回実行(Run Once Date / Time)**: スキャンを開始する日時を変更します。ドロップダウン矢印をクリックすると、日付を選択するカレンダを表示できます。
   - **定期実行スケジュール(Recurrence Schedule)**: スライダを使用して、頻度(毎日(Daily)、毎週(Weekly)、または毎月(Monthly))を選択します。次に、スキャンを開始する時刻を指定し、(**[毎週(Weekly)]** または **[毎月(Monthly)]** の場合は)その他のスケジュール情報を指定します。
3. **[次へ(Next)]** をクリックします。
4. エンタープライズスキャンウィザードのステップ2で、 **[エンタープライズスキャン名(Enterprise Scan Name)]** ボックスに、このエンタープライズスキャンの固有名を入力します。
5. この時点で、次の表で説明する1つ以上の機能を実行できます。

目的の作業...	その場合...
指定したIPアドレスとポートの範囲内で使用可能なすべてのサーバを検出するようにOpenText DASTに指示します。	a. **[検出(Discover)]** をクリックします。 **[Webサーバの検索(Search for Web Servers)]** ウィンドウが表示されます。 b. **[IPV4/IPV6アドレス(または範囲)(IPV4/IPV6 Addresses (or ranges))]** ボックスに、1つ以上のIPアドレスまたはIPアドレスの範囲を入力します。 ◦ 複数のアドレスを区切るには、セミコロンを使用します。 例: 172.16.10.3;172.16.10.44;188.23.102.5 ◦ 範囲の開始IPアドレスと終了IPアドレスを区切るには、ダッシュまたはハイフンを使用します。 例: 10.2.1.70-10.2.1.90。 **注記:** IPV6アドレスは括弧で囲む必要があります。「"Internet Protocolバージョン6"

目的の作業...	その場合...
	ページ401」を参照してください。 c. [ポート(または範囲)(Ports (or ranges))]ボックスに、スキャンするポートを入力します。 ◦ 複数のポートを区切るには、セミコロンを使用します。 例:80;8080;443 ◦ 範囲の開始ポートと終了ポートを区切るには、ダッシュまたはハイフンを使用します。 例:80-8080。 d. (オプション) [設定(Settings)]をクリックして、検出プロセスで使用するソケットとタイムアウトのパラメータの数を変更します。 e. [開始(Start)]をクリックして検出プロセスを開始します。 結果が [検出されたエンドポイント(Discovered End Points)]エリアに表示されます。 ◦ [IPアドレス(IP Address)]列のエントリをクリックして、そのサイトをブラウザで表示します。 ◦ [識別(Identification)]列のエントリをクリックして、 [セッションプロパティ(Session Properties)]ウィンドウを開きます。このウィンドウでは、生の要求と応答を表示できます。 f. サーバをリストから削除するには、 [選択(Selection)]列の対応するチェックボックスをオフにします。 g. [OK]をクリックします。 [スキャン対象ホスト(Hosts to Scan)]リストにIPアドレスが表示されます。
スキャンするURLまたはIPアドレスのリストを手動で入力する	a. [追加(Add)]をクリックします。 スキャンウィザードが開きます。 b. "基本スキャンの実行(Webサイトスキャン)"

目的の作業...	その場合...
	ページ199の説明に従って情報を入力します。 c. その他の各サーバに対して同じ手順を繰り返します。
スキャンするサーバのリストをインポートする **ヒント:** エンタープライズスキャン機能またはWeb Discoveryツールを使用してサーバを検出し、その結果をテキストファイルにエクスポートして作成したリストが必要です。	[**インポート(Import)**]をクリックし、保存しファイルを選択します。

[スキャン対象ホスト(Hosts to Scan)]リストの編集

上記の1つ以上の方法を使用してサーバのリストを作成した後、リストを変更できます。

特定のスキャンの設定を変更するには:

1. サーバを選択します。
2. [**編集(Edit)**]をクリックします。
   スキャンウィザードが開きます。
3. 設定を変更します。
4. (基本スキャンの編集(Edit Basic Scan)]ウィンドウで) [**完了(Finish)**]をクリックします。

リストからサーバを削除するには:

1. サーバを選択します。
2. [**削除(Delete)**]をクリックします。

リストをエクスポートする

[スキャン対象ホスト(Hosts to Scan)]リストを保存するには:

1. [**エクスポート**]をクリックします。
2. 標準のファイル選択ウィンドウを使用して、ファイル名と場所を指定します。

スキャンを開始する

エンタープライズスキャンを開始するには、 [スケジュール(Schedule)]をクリックします。各サーバのスキャン結果が、完了時にデフォルトのScansフォルダに自動的に保存されます。サーバの名前、日付、およびタイムスタンプがファイル名に含まれます。

注記: OpenText DASTライセンスにより、特定のIPアドレスまたはアドレス範囲のスキャンがユーザに許可されます。ライセンスで許可されていないIPアドレスがサーバにある場合、そのサーバはスキャンに含まれません。

手動スキャンの実行

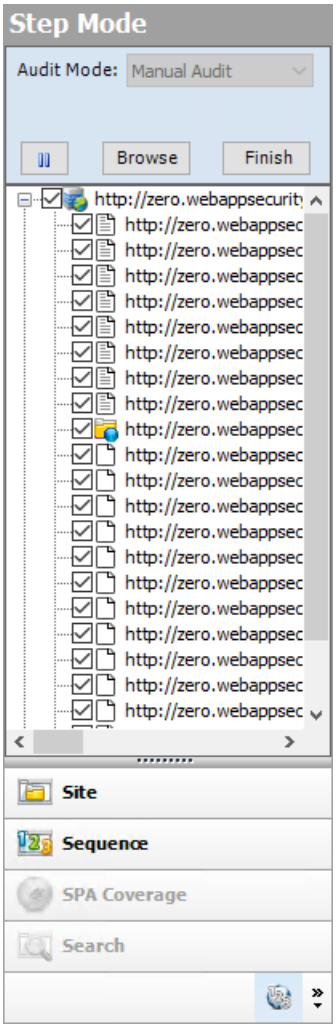
手動スキャン(ステップモードとも呼ばれる)は、FirefoxでTruClientを使用して、アクセス対象として選択したアプリケーションの任意のセクションに手動で移動できる、基本スキャンのオプションです。サイト全体のWeb探索は実行されず、サイト内を手動で移動中に検出したリソースに関する情報のみを記録します。この機能は、Webフォームのログオンページからサイトに入る場合、または調査するアプリケーションの個別のサブセットまたは部分を定義する場合に最もよく使用されます。サイト内を移動し終わったら、結果を監査して、記録したサイトのその部分に関連するセキュリティ脆弱性を評価できます。

手動スキャンを実行するには:

1. OpenText DASTの [開始ページ(Start Page)]で、 **基本スキャンの開始(Start A Basic Scan)**]を選択します。
2. スキャン方法として [**手動(Manual)**]を選択し、基本スキャンウィザードで説明される基本スキャンの設定手順に従います。詳細については、「"基本スキャンの実行(Webサイトスキャン)" ページ199」を参照してください。
3. [**スキャン(Scan)**]をクリックします。
4. ブラウザが開いたら、サイト内を移動して記録するエリアにアクセスします。

   ヒント: セッションを記録せずにアプリケーションの特定のエリアにアクセスする場合は、OpenText DASTに戻り、ナビゲーションペインの [ステップモード(Step Mode)]ビューに表示される [**一時停止(Pause)**]ボタン をクリックします。セッション記録を再開するには、 [**記録(Record)**]ボタン をクリックします。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。
5. 完了したら、ブラウザを閉じます。

OpenText DASTのナビゲーションペインに[ステップモード(Step Mode)]ビューが表示されます。



6. 次のいずれかを実行します。
   - アプリケーションのブラウズを再開するには、セッションを選択して[**ブラウズ(Browse)**]をクリックします。
   - セッションをスキャンにインポートするには、[**完了(Finish)**]をクリックします。個々のセッションをインポートから除外するには、対応するチェックボックスをオフにします。
7. 記録されたセッションを監査するには、(ツールバーの)Auditをクリックします。

権限のエスカレーションスキャンについて

権限のエスカレーション脆弱性は、プログラミングエラーや設計上の欠陥から生じ、攻撃者にアプリケーションとそのデータへの昇格されたアクセス権を付与します。OpenText DASTでは、同じスキャンで、低い権限または未認証のWeb探索に続いて、高い権限のWeb探索と監査を行って、権限のエスカレーション脆弱性を検出できます。OpenText DASTには、権限のエ

スカレーションポリシーと共に、カスタムポリシーを含む他のポリシーで有効にできる権限のエスカレーションチェックが含まれています。ガイド付きスキャンでは、権限のエスカレーションチェックが有効なポリシーが選択されると、OpenText DASTがそれを自動的に検出し、必要なログインマクロの入力を求めるプロンプトを表示します。

権限のエスカレーションスキャンの2つのモード

OpenText DASTでは2つのモードで権限のエスカレーションスキャンを実行できます。これは、使用するログインマクロの数によって決まります。

- 認証モード-このモードでは、低い権限によるアクセス用と、高い権限によるアクセス用の、2つのログインマクロを使用します。このモードでは、低い権限によるWeb探索の後に、高い権限によるWeb探索と監査が続きます。このタイプのスキャンは、ガイド付きスキャンを使用して実行できます。詳細については、「"ガイド付きスキャンの実行" ページ112」を参照してください。
- 未認証モード-このモードでは、高い権限のログインマクロのみを使用します。このモードでは、低い権限によるWeb探索は、実際には未認証のWeb探索です。このスキャンで検出される権限のエスカレーションは、未認証から高い権限に移行するものです。このタイプのスキャンは、(高い権限のログインマクロのみを提供して)ガイド付きスキャンウィザードを使用して実行するか、基本スキャンウィザードを使用して実行することができます。詳細については、「"基本スキャンの実行(Webサイトスキャン)" ページ199」を参照してください。

スキャン時の動作について

権限のエスカレーションチェックを有効にしたスキャンを実行する場合、OpenText DASTはまずサイトに対して低い権限によるWeb探索を実行します。このWeb探索では、Webサイトの階層構造は [サイト(Site)]ビューに表示されません。サマリペインにも脆弱性は表示されません。ただし、サマリペインの [スキャンログ(Scan Log)]タブをクリックすると、スキャンが実際に動作していることを確認できます。ログには、「スキャンの開始(Scan Start)」時刻と「LowPrivilegeCrawlStart」時刻を示すメッセージが記録されます。サイトに対する低い権限によるWeb探索が完了すると、高い権限によるWeb探索と監査のスキャンフェーズが実行されます。このフェーズでは、 [サイト(Site)]ビューに情報が入力され、検出された脆弱性がサマリペインに表示されます。詳細については、「"サマリペイン" ページ104」を参照してください。

制限のあるページを識別するために使用される正規表現パターン

「禁止(Forbidden)」、「制限付き(Restricted)」、または「アクセス拒否(Access Denied)」などのテキストを使用してブロックされる、制限のあるページがサイトに含まれる場合、権限のエスカレーションチェックには、これらのページが現在のユーザに対して禁止されていることを判断するための正規表現パターンが含まれます。したがって、これらのページは権限のエスカレーションに対して脆弱なものとして特定されません。ただし、組み込みの正規表現パターンに一致しない、権限を制限する他のテキストがサイトで使用されている場合は、独自のテキストパターンを含むように正規表現を変更する必要があります。変更しない場合、これらのページに対する権限のエスカレーションチェックで誤検出が発生するおそれがあります。

権限の制限パターンに合わせた正規表現の変更

正規表現を変更するには、次の方法を実行します。

1. **[編集(Edit)] > [デフォルトのスキャン設定(Default Scan Settings)]** の順にクリックします。
   [デフォルト設定(Default Settings)] ウィンドウが表示されます。
2. **[監査設定(Audit Settings)]** グループで、 **[攻撃の除外(Attack Exclusions)]** を選択します。
3. **[Audit Inputs Editor...]** をクリックします。
   Audit Inputs Editorが表示されます。
4. **[入力のチェック(Check Inputs)]** を選択します。
5. **[11388権限のエスカレーション(11388 Privilege Escalation)]** のチェックを選択します。
   [権限の制限パターン(Privilege Restriction Patterns)] が右側のペインに表示されます。デフォルトのパターンは次のとおりです。

```
'forbidden|restricted|access\sdenied|(?:operation\snot\s
(?:allowed|permitted|authorized))|(?:you\s(?:do\snot|don't)\shave\s
(?:access|permission|authorization))|(?:you\s(?:are\snot|aren't)\s
(?:allowed|permitted|authorized))'
```

6. 正規表現構文を使用して、サイトで使用されている、禁止されているアクションを表す新しい単語を追加します。
7. **[OK]** をクリックして、変更した **[入力のチェック(Check Inputs)]** を保存します。
8. **[OK]** をクリックして、 **[デフォルト設定(Default Settings)]** ウィンドウを閉じます。

Web探索プログラムの制限設定によって権限のエスカレーションスキャンに及ぶ影響

OpenText DASTは、スキャン中に各パラメータ値を監査します。したがって、権限のエスカレーションスキャンは、Web探索プログラムを制限する次のような設定の影響を受けます。

- 1つのURLの最大ヒット数を以下に制限する(Limit maximum single URL hits to)
- ヒット数にパラメータを含める(Include parameters in hit count)
- Webフォームの最大送信数を以下に制限する(Limit maximum Web form submission to)
- 冗長ページ検出の実行(Perform redundant page detection)

たとえば、 **[1つのURLの最大ヒット数を以下に制限する(Limit maximum single URL hits to)]** に1を設定し、サイトに次のようなリンクが含まれているとします。

```
index.php?id=2
 index.php?id=1
 index.php?id=3
```

ここで、OpenText DASTは高い権限によるスキャンの際に「index.php?id=1」を検出し、低い権限によるスキャンの際に「index.php?id=3」を検出します。このシナリオでは、OpenText DASTは「index.php?id=1”」に対して権限のエスカレーション脆弱性のマークを付けます。この脆弱性は誤検出です。

詳細については、「"スキャン設定: 全般" ページ406」を参照してください。

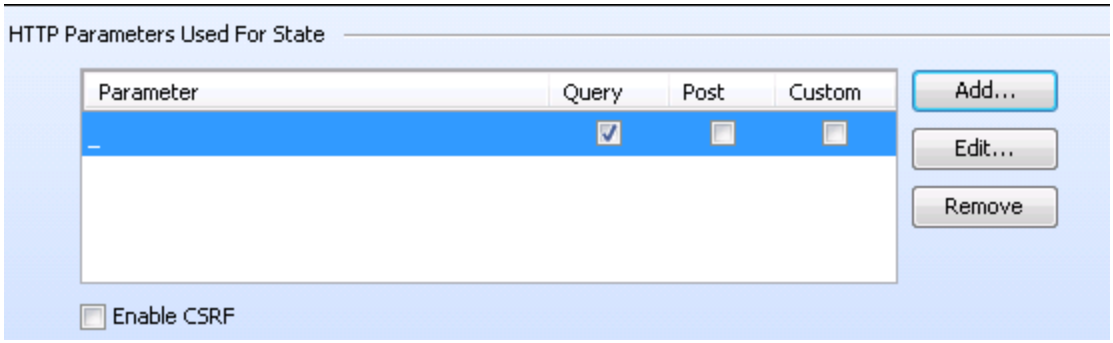
乱数を含むパラメータによって権限のエスカレーションスキャンに及ぶ影響

サイトに乱数を含むパラメータが含まれている場合は、そのパラメータを「状態に使用されるHTTPパラメータ(HTTP Parameters Used For State)」のリストに追加して、このようなセッションを監査から除外し、誤検出の数を減らすことができます。

たとえば、次のパラメータがあるとします。

```
index.php?_=1440601463586
index.php?_=1440601465662
index.php?_=1440601466365
```

次のように、このパラメータを「状態に使用されるHTTPパラメータ(HTTP Parameters Used For State)」のリストに追加します。



詳細については、「"スキャン設定: HTTP解析" ページ422」を参照してください。

参照情報

"基本スキャンの実行(Webサイトスキャン)" ページ199

"事前定義テンプレートの使用" ページ113

"モバイルスキャンテンプレートの使用" ページ130

"ネイティブスキャンテンプレートの使用" ページ147

シングルページアプリケーションスキャンについて

このトピックでは、アプリケーションのDOM (Document Object Model)のWeb探索および監査のためのSPA (シングルページアプリケーション)のサポートについて説明します。

シングルページアプリケーションの課題

開発者は、JavaScriptフレームワーク(Angular、Ext JS、Ember.jsなど)を使用してSPAを構築します。これらのフレームワークを使用することで開発者のアプリケーション構築は容易になりますが、セキュリティテスト担当者がセキュリティ脆弱性を検出するためにアプリケーションをスキャンすることが難しくなります。

従来のサイトで使用されているシンプルなバックエンドサーバレンダリングでは、サーバサイドで完全なHTML Webページが構築されます。SPAおよびその他の「Web 2.0」サイトで使用されているのは、フロントエンドDOMレンダリング、またはフロントエンドとバックエンドのDOMレンダリングの組み合わせです。SPAでは、ユーザがメニュー項目を選択すると、ページ全体を消去し、新しいコンテンツで再作成することができます。ただし、メニュー項目を選択するイベントで、サーバに対する新しいページの要求が生成されることはありません。サーバからページを再ロードすることなく、コンテンツの更新が行われます。

従来の脆弱性テストでは、新しいコンテンツをトリガしたイベントにより、SPAで以前に監査のために収集された他のイベントが破壊される可能性があります。OpenText DASTではSPAのサポートによって、SPAでの脆弱性テストの課題に対する解決策を提供します。

SPAサポートの有効化

SPAサポートを有効にすると、DOMスクリプトエンジンは、Web探索中に、JavaScriptインクルード、フレームとiframeのインクルード、CSSファイルインクルード、およびAJAX呼び出しを検索してから、それらのイベントによって生成されたすべてのトラフィックを監査します。

SPAサポートは、スキャン設定またはガイド付きスキャンで有効にできます。

注意! {/b}SPAサポートは、シングルページアプリケーションに対してのみ有効にするべきです。SPAサポートを有効にしてSPA以外のWebサイトをスキャンすると、スキャンが遅くなります。

参照情報

"スキャン設定: JavaScript" ページ412

"事前定義テンプレートの使用" ページ113

"モバイルスキャンテンプレートの使用" ページ130

"ネイティブスキャンテンプレートの使用" ページ147

スキャンステータス

特に指定されていない限り、スキャンステータスはデータベースから直接読み込まれます。次の表で、スキャンステータスについて説明します。

ヒント: ほとんどのスキャンステータスに関しては、ステータスの理由はスキャンログで確認できます。

ステータス	説明
完了	スキャンが完了しました。
未完了(Incomplete)	ユーザがスキャンを一時停止して閉じました。スキャンの実行は完了していません。
中断(Interrupted)	テスト中のアプリケーションやデータベースとのコネクティビティの問題など、環境上の問題があります。
ロック状態	OpenText DASTの1つのインスタンスがSQL Serverに接続しながらスキャンを実行しており、同じSQL Serverデータベースに接続されているOpenText DASTの2番目のインスタンスが同じスキャンにアクセスしようとしました。 **注記:** リモートSQL Server(フルバージョン)にのみ適用されます。
開く	ローカルマシンのユーザが、OpenText DASTでスキャンを開いています。ユーザは現在のユーザの場合もあれば(その場合は、[スキャン(Scan)]タブにスキャンが表示される)、同じマシン上の別のユーザの場合もあります(ターミナルサービスを使用している場合など)。スキャンデータベースに保存されている状態は無視されます。
一時停止(Paused)	ユーザがスキャンを一時停止しました。
実行中(Running)	スキャンは現在ローカルマシンで実行されています。 **注記:** このステータスには、スケジュールされたスキャンと、コマンドラインインタフェース(CLI)を介して開始されたスキャンが含まれます。

スキャンマネージャの情報の更新

スキャンマネージャは、現在表示されているスキャンに関するリアルタイムのステータス情報を提供することを目的としていませんが、次の3つの重要な例外があります。

- 新しいスキャンが作成されたか、開かれた場合。この場合、スキャンマネージャは新しいスキャンを一覧に示し、「オープン(Open)」ステータスを表示します。
- 現在のユーザによって以前に開かれたスキャンが閉じられた場合。たとえば、ユーザがスキャンを開くか作成した後、それを閉じます。スキャンマネージャ内でそのスキャンのステータスが更新され、閉じられた時点でのスキャンのステータスが反映されます(「完了(Completed)」や「未完了(Incomplete)」など)。その単一のスキャンに対してのみ、すべての統計情報が更新されます。
- スキャンが開かれている間、[期間(Duration)]フィールドが常に正確で使用可能であるとは限りません。したがって、スキャンの状態が[オープン(Open)]、[実行中(Running)]、また

は [ロック状態(Locked)] の場合、 **期間(Column)**] 列には値がないことが示されます(数字ではなく、「-」が表示されます)。

それ以外のステータス変更や更新されたカウント情報を表示するには、更新ボタンをクリックする必要があります。

参照情報

"スケジュールされたスキャンのステータス" ページ252

保存したスキャンを開く

次のいずれかの手順を使用して、前回のスキャンの結果を含む保存済みファイルを開きます。

メニューまたはツールバーの使用:

- **[ファイル(File)] > [開く(Open)] > [スキャン(Scan)]** の順にクリックします。
- **[開く(Open)]** ボタンのドロップダウン矢印をクリックし、 **[スキャン(Scan)]** を選択します。

[開始ページ(Start Page)] タブから:

- **[基本スキャンの開始(Start a Basic Scan)]** をクリックします。
- ホームペインで、 **[最近開いたスキャン(Recently Opened Scans)]** リスト内のエントリをクリックします。
- [スキャンの管理(Manage Scans)] ペインでスキャンを選択し、 **[開く(Open)]** をクリックします(またはスキャン名をダブルクリックします)。

OpenText DASTでスキャンデータがロードされ、別のタブに表示されます。

スキャンの比較

ターゲットが同じ2つの異なるスキャンから判明した脆弱性を比較し、この情報を次の目的で使用できます。

- 修復を検証する: 最初のスキャンで検出された脆弱性と、脆弱性の修復後に同じサイトに対して実行した別のスキャンで検出された脆弱性と比較します。
- スキャンヘルスをチェックする: スキャン設定を変更し、それらの変更によって攻撃露呈部分が広がっていないか検証します。
- 新しい脆弱性を検索する: 更新版のサイトが新しい脆弱性をもたらしていないか判断します。
- 問題を調査する: 誤検出や見落とされた脆弱性などのアノマリを追跡します。
- 権限付与アクセスを比較する: 2つの異なるユーザアカウントを使用してスキャンを実行し、両方のアカウントで固有のまたは共通の脆弱性を検出します。

注記: 両方のスキャンからのデータは、同じデータベースタイプ(SQL Server Express EditionまたはSQL Server Standard/Enterprise Edition)に保存する必要があります。

比較のためのスキャン選択

2つのスキャンを比較するには、次のいずれかを実行します。

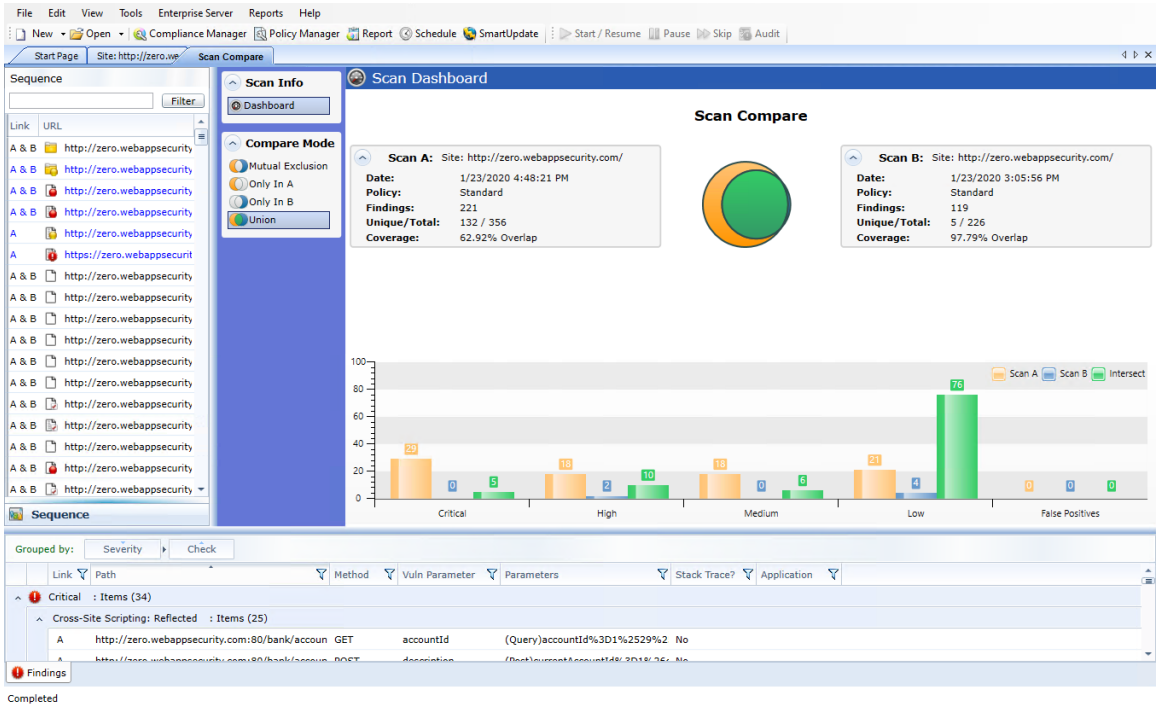
- [スキャンの管理(Manage Scans)]ページで、2つのスキャンを選択し、 **[比較(Compare)]**をクリックします。
- 開いているスキャン(比較ではスキャンAになる)を含むタブから:
  a. **[比較(Compare)]**をクリックします。
  b. [スキャンの比較(Scan Comparison)]ウィンドウのリストからスキャンを選択します。このスキャンが比較ではスキャンBになります。
  c. **[比較(Compare)]**をクリックします。

  注記: 開いているスキャンが「site retest」(**[再スキャン(Rescan)] > [脆弱性の再テスト(Retest Vulnerabilities)]**の結果)の場合は、OpenText DASTが比較対象の親スキャンを自動的に選択します。たとえば、「zero」という名前のスキャンを作成し、そのスキャンの脆弱性を検証した場合は、結果のスキャンに(デフォルトで)「site retest - zero」という名前が付けられます。再テストスキャンが開いている状態で、 **[比較(Compare)]**を選択すると、OpenText DASTが「site retest - zero」を親スキャン「zero」と比較します。

選択したスキャンの開始URLが異なる場合や異なるスキャンポリシーが使用されている場合、または、スキャンのタイプが異なる場合(基本スキャンとWebサービススキャンなど)は、警告メッセージが表示されます。続行を選択することも、機能を終了することもできます。

どちらかのスキャンが実行中は、比較を実行できません。

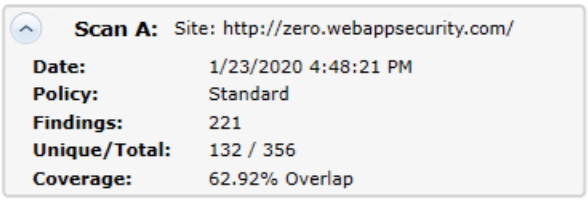
スキャン比較のイメージ



スキャンダッシュボードの確認

スキャン比較結果はスキャンダッシュボードに表示されます。

スキャンの説明



[スキャンA (Scan A)]ボックスと[スキャンB (Scan B)]ボックスに、スキャンに関する次の情報が表示されます。

- **スキャンA (Scan A)**または**スキャンB (Scan B)**: スキャンの名前。
- **日付(Date)**: オリジナルのスキャンが実行された日付と時刻。
- **ポリシー(Policy)**: スキャンに使用されたポリシー。詳細については、"OpenText DAST ポリシー" ページ509を参照してください。
- **検出事項(Findings)**: [検出事項(Findings)]タブで特定された問題と検出された誤検出の総数。
- **固有/合計(Unique/Total)**: このスキャン用に作成された固有のセッションの数(つまり、もう一方のスキャンではなく、このスキャンで出現したセッションの数)を、このスキャンのセッション

の総数と比較します。

- **カバレッジ(Coverage)**: 両方のスキャンに共通するセッションの割合。

ベン図

ベン図は、スキャンA(黄色の円)のセッションカバレッジとスキャンB(青色の円)のセッションカバレッジを示しています。2つのセットの交差は緑色のオーバーラップで表されます(以前のリリースでは、ベン図は脆弱性のオーバーラップを表していました)。

ベン図は、セット間の実際の関係を反映して拡大/縮小されます。

セッションカバレッジのオーバーラップの例を以下に示します。

				
0%の 交差	50%の 交差	Aが Bを 包含	Aのほとんどが Bと交差	完全な 交差

脆弱性棒グラフ

脆弱性の重大度のそれぞれと誤検出を別々のグループにすると、スキャンダッシュボードの下部に、スキャンA、スキャンB、およびそれらの交差(**交差(Intersect)**)で検出された脆弱性の数を示す棒グラフのセットが表示されます。ベン図と同じ色分けが使用されます。これらの棒グラフが、選択された **比較モード(Compare Mode)**]に基づいて変化することはありません。

スキーム、ホスト、およびポートの違いがスキャン比較に及ぼす影響

別々のサーバ上でホストされている2つの重複サイトからのスキャンを比較する場合、OpenText DASTはスキーム、ホスト、およびポートを無視しません。

たとえば、次のサイトのペアは、スキーム、ホスト、またはポートの違いにより、スキャン比較で相関性がありません。

- **スキーム**
  - サイトA - http://zero.webappsecurity.com/
  - サイトB - https://zero.webappsecurity.com/
- **ホスト**
  - サイトA - http://dev.foo.com/index.html?par1=123&par2=123
  - サイトB - http://qa.foo.com/index.html?par1=123&par2=123
- **ポート**

- サイトA - http://zero.webappsecurity.com:80/
- サイトB - http://zero.webappsecurity.com:8080/

比較モード

スキャンダッシュボードの左側にある **[比較モード(Compare Mode)]** セクションで次のいずれかのオプションを選択して、左側のペインの **[シーケンス(Sequence)]** エリアに別のデータを表示できます(スキャンダッシュボード内のデータには影響しません)。

- **相互除外(Mutual Exclusion)**: スキャンAまたはスキャンBに出現するものの、両方のスキャンには出現しないセッションを一覧にします。
- **Aのみ(Only In A)**: スキャンAにのみ出現するセッションを一覧にします。
- **Bのみ(Only in B)**: スキャンBにのみ出現するセッションを一覧にします。
- **結合(Union)** (デフォルト): スキャンAとスキャンBのいずれかまたは両方に出現するセッションを一覧にします。

セッションフィルタリング

[シーケンス(Sequence)] ペインには、選択された比較モードと一致する各セッションが一覧表示されます。URLの左側にあるアイコンは、そのセッションの脆弱性(もしあれば)の重大度を示します。重大度アイコンは次のとおりです。

重大	High	中間	Low
			

[シーケンス(Sequence)] ペインの上部で、フィルタを指定して **[フィルタ(Filter)]** をクリックすると、表示されるセッションのセットを次の方法で制限できます。

- URLは、「次の文字で始まる」の一致として、先頭の文字のみを入力できます。エントリは、プロトコル(http://またはhttps://)で始まる必要があります。
- URLを引用符で囲んで完全一致を検索できます。エントリは、引用符とプロトコル("http://または"https://)で始まる必要があります。
- 入力する文字列の先頭または末尾にワイルドカード文字としてアスタリスク(*)を使用できます。
- 入力する文字列の先頭と末尾の両方にアスタリスク(*)を使用できます。一致するには、アスタリスクの間の文字列が含まれている必要があります。
- 疑問符(?)の後に完全なクエリパラメータ文字列を入力して、そのクエリパラメータと一致する文字列を検索できます。

[セッション情報(Session Info)]パネルの使用

[シーケンス(Sequence)]ペインでセッションを選択すると、[比較モード(Compare Mode)]オプションの下で[セッション情報(Session Info)]パネルが開きます。セッションを選択した状態で、[セッション情報(Session Info)]パネルでオプションを選択すると、[セッション情報(Session Info)]パネルの右側に、そのセッションに関する詳細が表示されます。セッションに両方のスキャンのデータが含まれている場合は、[Webブラウザ(Web Browser)]、[HTTP要求(HTTP Request)]、[ステップ(Steps)]などの一部の機能に関するデータが分割ビューに表示されます(左側がスキャンAで右側がスキャンB)。

注記: [ステップ(Steps)]オプションは、[シーケンス(Sequence)]ペインで選択されたセッションまたは**サマリ**ペインで選択されたURLに到達するためにOpenText DASTがたどったパスを表示します。親セッション(リストの一番上)から始まり、それ以降にアクセスしたURLが順番に表示され、スキャン方法に関する詳細が提供されます。スキャン比較では、セッションのステップのいずれかがスキャン間で異なる場合に、[両方(In Both)]列が[ステップ(Steps)]テーブルに(最初の列として)追加されます。特定のステップの列内の[はい(Yes)]の値は、スキャンAとスキャンBの両方のそのセッションでステップが同じであることを示します。特定のステップの列内の[いいえ(No)]の値は、スキャンAとスキャンBのそれぞれのそのセッションでステップが異なることを示します。

サマリペインを使用した脆弱性の詳細の確認

スキャンを比較する場合は、ウィンドウの下部にある水平のサマリペインに、脆弱なリソースの一元管理されたテーブルが表示され、脆弱性情報に素早くアクセスできます。テーブルの上の水平区切り線をドラッグすると、表示される(または非表示になる)サマリペインの区画を増やすことができます。

[検出事項(Findings)]タブに表示される一連のエントリ(行)は、テーブルの[リンク(Link)]列に反映されているように、[比較モード(Compare Mode)]で選択されたオプションによって異なります。

脆弱性のグループ化とソート

脆弱性のグループ化とソートの詳細については、"サマリペイン" ページ104および"サマリペインのフィルタとグループの使用" ページ290を参照してください。

脆弱性のフィルタリング

任意の列見出しの右側にあるフィルタアイコン(▼)をクリックしてフィルタを開き、フィルタリング後に脆弱性(行)をテーブルに残すために満たすべき、その列に関するさまざまな条件を選択することができます。使用可能な条件には、列内の現在の値の一式が含まれます。また、その列の内容に関する論理式を指定することもできます。

たとえば、[Vulnパラメータ(Vuln Parameter)]列のフィルタで、次のように想定します。

1. チェックボックスの一番上のセットをそのままにします。
2. [次の値の行を表示する(Show rows with value that)]テキストの下で、ドロップダウンメニューから[次の値を含む(Contains)]を選択します。

3. ドロップダウンメニューの下にあるテキストボックスに「**Id**」と入力します。
4. [**フィルタ(Filter)**]をクリックします。

次に、[**Vulnパラメータ(Vuln Parameter)**]列に「Id」というテキストを含む行だけがテーブルに表示されます。これには、[**Vulnパラメータ(Vuln Parameter)**]の値が「**accountId**」や「**payeeId**」である行、または、「Id」を含むその他のエントリが含まれます。

複数の列にフィルタを指定できます(1回につき1つの列に指定)。それらのフィルタがすべて適用されます。

列のフィルタが指定されている場合、そのアイコンは未使用のフィルタのアイコンより濃い青色になります。

フィルタを素早くクリアするには、指定するフィルタが開いている間に[**フィルタのクリア(Clear Filter)**]をクリックします。

脆弱性の操作

サマリペインで項目を右クリックすると、次のコマンドを含むショートカットメニューが表示されます。

- **URLのコピー(Copy URL)**: URLをWindowsのクリップボードにコピーします。
- **選択した項目をコピー(Copy Selected Item(s))**: 選択した項目のテキストをWindowsのクリップボードにコピーします。
- **すべての項目をコピー(Copy All Items)**: すべての項目のテキストをWindowsのクリップボードにコピーします。
- **エクスポート(Export)**: すべての項目または選択した項目を含むカンマ区切り値(csv)ファイルを作成し、Microsoft Excelで表示します。
- **ブラウザで表示(View in Browser)**: ブラウザでHTTP応答をレンダリングします。

注記: Postパラメータおよびクエリパラメータの場合は、[**パラメータ(Parameters)**]列のエントリをクリックすると、パラメータのより分かりやすい概要が表示されます。

参照情報

"サマリペイン" ページ104

"サマリペインのフィルタとグループの使用" ページ290

スキャンの管理

スキャンを管理するには:

1. [**開始ページ(Start Page)**]で、[**スキャンの管理(Manage Scans)**]をクリックします。
   スキャンの一覧が、[**開始ページ(Start Page)**]の右側のペインに表示されます。
   デフォルトでは、自分のマシン上のSQL Server Express Editionと、SQL Server Standard Edition(設定されている場合)に保存されているスキャンがすべてOpenText

DASTによって一覧表示されます。スキャンの現在の状態は [ステータス(Status)] 列に示されます。詳細については、「"スキャンステータス" ページ236」を参照してください。

2. (オプション)列見出しに基づいてスキャンをカテゴリにグループ化するには、見出しをドラッグしてグループ化エリアにドロップします。
3. ツールバーを使用して、次の表に示すタスクを実行します。

目的...	その場合...
スキャンを検索する	[検索(Search)] ボックスにスキャン名またはスキャンIDを入力します。入力するにつれて、OpenText DASTにより、スキャンのリストがフィルタ処理されます。 **ヒント:** 検索条件をクリアするには、検索のクリアアイコン(×)をクリックします。
1つ以上のスキャンを開く	1つ以上のスキャンを選択して、 [開く(Open)] をクリックします(または、単にリスト内のエントリをダブルクリックします)。OpenText DASTによってスキャンデータがロードされ、それぞれのスキャンは個別のタブに表示されます。
選択されたスキャンに最後に使用された設定でスキャンウィザードを起動する	[再スキャン(Rescan)] > [もう一度スキャンする(Scan Again)] をクリックします。
スキャンを再利用する	[再スキャン(Rescan)] をクリックし、ドロップダウンメニューから必要な再使用オプションを選択します。詳細については、「"スキャンの再利用" ページ277」を参照してください。
前回のスキャン中に明らかになった脆弱性を含むセッションのみを再スキャンする	スキャンを選択し、 [再スキャン(Rescan)] > [脆弱性の再テスト(Retest Vulnerabilities)] をクリックします。
スキャンをマージする	2つのスキャンを選択(Ctrl+クリックを使用)して、右クリックし、 [マージ(Merge)] を選択します。詳細については、「"増分スキャン" ページ278」を参照してください。
選択したスキャンの名前を変更する	[名前変更(Rename)] をクリックします。
選択したスキャンを削除する	[削除(Delete)] をクリックします。

目的...	その場合...
スキャンをインポートする	[インポート(Import)]をクリックします。
スキャンまたはスキャンの詳細をエクスポートする、スキャンをSoftware Security Centerにエクスポートする、または保護ルールをWebアプリケーションファイアウォール(WAF)にエクスポートする	[エクスポート(Export)]でドロップダウンボタンをクリックします。
スキャンを比較する	2つのスキャンを選択(Ctrl+クリックを使用)し、[比較(Compare)]をクリックします。
スキャンおよびレポートのストレージと、スキャンの表示のどちらかまたはその両方のデータベース接続設定を変更する **注記:** デフォルトでは、ローカルSQL Server Express Editionと設定済みのSQL Server Standard Editionに保存されているスキャンがすべてOpenText DASTによって一覧表示されます。	[接続(Connections)]をクリックします。詳細については、「"アプリケーション設定:データベース" ページ484」を参照してください。
表示を更新する	[更新(Refresh)]をクリックします。
表示する列を選択する	[列(Columns)]をクリックします。 **ヒント:** [上へ移動(Move Up)]ボタンと[下へ移動(Move Down)]ボタンを使用して列を表示する順序を並べ替えたり、[スキャンの管理(Manage Scans)]リストで、単に列見出しをドラッグアンドドロップしたりすることができます。

注記: また、エントリを右クリックしてショートカットメニューからコマンドを選択することで、これらの機能のほとんどを実行できます。レポートの生成も選択できます。詳細については、「"レポートの生成" ページ306」を参照してください。

参照情報

"スケジュールされたスキャンの管理" ページ248

"開始ページ(Start Page)" ページ50

スキャンのスケジュール

基本スキャン、APIスキャン、またはエンタープライズスキャンを、選択した日時に実行するためのスケジュールを設定できます。

選択したオプションと設定は特別なファイルに保存されます。これは、OpenText DASTの起動(必要な場合)とスキャンの開始を行うWindowsサービスによってアクセスされます。スキャンの開始が指定されている時刻にOpenText DASTが実行されている必要はありません。

注記: スケジュールされたスキャンの完了後、これにアクセスするには、 **[開始ページ(Start Page)]**タブを選択して **[スキャンの管理(Manage Scans)]**をクリックします。

スキャンをスケジュール設定するには:

1. 次のいずれかを実行します。
   - OpenText DASTツールバーの **[スケジュール(Schedule)]**アイコンをクリックします。
   - OpenText DASTの **[開始ページ(Start Page)]**で、 **[スケジュールされたスキャンの管理(Manage Scheduled Scans)]**をクリックします。
2. **[スケジュールされたスキャンの管理(Manage Scheduled Scans)]**ウィンドウが表示されたら、 **[追加(Add)]**をクリックします。
3. **[スキャンのタイプ(Type of Scan)]**グループで、次のいずれかを選択します。
   - **[Webサイトスキャン(Web Site Scan)]**
   - **[APIスキャン(API Scan)]**
   - **[エンタープライズスキャン(Enterprise Scan)]**
4. スキャンを1回だけ実行するには、 **[1度だけ実行(Run Once)]**を選択し、 **[開始日(Start Date)]**と **[時刻(Time)]**を編集します。ドロップダウン矢印をクリックすると、カレンダを使用して日付を選択できます。
5. サイトを定期的にスキャンするには:
   a. **[繰り返し(Recurring)]**(または **[繰り返しスケジュール(Recurrence Schedule)]**)を選択し、開始時刻を指定して頻度(**[毎日(Daily)]**、 **[毎週(Weekly)]**、 **[毎月(Monthly)]**)を選択します。
   b. **[毎週(Weekly)]**または **[毎月(Monthly)]**を選択した場合は、要求される追加の情報を入力します。
6. **[次へ(Next)]**をクリックします。

参照情報

"基本スキャンの実行(Webサイトスキャン)" ページ199

"APIスキャンウィザードの使用" ページ165

"エンタープライズスキャンの実行" ページ227

"スケジュールされたスキャンの時間間隔の設定" 次のページ

スケジュールされたスキャンの時間間隔の設定

スキャンを実行する時間を設定したり、定期的なスキャンを設定したりするには:

1. [スキャンのタイプ(Type of Scan)]グループで、次のいずれかを選択します。
   - 基本スキャン(Basic Scan)
   - [APIスキャン(API Scan)]
   - [エンタープライズスキャン(Enterprise Scan)]
2. スキャンを今すぐ実行するには、 [即時(Immediately)]を選択します。
3. 後日または後刻に一度だけスキャンを実行するには:
   a. [1度だけ実行(Run Once)]を選択します。
   b. スキャンを開始する日時を変更します。

   ヒント: ドロップダウン矢印をクリックして、日付を選択するためのカレンダを表示します。
4. サイトを定期的にスキャンするには:
   a. [定期的(Recurring)]を選択します。
   b. スキャンを開始する時刻を指定します。
   c. 頻度を [毎日(Daily)]、 [毎週(Weekly)]、または [毎月(Monthly)]から選択します。
5. [次へ(Next)]をクリックします。

参照情報

"基本スキャンの実行(Webサイトスキャン)" ページ199

"APIスキャンウィザードの使用" ページ165

"エンタープライズスキャンの実行" ページ227

スケジュールされたスキャンの管理

指定した日時にスキャンを実行するように、OpenText DASTに指示できます。選択したオプションと設定は特別なファイルに保存されます。これは、OpenText DASTの起動(必要な場合)とスキャンの開始を行うWindowsサービスによってアクセスされます。スキャンの開始が指定されている時刻にOpenText DASTが実行されている必要はありません。

注記: スケジュールされたスキャンが完了しても、OpenText DASTの [開始ページ(Start Page)]に表示される [最近のスキャン(Recent Scans)]一覧には表示されません。スケジュールされたスキャンの完了後、これにアクセスするには、 [開始ページ(Start Page)]を選択して [スキャンの管理(Manage Scans)]をクリックします。

スケジュールされたスキャンへのアクセス

スケジュールされたスキャンのリストにアクセスするには、次の方法を実行します。

- [**開始ページ(Start Page)**]で、[**スケジュールの管理(Manage Schedule)**]をクリックします。

  以前にスケジュールされたスキャンの一覧が、[**開始ページ(Start Page)**]の右側のペインに表示されます。

  スキャンの現在の状態は[ステータス(Status)]列に示されます。詳細については、「"スケジュールされたスキャンのステータス" ページ252」を参照してください。

スキャンの削除

以前にスケジュールしたスキャンをリストから削除するには、次の方法を実行します。

- スキャンを選択し、[**削除(Delete)**]をクリックします。

スキャン設定の編集

スケジュールされたスキャンの設定を編集するには、次の方法を実行します。

- スキャンを選択し、[**編集(Edit)**]をクリックします。

スキャンの即時実行

スケジュールされた時間を待たずにスキャンをすぐに実行するには、次の方法を実行します。

- スキャンを選択して[**開始(Start)**]をクリックします(または、スキャンを右クリックしてショートカットメニューから[**スキャンの開始(Start Scan)**]を選択します)。

  すべてのスケジュールされたスキャンと同様に、スキャンはバックグラウンドで実行され、タブには表示されません。

スケジュールされているスキャンの停止

スケジュールされているスキャンを停止するには、次の方法を実行します。

- 実行中のスキャンを選択して[**停止(Stop)**]をクリックします(または、実行中のスキャンを右クリックしてショートカットメニューから[**スキャンの終了(Stop Scan)**]を選択します)。

スキャンのスケジューリング

スキャンをスケジュール設定するには:

1. [追加(Add)]をクリックします。
2. [スキャンのタイプ(Type of Scan)]グループで、次のいずれかを選択します。
   - 基本スキャン(Basic Scan)
   - Webサービススキャン(Web Service Scan)
   - エンタープライズスキャン(Enterprise Scan)
3. スキャンを実行するタイミングを指定します。次の選択肢があります。
   - 即時(Immediately)
   - 1回実行(Run Once): スキャンを開始する日時を変更します。ドロップダウン矢印をクリックすると、日付を選択するカレンダを表示できます。
   - 定期実行スケジュール(Recurrence Schedule): スライダを使用して、頻度(毎日(Daily)、毎週(Weekly)、または毎月(Monthly))を選択します。次に、スキャンを開始する時刻を指定し、([毎週(Weekly)]または[毎月(Monthly)]の場合は)その他のスケジュール情報を指定します。
4. [次へ(Next)]をクリックします。
5. 選択したスキャンのタイプの設定を入力します。
6. WebサイトおよびWebサービススキャンの場合に限り、スキャンの最後にレポートを実行するように選択できます。
   a. [レポートの生成(Generate Reports)]を選択し、[レポートの選択(Select Reports)]ハイパーリンクをクリックします。
   b. (下の)「レポートの選択」に進んでください。
7. レポートを生成せずにスキャンをスケジュール設定するには、[スケジュール(Schedule)]をクリックします。

レポートの選択

スケジュールされたスキャンにレポートを含めるように選択した場合は、[スケジュールされたスキャンのレポートウィザード(Scheduled Scan Report Wizard)]が表示されます。

レポートを選択するには、次の方法を実行します。

1. (オプション)[お気に入り(Favorites)]リストからレポートを選択します。
   「お気に入り」は、1つ以上のレポートとその関連パラメータの単なる名前付きコレクションです。レポートおよびパラメータを選択した後でお気に入りを作成するには、[お気に入り(Favorites)]リストをクリックして、[お気に入りに追加(Add to favorites)]を選択します。
2. 1つ以上のレポートを選択します。
3. 要求できるパラメータの情報を入力します。必須のパラメータは赤で囲まれます。

4. [次へ(Next)]をクリックします。
   [レポート設定(Configure Report Settings)]ウィンドウが表示されます。

レポートの設定

レポートを設定するには、次の方法を実行します。

1. [ファイル名の自動生成(Automatically Generate Filename)]を選択すると、レポートファイルの名前は*<reportname> <date/time>.<extension>*の形式になります。たとえば、pdf形式でコンプライアンスレポートを作成し、そのレポートが4月5日の6:30に生成される場合、ファイル名は「Compliance Report 04_05_2009 06_30.pdf」になります。これは、反復スキャンの場合に便利です。
   レポートは、生成されるレポート用にアプリケーション設定で指定されたディレクトリに書き込まれます。
2. [ファイル名の自動生成(Automatically Generate Filename)]を選択しなかった場合は、[ファイル名(Filename)]ボックスにファイルの名前を入力します。
3. [エクスポート形式(Export Format)]リストからレポート形式を選択します。
4. 複数のレポートを選択した場合は、[レポートを1つに集約(Aggregate reports into one report)]を選択することで、すべてのレポートを1つに結合できます。
5. レポートに使用するヘッダとフッタを定義するテンプレートを選択し、必要に応じて要求されたパラメータを指定します。
6. [完了(Finished)]をクリックします。
7. [スケジュール(Schedule)]をクリックします。

参照情報

"開始ページ(Start Page)" ページ50

"スキャンの管理" ページ244

"スケジュールされたスキャンのステータス" 次のページ

スケジュールされているスキャンの停止と再開

スケジュールされているスキャンを実行中に停止するには、[スケジュールの管理(Manage Schedule)]リストからスキャンを選択して、Stop をクリックします(またはスキャンを右クリックしてショートカットメニューから[スキャンの停止(Stop Scan)]を選択します)。

停止したスキャンを再開するには、[スケジュールの管理(Manage Schedule)]リストからスキャンを選択して、Start をクリックします(またはスキャンを右クリックしてショートカットメニューから[スキャンの開始(Start Scan)]を選択します)。

スケジュールされたスキャンのステータス

スケジュールされたスキャンそれぞれのステータスは、 **[スケジュールの管理(Manage Schedule)]**ペインの **前回の実行のステータス(Last Run Status)**]列に表示されます。次の表に、それぞれのステータスの定義を示します。

ステータス	定義
失敗(Failure)	OpenText DASTはスキャンを実行できませんでした。
成功	スキャンが実行され、エラーはありませんでした。
未実行(Not Yet Run)	スキャンは、スケジュールされた時刻に実行するためにキューに登録されていますが、まだ実行されていません。
スキップ済み(Skipped)	サービスが一時的にダウンしたため、スケジュールされたスキャンが実行されませんでした。
停止中(Stopping)	ユーザが **停止(Stop)**]ボタンをクリックしましたが、スキャンはまだ停止していません。
停止済み(Stopped)	スキャンはユーザによって停止されました。
実行中(Running)	スケジュールされたスキャンが進行中です。
実行中、エラーあり(Running with Error)	スキャンを停止できませんでした。詳細についてはログを参照してください。

スキャンのエクスポート

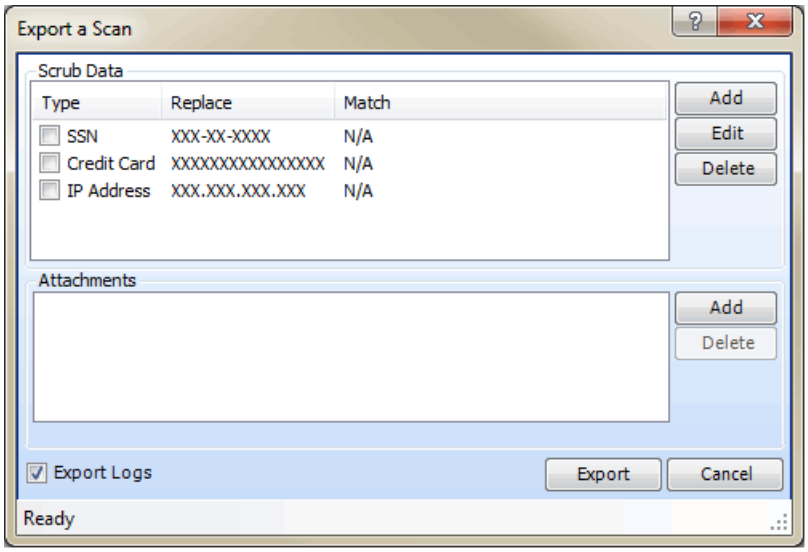
スキャンのエクスポート機能を使用して、OpenText DASTのWeb探索または監査時に収集された情報を保存します。

注記: Fortify Software Security Centerにエクスポートする場合、.fpr形式にエクスポートした後で、.fprファイルをFortify Software Security Centerに手動でアップロードする必要があります。OpenTextでは、OpenText DAST FPRアーティファクトとFortify WebInspect Enterprise FPRアーティファクトの両方をFortify Software Security Centerの同じアプリケーションバージョンにアップロードすることはサポートしていません。

スキャンをエクスポートするには、以下のステップに従います。

1. 次のいずれかを実行します。
   - スキャンを開き(または開いているスキャンを含むタブをクリックし)、 **[ファイル(File)] > [エクスポート(Export)]**をクリックして、 **[スキャン(Scan)]**または **[スキャンをSoftware Security Centerへ(Scan to Software Security Center)]**を選択します。
   - **[開始ページ(Start Page)]**の **[スキャンの管理(Manage Scans)]**ペインでスキャンを選択し、 **[エクスポート(Export)]**ボタンのドロップダウン矢印をクリックして、 **[スキャンのエクスポート(Export Scan)]**または **[Software Security Centerへのスキャンのエクスポート(Export Scan to Software Security Center)]**を選択します。

   [スキャンのエクスポート(Export a Scan)]ウィンドウ(または **[Software Security Centerへのスキャンのエクスポート(Export Scan to Software Security Center)]**ウィンドウ)が表示されます。



2. **[スクラブデータ(Scrub Data)]**グループには、デフォルトで、社会保障番号、クレジットカード番号、またはIPアドレスとしてフォーマットされた文字列内の各数字を**X**に置き換える、編集不可の3つの正規表現関数が含まれています。検索および置換機能を含めるには、関連するチェックボックスを**オン**にします。この機能により、機密データがエクスポートに含まれないようにすることができます。
3. スクラブデータ関数を作成するには:
   a. **[追加(Add)]**をクリックします。
   b. **[スクラブ項目の追加(Add Scrub Entry)]**ウィンドウで、 **[タイプ(Type)]**リストから **[正規表現(Regex)]**または **[リテラル(Literal)]**を選択します。
   c. **[一致(Match)]**ボックスに、検索する文字列(または文字列を表す正規表現)を入力します。正規表現を使用する場合は、省略記号ボタン**...**をクリックしてRegular Expression Editorを開き、正規表現を作成およびテストできます。
   d. **[置換(Replace)]**ボックスに、 **[一致(Match)]**文字列で指定したターゲットを置き換える文字列を入力します。
   e. **[OK]**をクリックします。
4. Software Security Centerにエクスポートする場合は、ステップ7に進みます。

5. 添付ファイルを含める場合:
   a. **[添付ファイル(Attachments)]** グループで、 **[追加(Add)]** をクリックします。
   b. 標準のファイル選択ウィンドウを使用して、添付するファイルを含むディレクトリに移動します。
   c. ファイルを選択し、 **[開く(Open)]** をクリックします。
6. スキャンのログファイルを含めるには、 **[ログのエクスポート(Export Logs)]** を選択します。
7. **[エクスポート]** をクリックします。
8. 標準のファイル選択ウィンドウを使用して場所を選択し、 **[保存(Save)]** をクリックします。

参照情報

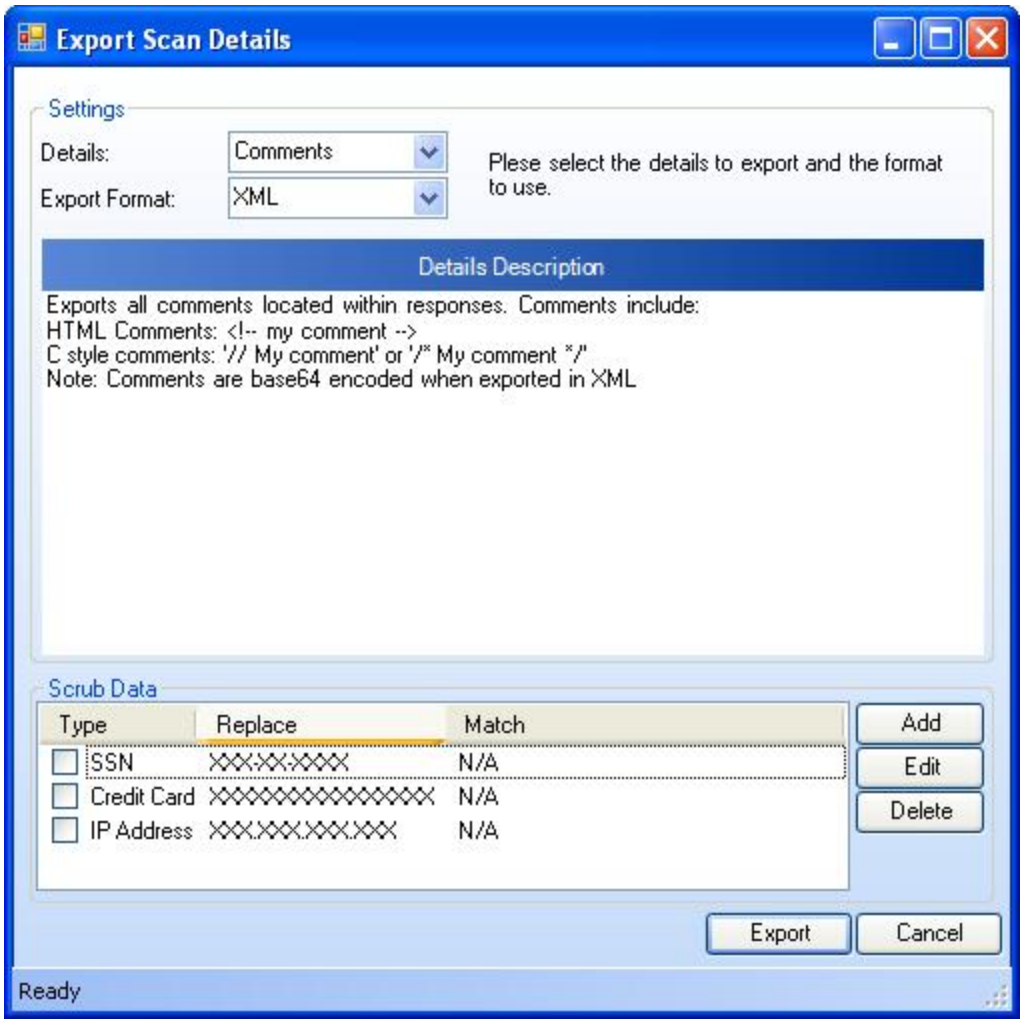
"スキャンのインポート" ページ260

"スキャン詳細のエクスポート" 下

スキャン詳細のエクスポート

この機能を使用して、OpenText DASTのWeb探索または監査時に収集された情報を保存します。

1. スキャンを開くか、スキャンを含むタブをクリックします。
2. **[ファイル(File)] > [エクスポート(Export)] > [スキャンの詳細(Scan Details)]** の順にクリックします。
   [スキャン詳細のエクスポート(Export Scan Details)] ウィンドウが表示されます。



3. **詳細(Details)**]リストから、エクスポートする情報のタイプを選択します。オプションは次のとおりです。
   - **コメント(Comments)** - 応答内のすべてのコメントをエクスポートします。

     注記: コメントは、XML形式でエクスポートされる場合、base64でエンコードされます。

   - **CycloneDX** - オープンソースクライアント側ライブラリ用のCycloneDXソフトウェア部品表(SBOM)をエクスポートします。

     注記: CycloneDX出力はJSONファイルです。 **エクスポート形式(Export Format)**]リストは、この出力タイプでは使用できません。

     ヒント: Fortify Software Security Centerは、CycloneDX SBOMデータをインポートする際にZIPファイル形式を要求します。回避策として、JSONファイルを`scan.info`という名前のファイルと一緒にZIPファイルに追加する必要があります。このscan.infoファイルには、次のテキスト行を含める必要があります。

```
engineType=WEBINSPECT
```

現在、Fortify Software Security Centerの「アーティファクト履歴(ARTIFACT HISTORY)」ページでは、エンジンの「タイプ(Type)」は「不明(Unknown)」として識別されます。

- **電子メール(Emails)** - スキャン中に検出されたすべての電子メールアドレスのリストをエクスポートします。
- **完全(Full)** - セッション要求と応答(解析済みのものも未解析のものも含む)、およびすべてのセッション脆弱性情報をエクスポートします。
- **非表示フィールド(Hidden Fields)** - 応答内のすべての非表示フィールドをエクスポートします。

  注記: 非表示フィールドは、XML形式でエクスポートされる場合、base64でエンコードされます。

- **オフサイトリンク(Offsite Links)** - すべてのオフサイトリンクをエクスポートします。
- **パラメータ(Parameters)** - パラメータを持つスキャンツリー内のすべてのセッションをエクスポートします。
- **要求(Requests)** - すべてのURLと、Web探索中に送信された生の関連要求をエクスポートします。

  注記: 要求は、XML形式でエクスポートされる場合、base64でエンコードされます。

- **スクリプト(Scripts)** - 応答内のすべてのスクリプトをエクスポートします。

  注記: コメントは、XML形式でエクスポートされる場合、base64でエンコードされます。

- **セッション(Sessions)** - すべてのURLと生の関連要求、および応答をエクスポートします。

  注記: 要求と応答は、XML形式でエクスポートされた場合、base64でエンコードされます。

- **設定されているクッキー(Set Cookies)** - サーバによって設定されたすべてのクッキーをエクスポートします。

  注記: クッキーは、XML形式でエクスポートされる場合、base64でエンコードされます。

- **URL** - Web探索されたすべてのURLをエクスポートします。
- **脆弱性(Vulnerabilities)** - 関連するコンテキスト情報と共に脆弱性をエクスポートします。

- **Web探索のダンプ(Web Crawl Dump)** - Web探索された各セッションの応答本文を、元のファイル名とディレクトリ構造を使用してファイルシステムにダンプします。
- **サイトツリーのダンプ(Site Tree Dump)** - Web探索された各セッションの応答本文を、元のファイル名とディレクトリ構造を使用してファイルシステムにダンプします。
- **Webフォーム(Web Forms)** - 応答内のすべてのフォームをエクスポートします。

注記: 一部の選択肢はWebサービススキャンでは使用できません。

4. [**エクスポート形式(Export Format)**]リストから出力形式を選択します。オプションは、[**テキスト(Text)**]と[**XML**]です。ただし、詳細のタイプによっては使用できる形式が1つのみのものもあります。
5. [**スクラブデータ(Scrub Data)**]グループには、デフォルトで、社会保障番号、クレジットカード番号、またはIPアドレスとしてフォーマットされた文字列内の各数字をXに置き換える、編集不可の3つの正規表現関数が含まれています。データタイプにこの検索および置換機能を含めるには、関連するチェックボックスをオンにします。この機能により、機密データがエクスポートに含まれないようにすることができます。
6. スクラブデータ関数を作成するには:
   a. [**追加(Add)**]をクリックします。
   b. [スクラブ項目の追加(Add Scrub Entry)]ウィンドウで、[**タイプ(Type)**]リストから[**正規表現(Regex)**]または[**リテラル(Literal)**]を選択します。
   c. [**一致(Match)**]ボックスに、検索する文字列(または文字列を表す正規表現)を入力します。正規表現を使用する場合は、省略記号ボタン…をクリックしてRegular Expression Editorを開き、正規表現を作成およびテストできます。
   d. [**置換(Replace)**]ボックスに、[**一致(Match)**]文字列で指定したターゲットを置き換える文字列を入力します。
   e. [**OK**]をクリックします。
7. [**エクスポート**]をクリックします。
8. 標準のファイル選択ウィンドウを使用して、エクスポートするファイルの名前と場所を指定し、[**保存(Save)**]をクリックします。

参照情報

"スキャンのエクスポート" ページ252

Fortify Software Security Centerにスキャンをエクスポートする

この機能を使用すると、Fortify Software Security Centerで利用できる形式(.fpr形式)でOpenText DASTスキャンの結果をエクスポートできます。

注記: .fpr形式にエクスポートした後、その.fprファイルをFortify Software Security Centerに手動でアップロードする必要があります。OpenTextでは、OpenText DAST FPRアー

ティファクトとFortify WebInspect Enterprise FPRアーティファクトの両方をFortify Software Security Centerの同じアプリケーションバージョンにアップロードすることはサポートしていません。

1. 次のいずれかを実行します。
   - スキャンを開き(または開いているスキャンを含むタブをクリックし)、 **[ファイル(File)] > [エクスポート(Export)] > [スキャンをSoftware Security Centerへ(Scan to Software Security Center)]**をクリックします。
   - [開始ページ(Start Page)]の [スキャンの管理(Manage Scans)]ペインでスキャンを選択し、 **[エクスポート(Export)]**ボタンのドロップダウン矢印をクリックして、 **[Software Security Centerへのスキャンのエクスポート(Export Scan to Software Security Center)]**を選択します。

   [Software Security Centerへのスキャンのエクスポート(Export Scan to Software Security Center)]ウィンドウが表示されます。
2. **[スクラブデータ(Scrub Data)]**グループには、デフォルトで、社会保障番号、クレジットカード番号、またはIPアドレスとしてフォーマットされた文字列内の各数字を**X**に置き換える、編集不可の3つの正規表現関数が含まれています。検索および置換機能を含めるには、関連するチェックボックスをオンにします。この機能により、機密データがエクスポートに含まれないようにすることができます。
3. スクラブデータ関数を作成するには:
   a. **[追加(Add)]**をクリックします。
   b. [スクラブ項目の追加(Add Scrub Entry)]ウィンドウで、 **[タイプ(Type)]**リストから **[正規表現(Regex)]**または **[リテラル(Literal)]**を選択します。
   c. **[一致(Match)]**ボックスに、検索する文字列(または文字列を表す正規表現)を入力します。正規表現を使用する場合は、省略記号ボタン…をクリックしてRegular Expression Editorを開き、正規表現を作成およびテストできます。
   d. **[置換(Replace)]**ボックスに、 **[一致(Match)]**文字列で指定したターゲットを置き換える文字列を入力します。
   e. **[OK]**をクリックします。
4. **[エクスポート]**をクリックします。
5. 標準のファイル選択ウィンドウを使用して場所を選択し、 **[保存(Save)]**をクリックします。

一時停止したスキャンからのFPRのアップロードに伴う既知の問題

次のシナリオでは、OpenText DASTからFortify Software Security Centerに手動でFPRをエクスポートすると、既知の問題が発生します。

1. スキャンはOpenText DASTで開始された。
2. スキャンは一時停止している。
3. スキャンはFPRにエクスポートされてから、Fortify Software Security Centerにアップロードされた。

4. スキャンはOpenText DASTで再起動された。
5. スキャンは完了し、アプリケーションで追加の脆弱性が見つかった。
6. スキャンはFPRにエクスポートされ、Fortify Software Security Centerにアップロードされた。

FPRをアップロードするとき、Fortify Software Security Centerでは、FPRのスキャン作成時刻を使用して、ファイルがすでに存在するかどうかを判断します。このシナリオでは、部分スキャンと完了したスキャンの作成時刻は両方同じになります。部分スキャンがFortify Software Security Center内にすでに存在するため、完了したスキャンはアップロードされません。スキャンの再開後に検出されたその他の脆弱性は、Fortify Software Security Centerに表示されません。

回避策として、完了した結果をアップロードする前に、Fortify Software Security Centerから部分FPRを削除する必要があります。

Webアプリケーションファイアウォール(WAF)への保護ルールのエクスポート

Webアプリケーションのスキャン中にOpenText DASTによって検出された脆弱性に基づく完全なエクスポート(.xml)ファイルを生成して保存するには:

1. 対象となるスキャンを開き(または開いているスキャンを含むタブをクリックし)、 **[ファイル(File)] > [エクスポート(Export)] > [保護ルールをWebアプリケーションファイアウォールへ(Protection Rules to Web Application Firewall)]** をクリックします。
2. **[ファイル(File)] > [エクスポート(Export)] > [スキャン(Scan)]** オプションと同じ方法でスクラブデータのタイプを指定します。 **[スクラブデータ(Scrub Data)]** グループには、デフォルトで、社会保障番号、クレジットカード番号、またはIPアドレスとしてフォーマットされた文字列内の各数字をXに置き換える、編集不可の3つの正規表現関数が含まれています。データタイプにこの検索および置換機能を含めるには、関連するチェックボックスをオンにします。この機能により、機密データがエクスポートに含まれないようにすることができます。
3. **[エクスポート]** をクリックします。
4. エクスポートしたデータを保存するパスとファイル名を指定し、 **[保存(Save)]** をクリックします。

   完全なエクスポート(.xml)ファイルが、指定どおりに保存されます。

スキャンのインポート

スキャンをインポートするには:

1. [ファイル(File)] > [スキャンのインポート(Import Scan)]をクリックします。
2. 標準のファイル選択ウィンドウを使用して、[ファイルの種類(Files Of Type)]リストから次のいずれかのオプションを選択します。
   - スキャンファイル(*.scan) - 7.0以降のバージョンのOpenText DASTで設計または作成されたスキャンファイル。
   - SPAファイル(*.spa) - 7.0より前のバージョンのOpenText DASTによって作成されたスキャンファイル。
3. ファイルを選択し、[開く(Open)]をクリックします。

スキャンと一緒に添付ファイルをエクスポートした場合、その添付ファイルがインポートされて、インポートされたスキャンのサブディレクトリに保存されます。デフォルトの場所は、`C:\Users\<username>\AppData\HP\HP WebInspect\ScanData\Imports\<DirectoryName>\<filename>`です。この場合、DirectoryNameは、エクスポートまたはインポートされたスキャンのID番号です。

参照情報

"スキャンのエクスポート" ページ252

スキャンを選択して、抑制された検出事項をインポートする

[スキャンを選択して、抑制された検出事項をインポートする(Select a Scan to Import Suppressed Findings)]ダイアログを使用して、抑制された検出事項を現在のスキャンにインポートするスキャンを1つ以上選択します。

注記: スキャンのスケジューリング時やエンタープライズスキャンの実行時には、抑制された検出事項をインポートできません。

抑制された検出事項をインポートするには:

1. 抑制された検出事項のインポート元のスキャン(複数可)のチェックボックスを選択して、[OK]をクリックします。

   [抑制された検出事項のインポート中(Importing Suppressed Findings)]ウィンドウが表示され、インポートの進行状況が表示されます。
2. インポートが完了したら、次のいずれかを実行します。
   - [詳細(Details)]をクリックして、インポートのログファイルを表示します。
   - [閉じる(Close)]をクリックして、[スキャンの誤検出(Scan False Positives)]ウィンドウに誤検出を表示します。

レガシWebサービススキャンのインポート

OpenText DAST 10.00以降では、9.00より前のバージョンのOpenText DASTで作成されたWebサービススキャンに対して最小限のサポートを提供します。これらのスキャンには、現在のユーザインタフェースで適切にレンダリングするために必要な情報がすべて含まれているわけではなく、次のような特性があります。

- ツリービューに正しい構造が表示されない場合があります。
- 操作がツリービューに表示されない場合でも、脆弱性リストに脆弱性が表示されます。これらの脆弱性を選択し、脆弱性情報、および要求と応答を表示できます。
- XmlGridには何も表示されません。
- 再スキャン機能により、Webサービススキャンウィザードが起動され、選択したWSDLがすでに入力されている状態で最初のオプションが選択されます。これにより、Web Service Test Designerがページ3で強制的に開かれます。
- 「脆弱性レビュー」機能は無効になっている必要があります。
- すべてのレポートは、以前のOpenText DASTリリースと同様に機能します。
- スキャンビューは「ReadOnly」モードでレンダリングされます。このモードでは、 **開始(Start)**] ボタン、 **監査(Audit)**] ボタン、および **現在の設定(Current Settings)**] ボタンが無効になります。

OpenTextでは、Webサービスを再スキャンすることをお勧めします。

スキャン設定のインポートとエクスポート

スキャンアクションごとに異なる設定が必要な場合は、XMLファイルに設定を保存し、必要に応じてその設定をロードできます。また、OpenText DASTの出荷時のデフォルト設定を再ロードすることもできます。これらのタスクは、 デフォルト設定(Default Settings)] ウィンドウで実行できます。

ヒント: 設定の管理(Manage Settings)] ウィンドウからスキャン設定ファイルを作成、編集、削除、インポート、およびエクスポートすることもできます。 **編集(Edit)**] をクリックし、 **設定の管理(Manage Settings)**] を選択します。

設定をインポート、エクスポート、または復元するには:

1. **編集(Edit)] > デフォルト設定(Default Settings)]** をクリックします。
   デフォルト設定(Default Settings)] ウィンドウが表示されます。
2. 次の表に従って続行します。

目的...	その場合...
設定をエクスポートする	a. 左ペインの下部にある **設定に名前を付けて保存**

目的...	その場合...
	(Save settings as)]をクリックします。 b. Save Scan Settings (スキャン設定の保存)]ウィンドウで、フォルダを選択してファイル名を入力します。 c. Save]をクリックします。
設定をインポートする	a. 左ペインの下部にある ファイルから設定をロード(Load settings from file)]をクリックします。 b. スキャン設定ファイルを開く(Open Scan Settings File)]ウィンドウで、ファイルを選択します。 c. 開く(Open)]をクリックします。
出荷時のデフォルト設定を復元する	a. 左ペインの下部にある 出荷時のデフォルト設定を復元(Restore factory defaults)]をクリックします。 b. 選択内容を確認するプロンプトが表示されたら、 はい(Yes)]をクリックします。

エンタープライズサーバからのスキャンのダウンロード

次の手順を使用して、エンタープライズサーバ(Fortify WebInspect Enterprise)からOpenText DASTにスキャンをダウンロードします。

1. エンタープライズサーバ(Enterprise Server)]メニューをクリックし、 スキャンのダウンロード(Download Scan)]を選択します。
2. スキャンのダウンロード(Download Scan)]ウィンドウで、使用可能なスキャンのリストから1つ以上のスキャンを選択します。
3. OK]をクリックします。

ダウンロードしたスキャンは、 スキャンの管理(Manage Scans)]ペインのスキャンのリストに追加されます。スキャンの日付は、サイトが最初にスキャンされた日付ではなく、スキャンをダウンロードした日付になります。詳細については、「"スキャンの管理" ページ244」を参照してください。

ログファイルがダウンロードされない

トラフィックセッションファイルを含むログファイルは、Fortify WebInspect EnterpriseからOpenText DASTにセンサスキャンをダウンロードする際にダウンロードされません。スキャンのログファイルを取得して表示するには、Fortify WebInspect Enterpriseからスキャンを手動でエクスポートしてから、そのスキャンをOpenText DASTにインポートする必要があります。詳細については、「"スキャンのインポート" ページ260」を参照してください。

参照情報

"エンタープライズサーバへのスキャンのアップロード" 下

エンタープライズサーバへのスキャンのアップロード

OpenText DASTからエンタープライズサーバ(Fortify WebInspect Enterprise)へスキャンファイルをアップロードするには、次の手順を使用します。

1. OpenText DASTの [**エンタープライズサーバ(Enterprise Server)**] メニューをクリックして、 [**スキャンのアップロード(Upload Scan)**] を選択します。
2. [スキャンのアップロード(Upload Scan(s))] ウィンドウで、 [**スキャン名(Scan Name)**] 列から1つ以上のOpenText DASTスキャンを選択します。

   注記: 別のデータベースのスキャンにアクセスするには、 [**接続(Connections)**] をクリックし、データベースアプリケーション設定で [**スキャン表示の接続設定(Connection Settings for Scan Viewing)**] のオプションを変更します。
3. スキャンごとに、該当するドロップダウンリストから**アプリケーション**および**バージョン**を選択します。

   プログラムはスキャンファイルの「スキャンURL」を基に正しいアプリケーションとバージョンの選択を試みますが、代わりのものを自分で選択しても構いません。
4. [**アップロード(Upload)**] をクリックします。

参照情報

"エンタープライズサーバからのスキャンのダウンロード" 前のページ

Fortify WebInspect Enterpriseでのスキャンの実行

この機能は、OpenText DASTではなく、Fortify WebInspect Enterpriseでスキャンを設定することを望むユーザ向けです。設定を変更してOpenText DASTでスキャンを実行し、最適な設定が得られるまでこのプロセスを繰り返すことができます。その後、開いているスキャンの設定をFortify WebInspect Enterpriseに送信すると、スキャン要求が作成され、次に利用可能なセンサのスキャンキューに配置されます。

Fortify WebInspect Enterpriseでスキャンを実行するには:

1. スキャンを開きます。
2. エンタープライズサーバに接続していない場合は、 [**エンタープライズサーバ(Enterprise Server)**] メニューをクリックして、 [**WebInspect Enterpriseに接続する(Connect to WebInspect Enterprise)**] を選択します。
3. [**スキャン(Scan)**] メニューをクリックし、 [**WebInspect Enterpriseで実行(Run in WebInspect Enterprise)**] を選択します(またはツールバーの適切なボタンをクリックします)。

4. [**WebInspect Enterpriseでスキャンを実行(Run Scan in WebInspect Enterprise)**]ダイアログボックスで、スキャンの名前を入力します。
5. [**アプリケーション(Application)**]と[**バージョン(Version)**]を選択します。
6. [**OK**]をクリックします。

すべての許可チェックに合格するとスキャンが作成され、スキャンに割り当てられる優先度は、役割で許可されている最高の優先度に設定されます(最大3で、これがデフォルトです)。

エンタープライズサーバとの間での設定の転送

この機能は、次の目的で使用します。

- OpenText DAST設定ファイルに基づいてFortify WebInspect Enterpriseスキャンテンプレートを作成し、OpenText DASTからエンタープライズサーバ(Fortify WebInspect Enterprise)にそのテンプレートをアップロードする。
- エンタープライズサーバのスキャンテンプレートに基づいてOpenText DAST設定ファイルを作成し、OpenText DASTにその設定ファイルをダウンロードする。

OpenText DAST設定ファイルとFortify WebInspect Enterpriseスキャンテンプレートの形式は同じではありません。一方の形式のすべての設定がもう一方の形式で複製されるわけではありません。変換手順の説明の後の警告に注意してください。

Fortify WebInspect Enterpriseスキャンテンプレートの作成

Fortify WebInspect Enterpriseスキャンテンプレートを作成するには:

1. OpenText DASTの[**エンタープライズサーバ(Enterprise Server)**]メニューをクリックし、[**転送設定(Transfer Settings)**]を選択します。
2. [転送設定(Transfer Settings)]ウィンドウで、[**ローカル設定ファイル(Local Settings File)**]リストからOpenText DAST設定ファイルを選択します。
3. (オプション)[**表示(View)**]をクリックして、OpenText DAST設定ファイルに表示される設定を確認します。続行するには、[**閉じる(Close)**]をクリックします。

   注記: これは読み込み専用ファイルです。変更は保持されません。
4. Fortify WebInspect Enterpriseでテンプレートの転送先となる**アプリケーション**および**バージョン**を選択します。
5. 必要に応じて、[**更新(Refresh)**]をクリックして、リストに最新の設定ファイルとスキャンテンプレートが含まれていることを確認します。
6. 作成するスキャンテンプレートの名前を入力します。既存のテンプレートの名前を複製することはできません。
7. [**アップロード(Upload)**]をクリックします。

OpenText DASTから抽出されないテンプレート設定はすべて、Fortify WebInspect Enterpriseテンプレートのデフォルト設定を使用します。

- スキャンテンプレートでは、OpenText DAST設定ファイルで使用されるポリシーは指定されません。代わりに、「Use Any」オプションが含まれます。
- OpenText DAST設定ファイルに含まれているクライアント証明書情報はスキャンテンプレートに転送されますが、証明書は送信されません。
- すべてのOpenText DAST設定は、Fortify WebInspect Enterpriseで使用されていない場合でもスキャンテンプレートに保持されます。したがって、元の設定ファイルから作成したスキャンテンプレートに基づいて、後でOpenText DAST設定ファイルを作成すると、OpenText DAST設定は保持されます。

OpenText DAST設定ファイルの作成

OpenText DAST設定ファイルを作成するには:

1. OpenText DASTの [**エンタープライズサーバ(Enterprise Server)**] メニューをクリックし、 [**転送設定(Transfer Settings)**] を選択します。
2. Fortify WebInspect Enterpriseでテンプレートの転送元となる**アプリケーション**および**バージョン**を選択します。
3. [転送の設定(Transfer Settings)] ウィンドウで、リストからスキャンテンプレートを選択します。
4. (オプション) [**表示(View)**] をクリックして、OpenText DAST設定ファイルに表示される設定を確認します。続行するには、 [**閉じる(Close)**] をクリックします。

   注記: これは読み込み専用ファイルです。変更は保持されません。
5. 必要に応じて、 [**更新(Refresh)**] をクリックして、リストに最新の設定ファイルとスキャンテンプレートが含まれていることを確認します。
6. [**ダウンロード(Download)**] をクリックします。
7. 標準のファイル選択ウィンドウを使用して、設定ファイルに名前を付け、保存先を選択し、 [**保存(Save)**] をクリックします。

OpenText DAST設定ファイルでは、スキャンテンプレートで使用されるポリシーは指定されません。代わりに、標準ポリシーが指定されます。

スキャンの発行(Fortify WebInspect Enterprise接続)

注記: このトピックは、Fortify WebInspect EnterpriseがFortify Software Security Centerと統合されている場合にのみ適用されます。

Fortify WebInspect Enterpriseを介して、OpenText DASTからFortify Software Security Centerのサーバにスキャンデータを送信するには、次の手順に従います。

注記: 同じWebサイトまたはアプリケーションを複数回スキャンするときに、Fortify Software Security Centerの脆弱性のステータスを管理する方法については、"Fortify

Software Security Centerへの脆弱性対策の統合" ページ267を参照してください。

1. Fortify WebInspect EnterpriseおよびFortify Software Security Centerを設定します。
2. OpenText DASTでスキャンを実行します(または、インポートまたはダウンロードしたスキャンを使用します)。
3. [エンタープライズサーバ(Enterprise Server)]メニューをクリックして、 [WebInspect Enterpriseへの接続(Connect to WebInspect Enterprise)]を選択します。資格情報の送信を求めるプロンプトが表示されます。
4. フォーカスされているタブでスキャンが開かれていて、そのスキャンのみを発行する場合:
   a. Synchronizeをクリックします。
   b. アプリケーションとバージョンを選択し、 [OK]をクリックします。
   c. 結果を検査します。サマリペインに「発行済みステータス(Published Status)」と「保留中のステータス(Pending Status)」を示すカラムが表示されます。「発行済みステータス」は、このスキャンが最後にFortify WebInspect Enterpriseに発行された時の脆弱性のステータスです。「保留中のステータス」は、このスキャンが発行された後の脆弱性のステータスが何になるかを示します。一部の「保留中のステータス」は、脆弱性が解決済みか、それともまだ存在しているか示すために変更することができます(次のステップ7を参照)。また、 [未検出(Not Found)]という名前の新しいタブが表示されます。このタブには、前回のスキャンでは検出されたものの、現在のスキャンでは検出されていない脆弱性が含まれています。脆弱性にスクリーンショットやコメントを追加したり、脆弱性に誤検出または無視のマークを付けたりすることができます。また、脆弱性を確認して再テストし、スキャン結果を変更して発行の準備を行うことができます。
   d. Publishをクリックします。ステップ7に進みます。
5. スキャンのリストから選択するには:
   a. [エンタープライズサーバ(Enterprise Server)]メニューをクリックして、 [スキャンの発行(Publish Scan)]を選択します。
   b. [スキャンをSoftware Security Centerに発行する(Publish Scan(s) to Software Security Center)]ダイアログボックスで、1つ以上のスキャンを選択します。
   c. アプリケーションとバージョンを選択します。
   d. [次へ(Next)]をクリックします。OpenText DASTは自動的にFortify Software Security Centerと同期します。
6. OpenText DASTには、ステータスおよび重大度別に分類された、発行される脆弱性の数の一覧が表示されます。

   ステータスを判断するために、OpenText DASTは以前に送信された脆弱性(Fortify Software Security Centerと同期して取得されたもの)を現在のスキャンで報告された脆弱性と比較します。これがアプリケーションのあるバージョンに対して初めて送信されたスキャンである場合、すべての脆弱性は「新規(New)」になります。

   脆弱性が以前に報告されているものの現在のスキャンに含まれていない場合、「未検出(Not Found)」のマークが付けられます。見つからなかった理由が、修復されたためか、それともスキャンの設定が異なっているからなのかを判断する必要があります(たとえば、別のスキャンポリシーを使用していた場合や、サイトの別の部分をスキャンした場合、スキャンを途中で終了した場合などがあります)。結果を調べるときに(ステップ4c)、最初のスキャンを除くすべての脆弱性で検出された個々の脆弱性の「保留中のステータス」を変

更できます(サマリペインで脆弱性を右クリック)。ただし、発行時に、OpenText DASTが残りの「未検出(Not Found)」の脆弱性を処理する方法を指定する必要があります。

Fortify Software Security Centerでこれらの「未検出(Not Found)」の脆弱性を保持する(脆弱性が依然として存在することを示すため)には、 **保持: スキャンでまだ「未検出」とマークされているすべての脆弱性をまだ存在していると見なす(Retain: Assume all vulnerabilities still marked "Not Found" in the scan are still present)**]を選択します。

これらの脆弱性を削除する(修復済みであることを示して)には、 **解決: スキャンでまだ「未検出」とマークされているすべての脆弱性を修復済みと見なす(Resolve: Assume all vulnerabilities still marked "Not Found" in the scan are fixed)**]を選択します。

7. このスキャンが、Fortify Software Security Centerで開始されたスキャン要求に応じて実行された場合は、 **[スキャンを、現在のアプリケーションバージョンに対する「進行中」スキャン要求に関連付ける(Associate scan with an "In Progress" scan request for the current application version)**]を選択します。
8. **[発行(Publish)**]をクリックします。

Fortify Software Security Centerへの脆弱性対策の統合

注記: このトピックは、Fortify WebInspect EnterpriseにFortify Software Security Centerが統合されている場合にのみ適用されます。

Fortify Software Security Centerは、ソフトウェアのセキュリティ脆弱性を特定し、順位付けし、修復する、緊密に統合されたソリューションから成るスイートです。OpenText™ Static Application Security Testingからの静的分析スキャンと、OpenText DASTからの動的アプリケーションセキュリティスキャンを保存します。Fortify WebInspect Enterpriseは、複数のOpenText DASTスキャナを管理し、Fortify Software Security Center内の個々のアプリケーションバージョンに直接発行できるスキャン結果を相関させるための中央の場所を提供します。

Fortify WebInspect Enterpriseは、特定のFortify Software Security Centerアプリケーションバージョンのすべての脆弱性の履歴を保持します。OpenText DASTは、スキャンを実行した後、Fortify WebInspect Enterpriseと同期してその履歴を取得し、スキャンの脆弱性と履歴内の脆弱性を比較して、各脆弱性にステータスを割り当てます。次の表で、ステータスについて説明します。

Fortify Software Security Centerのステータス	説明
新規(New)	以前に報告されていない問題。

Fortify Software Security Centerのステータス	説明
既存(Existing)	すでに履歴にあるスキャンの脆弱性。
未検出(Not Found)	履歴にはあるものの、スキャンでは見つからない脆弱性。これは、(a)脆弱性が改善されて存在しなくなった、または(b)最新のスキャンで別の設定が使用されたか、サイトの別の部分がスキャンされたか、または他の何らかの理由で脆弱性が検出されなかったために発生する可能性があります。
解決済み(Resolved)	修復された脆弱性。
復活(Reintroduced)	以前に「解決済み(Resolved)」と報告されたが、現在のスキャンに表示される脆弱性。
依然として問題(Still an Issue)	現在のスキャンで「未検出(Not Found)」であったが、実際には存在する脆弱性。

個々の脆弱性のFortify Software Security Centerのステータスを変更するには、 **検出事項(Findings)**]タブで脆弱性を右クリックし、 **保留中のステータスの変更(Modify Pending Status)**]を選択します。このオプションは、Fortify WebInspect Enterpriseに接続した後にのみ表示され、OpenText DASTをFortify Software Security Centerと同期した後でのみ有効になります。

以下に、脆弱性をFortify Software Security Centerに統合するための仮想の一連のスキャンの例を示します。

最初のスキャン

1. OpenText DASTでターゲットサイトをスキャンします。この例では、1つの脆弱性(Vuln A)のみ検出されたとします。
2. 結果を検査します。脆弱性にスクリーンショットやコメントを追加したり、脆弱性に誤検出または無視のマークを付けたりすることができます。脆弱性を確認、再テスト、および削除することもできます。
3. Fortify Software Security Centerでスキャンをアプリケーションバージョンと同期してから、スキャンを発行します。

2回目のスキャン

1. 2回目のスキャンでVuln Aが再び明らかになり、さらに4つの脆弱性(Vuln B、C、D、およびE)も検出されます。
2. Fortify Software Security Centerでスキャンをアプリケーションバージョンと同期します。

3. 次に、結果を検査します。最初のスキャンを発行するときに監査データ(コメントやスクリーンショットなど)をVuln Aに追加した場合、そのデータは新しいスキャンにインポートされます。
4. スキャンをFortify Software Security Centerに発行します。Vuln Aには「既存」のマークが付けられ、Vuln BからEには「新規」のマークが付けられます。Fortify Software Security Centerシステムには5つの項目が存在することになります。

3回目のスキャン

1. 3回目のスキャンでは、Vuln B、C、およびDは検出されますが、Vuln AもVuln Eも検出されません。
2. Fortify Software Security Centerでスキャンをアプリケーションバージョンと同期します。
3. Vuln Aの再テスト後、実際にはVuln Aは存在すると判断します。その保留中のステータスを「依然として問題(Still an Issue)」に変更します。
4. Vuln Eの再テスト後、Vuln Eは存在しないと判断します。その保留中のステータスを「解決済み(Resolved)」に変更します。
5. スキャンをFortify Software Security Centerに発行します。Vuln B、C、およびDには「既存(Existing)」のマークが付けられます。Fortify Software Security Centerシステムには5つの項目が存在することになります。

4回目のスキャン

1. 4回目のスキャンでは、Vuln AもVuln Bも検出されません。このスキャンでは、Vuln C、D、E、およびFが検出されます。
2. Fortify Software Security Centerでスキャンをアプリケーションバージョンと同期します。
3. Vuln Eは以前に解決済みと宣言されたので、そのステータスは「復活(Reintroduced)」に設定されています。
4. 検出されなかった脆弱性を調べます(この例では、AとB)。脆弱性がまだ存在すると判断した場合は、保留中のステータスを「依然として問題(Still an Issue)」に更新します。再テストによって脆弱性が存在しないと確認された場合は、保留中のステータスを「解決済み(Resolved)」に更新します。
5. スキャンをFortify Software Security Centerに発行します。Vuln CおよびDは「Existing(既存)」のマークが付いたままになります。

Fortify Software Security Centerとの同期

注記: このトピックは、Fortify WebInspect EnterpriseにFortify Software Security Centerが統合されている場合にのみ適用されます。

このダイアログボックスを使用して、アプリケーションとバージョンを指定し、Fortify Software Security Centerと同期します。OpenText DASTは次にFortify Software Security Centerから脆弱性のリストをダウンロードし、ダウンロードした脆弱性と現在のスキャンで検出された脆

弱性を比較し、適切なステータス(新規(New)]、 既存(Existing)]、 再導入(Reintroduced)]、または 未検出(Not Found)])を割り当てます。詳細情報については、"Fortify Software Security Centerへの脆弱性対策の統合" ページ267を参照してください。

Fortify Software Security Centerと同期するには:

1. ツールバーの [同期(Synchronize)]をクリックします。
2. アプリケーションを選択します。
3. バージョンを選択します。
4. [OK]をクリックします。

第5章:OpenText DAST機能の使用

この章では、Server ProfilerやWeb Macro Recorderツールなど、OpenText DASTで使用できる特定のツールについて説明します。また、スキャン結果を検査し、スキャン中に検出された脆弱性を処理する方法も説明します。OpenText DAST API、正規表現、およびOpenText DASTポリシーの使用法を説明します。この章には、コンプライアンステンプレートとOpenText DASTのレポーティング機能に関する情報も含まれています。

OpenText DASTで使用できるすべてのツールの詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』を参照してください。

再テストと再スキャン

OpenText DASTには、検出された脆弱性を再テストおよび再スキャンする複数の方法が用意されています。以下を実行できます。

- 個々の脆弱性、すべての脆弱性、または特定の重大度を持つすべての脆弱性を再テストする。詳細については、「"脆弱性の再テスト" 下」を参照してください。
- サイト全体を再スキャンする。詳細については、「"サイトの再スキャン" ページ276」を参照してください。
- 以前のスキャンのデータを新しいスキャンを支援するために再利用する。詳細については、「"スキャンの再利用" ページ277」および「"増分スキャン" ページ278」を参照してください。

脆弱性の再テスト

スキャンの実行と検出された脆弱性の報告が済むと、開発者がコードの修正とサイトの更新を行えるようになります。その後、元のスキャンを開いて再テストのスキャンを行うことで、次が修復されていることを確認できます。

- 選択した脆弱性
- すべての脆弱性
- 特定の重大度を持つすべての脆弱性

OpenText DASTは新しいスキャンを開始して、問題が修復されたかどうかを判断します。再テストのスキャンでは、元のスキャン名の前に「`retest:`」が付くので、元のスキャンと再テストのスキャンを簡単に識別できます。

再テストのスキャン中、再テストのキューに登録されている脆弱性はサマリペインの [検出事項(Findings)] タブに一覧表示され、 [再テストのステータス(Retest Status)] 列には再テストの結果が示されます。

重要! {/b}OpenTextでは、前のバージョンのOpenText DASTを使用して作成されたスキャンで脆弱性を再テストすることはお勧めしません。前のバージョンからのスキャンの再テ

ストは多くのインスタンスで機能すると考えられますが、再テストの際に個々のチェックで同じ脆弱性にフラグが付けられるとは限らないため、常に信頼できるわけではありません。前のバージョンのOpenText DASTからのスキャンを再テストする際に、チェックが同じ脆弱性にフラグを付けないとしても、脆弱性が改善されたことを意味するとは限りません。

再テストのステータスについて

次の表で、 再テストのステータス(Retest Status)] 列に表示される値について説明します。

ステータス	説明
処理中(Processing)	脆弱性は現在再テスト中です。これは一時的なステータスで、再テストが完了すると最終的なステータスに置き換えられます。
検出済み(Detected)	脆弱性は再テストのスキャンで再現されました。
検出なし、相関エラーの可能性(Not Detected, Possible Correlation Failure)	再テストのスキャン中に同じチェックIDを持つ脆弱性が検出されましたが、再テスト中の検出事項と相関が一致しませんでした。 **注記:** 相関とは、OpenText DASTが、同じパラメータまたは場所を使用して脆弱性を固有に識別する方法を指します。
検出なし(Not Detected)	脆弱性は、テスト対象のパラメータまたは場所に存在しません。
サポート対象外	脆弱性は再テストされませんでした。再テストは、この特定の脆弱性に対してサポートされていません。詳細については、「"失敗した脆弱性およびサポート対象外の脆弱性に関する推奨事項" 次のページ」を参照してください。
失敗	特定の脆弱性の再テストが失敗しました。失敗の理由を示す次の失敗ステータスも確認できます。 • 失敗、トリガセッションが見つかりません(Failed, Trigger Session Not Found) • 失敗、トリガセッションの応答がありません(Failed, Trigger Session Response Missing) • 失敗、トリガセッションのステータスコードが異なります(Failed, Trigger Session Status Code Different) 詳細については、「"失敗した脆弱性およびサポート対象外の脆弱性に関する推奨事項" 次のページ」を参照してください。

ステータス	説明
依存関係の失敗 (Dependency Failed)	元のスキャンに存在していた依存関係を検証スキャンで複製できなかったため、再テストを完了できませんでした。

失敗した脆弱性およびサポート対象外の脆弱性に関する推奨事項

再テストのステータスが「失敗」または「サポート対象外」である脆弱性に対して、OpenTextでは、改善の再利用スキャン、または新しいスキャンの実行をお勧めします。改善の再利用スキャンの詳細については、"スキャンの再利用" ページ277を参照してください。

すべての脆弱性の再テスト

スキャンのすべての脆弱性を再テストするには:

- 次のいずれかを実行します。
  - **[スキャンの管理(Manage Scans)]**リストでスキャンを右クリックして、**再スキャン(Rescan)] > 脆弱性の再テスト(Retest Vulnerabilities)] > すべての再テスト(Retest All)]**を選択します。
  - 開いているスキャンの**[スキャン(Scan)]**メニューで、**再スキャン(Rescan)]**ドロップダウンリストをクリックして、**脆弱性の再テスト(Retest Vulnerabilities)] > すべての再テスト(Retest All)]**を選択します。
  - 開いているスキャンのサマリペインの**検出事項(Findings)]**タブで脆弱性を右クリックし、**再テスト(Retest)] > すべての再テスト(Retest All)]**を選択します。

  元のスキャン名の前に「`retest:`」が付けられて、再テストのスキャンが開始します。

特定の重大度を持つすべての脆弱性の再テスト

スキャンの特定の重大度を持つすべての脆弱性を再テストするには:

1. 次のいずれかを実行します。
   - **[スキャンの管理(Manage Scans)]**リストでスキャンを右クリックして、**再スキャン(Rescan)] > 脆弱性の再テスト(Retest Vulnerabilities)] > 重大度別の再テスト(Retest by Severity)]**を選択します。
   - 開いているスキャンの**[スキャン(Scan)]**メニューで、**再スキャン(Rescan)]**ドロップダウンリストをクリックして、**脆弱性の再テスト(Retest Vulnerabilities)] > 重大度別の再テスト(Retest by Severity)]**を選択します。
   - 開いているスキャンのサマリペインの**検出事項(Findings)]**タブで脆弱性を右クリックし、**再テスト(Retest)] > 重大度別の再テスト(Retest by Severity)]**を選択します。
2. 特定の重大度(**重大(Critical)]** **高(High)]**、**中(Medium)]**、**低(Low)]**)を選択します。

注記: ある重大度がコンテキストメニューにない場合、スキャンにはその重大度の脆弱性がありません。

元のスキャン名の前に「retest:」が付けられて、再テストのスキャンが開始します。

選択した脆弱性の再テスト

選択した1つ以上の脆弱性を再テストするには:

1. 開いているスキャンのサマリペインの **検出事項(Findings)]** タブで、次のいずれかを実行します。
   - 1つの脆弱性を再テストするには、その脆弱性を右クリックします。
   - 複数の脆弱性を再テストするには、<CTRL>キーを押しながら脆弱性をクリックしてそれらを選択し、次いで右クリックします。
2. **再テスト(Retest)]> 選択した脆弱性の再テスト(Retest Selected)]** を選択します。

元のスキャン名の前に「retest:」が付けられて、再テストのスキャンが開始します。

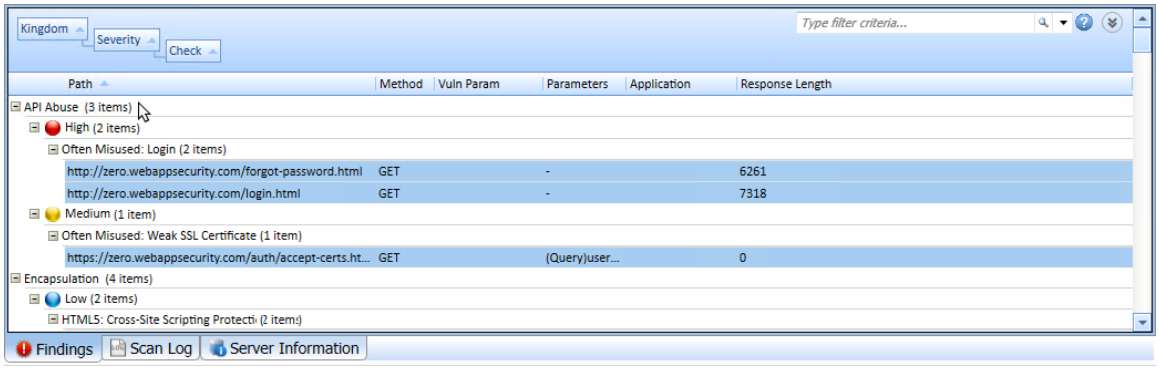
グループ化されたカテゴリの再テスト

検出事項がカテゴリにグループ化されている場合は、グループを選択して、そのカテゴリ内のすべての項目を再テストできます。

グループを再テストするには:

1. 再テストするグループを選択します。

   グループ内のすべての検出事項が選択されます。たとえば、次のイメージでは、検出事項が「界(Kingdom)」、「重大度(Severity)」、「チェック(Check)」の順でグループ化されています。 [APIの誤用]グループが選択されているため、そのカテゴリ内のすべての検出事項が選択されています。



2. 右クリックし、 **再テスト(Retest)]> 選択した脆弱性(Selected)]** を選択します。

ヒント: グループを右クリックすると、カテゴリ内のすべての検出事項を選択し、コンテキストメニューを表示することが1つのアクションで行えます。

グループの詳細については、"サマリペインのフィルタとグループの使用" ページ290を参照してください。

再テストのスキャンの再テスト

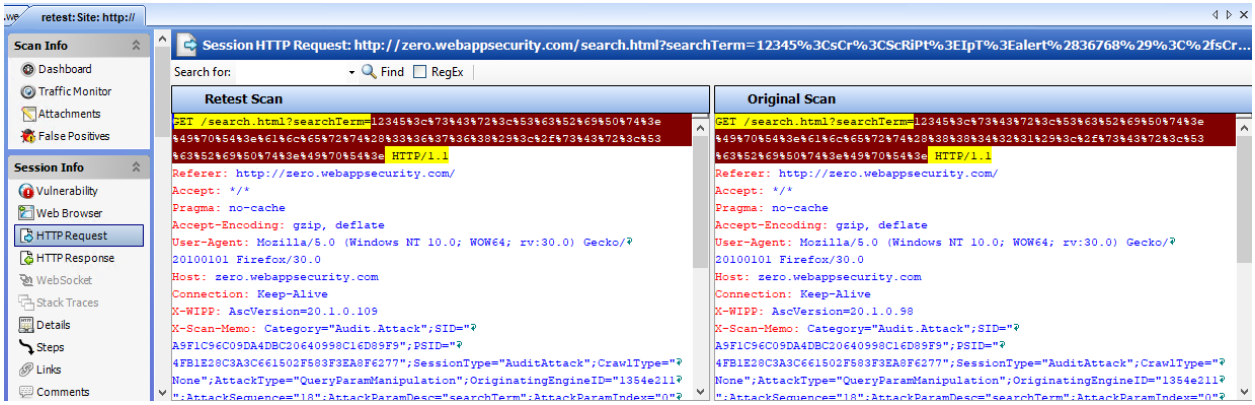
元のスキャンを再テストするのと同じ方法で、再テストのスキャンの検出事項を再テストできます。ただし、再テストできるのは、再テストのステータスが「検出済み(Detected)」の検出事項のみです。それ以外の再テストのステータスを持つ検出事項は再テストされません。

再テストのスキャンログ

スキャンの多数の検出事項を再テストする場合は、再テストのスキャンの [スキャンログ(Scan Log)]タブで結果のスナップショットを確認できます。

比較ビュー

再テストのスキャンで脆弱性を選択する場合、両方のスキャンからの特定のデータをデュアルペインビューで確認できます。 [**HTTP要求(HTTP Request)**]、 [**HTTP応答(HTTP Response)**]、または [**ステップ(Steps)**]を選択して、再テストのスキャンと元のスキャンを比較するデュアルペインビューを表示します。元のスキャンが使用できない場合は、再テストのスキャンのデータだけが表示されます。



[HTTP要求(HTTP Request)]ビューおよび [HTTP応答(HTTP Response)]ビューでデータを検索するには:

1. [**検索対象(Search for)**]フィールドに検索用語を入力します。
2. 必要に応じて、検索条件で正規表現を使用するには、 [**RegEx**]オプションを選択します。
3. [**Find**]をクリックします。

   データが見つかった場合は、再テストのスキャンと元のスキャンの両方で強調表示されます。

詳細については、「"HTTP要求(HTTP Request)" ページ90」、「"HTTP応答(HTTP Response)" ページ90」、および「"ステップ(Steps)" ページ91」を参照してください。

再テストのスキャンの保持または削除

開いているスキャンを閉じると、OpenText DASTはそれが再テストのスキャンであるかどうかを検出します。次の条件が満たされた場合は、スキャンの保持についてプロンプトが表示されま

す。

- 再テストのスキャンである。
- 親スキャンがスキャンデータベースに存在する。
- 以前にそのスキャンのプロンプトが表示されたことがない。

これらの条件が満たされた場合、「**スキャン"retest:<*ScanName*>"を保持しますか? (Do you want to keep the scan "retest:<ScanName>?)**」というメッセージが表示されます。これらの条件を満たす再テストのスキャンのタブを複数閉じると、再テストのスキャンごとにプロンプトが表示されます。

次のいずれかを実行します。

- 再テストのスキャンを保持するには、 **[はい(Yes)]**をクリックします。
  スキャンが保存され、 **[最近開いたスキャン(Recently Opened Scans)]**リストに追加されます。さらに、プロンプトが再び表示されないようにスキャンの設定にフラグが付きます。このフラグは、スキャンがエクスポートされて、別のスキャンデータベースにインポートされた場合でも保持されます。
- 再テストのスキャンを削除するには、 **[いいえ(No)]**をクリックします。
  [スキャンの削除(Deleting Scans)]ウィンドウが表示されます。スキャンが削除されたら、**[完了(Done)]**をクリックします。

サイトの再スキャン

再スキャン機能を使用すると、開いたスキャンまたは選択したスキャンから、元のスキャン設定が事前に読み込まれたスキャンウィザードに簡単に移行できます。更新されたサイトに対して(元のスキャンで使用されたのと同じ設定を使用して)同一のスキャンを実行して、以前に検出された脆弱性が修復されていることと、別の脆弱性が入り込んでいないことを確認できます。また、一部の設定を微調整して、Web探索または監査を改善することもできます。

スキャンの再利用にも2つのオプションがあります。 **[増分の再利用(Reuse Incremental)]**と **[改善の再利用(Reuse Remediation)]**です。詳細については、「"スキャンの再利用" 次のページ」を参照してください。

再スキャン機能は、スキャンツールバーの **[再スキャン(Rescan)]**ボタンと、 **[スキャンの管理(Manage Scans)]**ペインで選択したスキャンに対する **[再スキャン(Rescan)]**ボタン(およびショートカットメニュー)の2箇所で利用できます。

1. 次のいずれかを実行します。
   - スキャンを開き、 **[再スキャン(Rescan)]**をクリックして **[スキャンを再度実行(Scan Again)]**を選択します。
   - OpenText DASTの **[開始(Start)]**ページで、 **[スキャンの管理(Manage Scans)]**をクリックします。その後スキャンを選択して **[再スキャン(Rescan)]**をクリックします。
2. スキャンウィザードを使用して、元のスキャンに使用した設定を変更することもできます。

注記: スキャン名はデフォルトで「<original_scan_name>-1」に設定されます。再スキャンの再スキャンを実行する場合、デフォルト名に追加される整数は1ずつインクリ

メントされます。

3. スキャンウィザードの最後のステップで、 **[スキャン(Scan)]**をクリックします。

スキャンの再利用

スキャンの再利用では、以前のスキャンのデータを新しいスキャンを支援するために使用します。再利用スキャンには、次の2つのスキャンが関係しています。

- 再利用スキャン。実行しようとしている新しいスキャンです。
- ソーススキャンまたはベーススキャン。再利用スキャンの完了に必要な作業と時間を短縮するためにデータが使用されるスキャンです。

再利用のオプション

スキャンの再利用には、4つのオプションがあります。

- **増分の再利用(Reuse Incremental)** -新しい攻撃露呈部分を見つけます。このスキャンでは通常のWeb探索を実行し、各セッションをベーススキャンと比較します。ベーススキャンに存在しなかった新しいセッションだけが監査されます。詳細については、「"増分スキャン" 次のページ」を参照してください。
- **改善の再利用(Reuse Remediation)** -ベーススキャンで検出された脆弱性を探します。このスキャンでは、ベーススキャンでフラグが設定されたチェックのみを含むポリシーが作成され、このカスタムポリシーを使用してサイトが再び監査されます。したがって、このスキャンでは、ベーススキャンでフラグが設定されたチェックだけが調査されます。

改善スキャンと脆弱性の再テストの違い

改善スキャンでは、ベーススキャンでフラグが設定された脆弱性に直接由来する縮小されたポリシーを、ベーススキャンで脆弱だったセッションだけでなく、改善スキャンのすべてのセッションに適用します。

たとえば、ベーススキャンにおいて、セッションAでクロスサイトスクリプティング(XSS)が検出され、セッションBでは検出されなかったとします。その後、セッションAではXSSが修復されたものの、セッションBではこれが作成されました。脆弱性の再テストのオプションではセッションBの脆弱性を発見できませんが、改善スキャンなら発見できます。したがって改善スキャンでは、以前に検出された脆弱性に関して、すべての既知の攻撃露呈部分が評価されます。

スキャンの再利用に関するガイドライン

スキャンを再利用する場合は、次のガイドラインに従います。

- 再利用スキャンを実行するマシンでベーススキャンが利用できる必要があります。
- ベーススキャンは、再利用スキャンと同じデータベースに存在する必要はありません。

スキャンの再利用

スキャンを再利用するには:

1. 次のいずれかを実行します。
   - 開いているスキャンから **再スキャン(Rescan)**]をクリックし、ドロップダウンメニューから目的の再利用オプションを選択します。
   - [スキャンの管理(Manage Scans)]ページでスキャンを右クリックして **再スキャン(Rescan)**]をクリックし、必要な再利用オプションをメニューから選択します。
   - [スキャンの管理(Manage Scans)]ページでスキャンを選択して **再利用(Rescan)**]をクリックし、必要な再利用オプションをドロップダウンメニューから選択します。

   再スキャンのオプションの詳細については、"再利用のオプション" 前のページを参照してください。
2. スキャンウィザードを使用して、元のスキャンに使用した設定を変更することもできます。

   ヒント: 増分スキャンでは、新しい攻撃露呈部分を検出するために設定を変更することが役に立つ場合があります。ただし、改善スキャンの場合、設定の変更はお勧めしません。

   注記: デフォルトでは、選択した再利用スキャンのタイプがベーススキャン名の前に付加され、末尾に-1が追加されます。
3. スキャンウィザードの最後のステップで、 **[スキャン(Scan)**]をクリックします。

参照情報

"増分スキャン" 下

増分スキャン

増分スキャンを使用すると、時間の経過とともに変化するWebアプリケーションのエリアを検索および監査すると同時に、すべての検出事項を単一のスキャンに保持できます。このようにするには、増分スキャンを実行し、それらのスキャンをベーススキャンにマージする必要があります。増分スキャンとベーススキャンの詳細については、"スキャンの再利用" 前のページを参照してください。

ベーススキャンと増分スキャンのマージ

ベーススキャンと増分スキャンを単一のスキャンにマージできます。その後、結合したスキャンの攻撃露呈部分を今後の増分スキャンのために使用できます。

増分スキャンを実行した後、増分スキャンとベーススキャンを選択し、右クリックすると、[マージ(Merge)]オプションが表示されます。

重要! {/b}増分スキャンの派生元のベーススキャンをクリックして、 [マージ(Merge)]オプションが有効になっていることを確認する必要があります。

[マージ(Merge)]をクリックすると、増分スキャンがベーススキャンにマージされます。ベーススキャンに、2つのスキャンの和集合が含まれるようになります。マージされた後のスキャンは新しいベーススキャンになります。増分-マージ-増分-マージを無期限に継続的に実行することで、継続的監査または遅延監査のプロセスを作成できます。詳細については、「"

継続的監査による増分" 次のページ」および「"遅延監査による増分" 下」を参照してください。

スキャンをマージするには:

1. [スキャンの管理(Manage Scans)]ページで、ベーススキャンと増分スキャンを選択します。
2. 右クリックして[**マージ(Merge)**]を選択します。

スキャンをマージすると、ベーススキャンと増分スキャンのIDを含むログエントリがスキャンログに書き込まれます。

継続的監査による増分

増分スキャンを使用して、継続的監査のプロセスを導入できます。このプロセスは次のようになります。

1. ベーススキャンを作成します。
2. 増分スキャンが必要な場合:
   a. ベーススキャンから増分監査スキャンを作成します。このスキャン中に、新しい露呈部分が監査されます。
   b. 増分スキャンをベーススキャンとマージします。マージされたスキャンが新しいベーススキャンになります。詳細については、「"ベーススキャンと増分スキャンのマージ" 前のページ」を参照してください。
   c. 増分スキャンを削除します。
   d. ステップ2に戻ります。

遅延監査による増分

増分スキャンを使用して、延期監査のプロセスを導入できます。このプロセスは次のようになります。

1. ベーススキャンを作成します。
2. 新しい増分スキャンが必要な場合:
   a. ベーススキャンからWeb探索のみの増分スキャンを作成します。
   b. 増分スキャンをベーススキャンとマージします。マージされたスキャンが新しいベーススキャンになります。詳細については、「"ベーススキャンと増分スキャンのマージ" 前のページ」を参照してください。
   c. 増分スキャンを削除します。
   d. 新しい攻撃露呈部分が見つかった場合に、ベースライン監査を再開し、新しい露呈部分を監査します。
   e. ステップ2に戻ります。

参照情報

"スキャンの再利用" ページ277

マクロの使用

マクロとは、Webサイトにアクセスしてログインするときに発生するイベントを記録したものです。その後、この記録を使用してスキャンを開始するようにOpenText DASTに指示できます。セッションベースのWebマクロレコーダツールまたはイベントベースのWebマクロレコーダツールを使用してログインマクロを記録することも、基本スキャンウィザードまたはガイド付きスキャンウィザードで作成することもできます。基本スキャンまたはガイド付きスキャンで作成されたマクロは、どちらのタイプのスキャンでも使用できます。

マクロは2種類あります。

- ログインマクロは、Webサイトにアクセスしてログインするときに発生するイベントをWeb Macro Recorderツールを使用して記録したものです。その後、この記録を使用してスキャンを開始するようにOpenText DASTに指示できます。

  ログインマクロを使用するスキャンの [スキャン設定: 認証(Scan Settings: Authentication)] で **[マクロ検証を有効にする(Enable macro validation)]** が選択されている場合、OpenText DASTはスキャンの開始時点でログインマクロをテストして、ログインが成功したことを確認します。マクロが無効で、アプリケーションへのログインに失敗した場合、スキャンは停止し、エラーメッセージがスキャンログファイルに書き込まれます。詳細とトラブルシューティングのヒントについては、「"ログインマクロのテスト" ページ546」を参照してください。

  注記: マクロテストは、2要素認証を含むマクロに対してはサポートされていません。

- ワークフローマクロは、Webサイト内を移動する場合に発生するHTTPイベントをWeb Macro Recorderツールを使用して記録したものです。OpenText DASTは、以前に記録したマクロに含まれているURLのみを監査し、監査中に検出されたハイパーリンクはたどりません。サポートされているマクロは、`.webmacro`ファイル、Burp Proxyキャプチャ、および`.har`ファイルです。

マクロに記録されるアクティビティにより、スキャン設定は無効になります。たとえば [除外URL(Excluded URL)] 設定にURLを指定してから、マクロの作成時にそのURLに実際に移動すると、OpenText DASTでサイトのWeb探索と監査を行うときに、その除外は無視されます。

注記: 記録されたマクロにクッキーヘッダが組み込まれている場合、マクロの再生時にそれがOpenText DASTから送信されることはありません。基本スキャンまたはガイド付きスキャンで記録されたマクロは、どちらのタイプのスキャンでも使用できます。

参照情報

"スキャン設定: 認証" ページ440

"ガイド付きスキャンの実行" ページ112

"基本スキャンの実行(Webサイトスキャン)" ページ199

"ワークフローマクロの選択" 次のページ

"Web Macro Recorderの使用" 次のページ

ワークフローマクロの選択

ワークフロー駆動型のスキャンを実行する場合、Webサイトのナビゲートに使用される、1つ以上のマクロを選択または作成できます。

- **[記録(Record)]** - Web Macro Recorderが開き、マクロを作成できます
- **[編集(Edit)]** - Web Macro Recorderが開き、選択したマクロがロードされます
- **[削除(Remove)]** -選択したマクロを削除します(ただし、ディスクからは削除されません)
- **[インポート(Import)]** - 標準のファイル選択ウィンドウが開き、過去に記録された`.webmacro`ファイル、Burp Proxyキャプチャ、または`.har`ファイルを選択できます。

  重要! {/b}ログインマクロをワークフローマクロと起動マクロのどちらかまたはその両方と組み合わせて使用する場合は、すべてのマクロが同じタイプでなければなりません。すべてが`.webmacro`ファイル、すべてがBurp Proxyキャプチャ、またはすべてが`.har`ファイルのいずれかです。同じスキャンで異なる種類のマクロを使用することはできません。

- **[エクスポート(Export)]** - 標準のファイル選択ウィンドウが開き、記録したマクロを保存できます

マクロを選択または記録したら、必要に応じて許可ホストを指定できます。

参照情報

"マクロの使用" 前のページ

Web Macro Recorderの使用

OpenText DASTには、2つのバージョンのWeb Macro Recorderツールがあります。

- イベントベースのWebマクロレコーダ
- セッションベースのWeb Macro Recorder

Web Macro Recorderツールはいくつかの方法で起動でき、ガイド付きスキャンまたは基本スキャンの設定中や、「スタンドアロン」モードとして知られるいずれかのスキャンの外部でも可能です。詳細については、Webマクロレコーダのヘルプまたは『*OpenText™ Dynamic Application Security Testingツールガイド*』の「Web Macro Recorder」の章を参照してください。

イベントベースのWebマクロレコーダ

OpenText DASTにはイベントベースのWebマクロレコーダツールが2つ含まれています。1つはログインマクロ用、もう1つはワークフローマクロ用です。このドキュメントでは、これらの2つのツールは、特定のログイン関連およびワークフロー関連のコンテンツを除き、一般的に「Webマクロレコーダ」と呼ばれます。

イベントベースのWebマクロレコーダツールは、TruClientテクノロジを使って設計されました。イベントベースの機能とFirefoxブラウザのテクノロジを使用してマクロを記録および再生します。

セッションベースのWeb Macro Recorder

OpenText DASTにはセッションベースのWeb Macro Recorderツールが含まれています。1つはログインマクロ用、もう1つはワークフローマクロ用です。このドキュメントで、これらの2つのツールは、特定のログイン関連およびワークフロー関連のコンテンツを除き、一般に「セッションベースのWeb Macro Recorder」と呼ばれます。

セッションベースのWeb Macro Recorderは、Internet Explorerブラウザテクノロジ(IEテクノロジとも呼ばれます)を使用してマクロを記録および再生します。

参照情報

"マクロの使用" ページ280

Traffic Monitor (Traffic Viewer)

OpenText DASTのナビゲーションペインには、通常、Webサイトまたはwebサービスの階層構造だけが表示され、それに加えて脆弱性が検出されたセッションが表示されます。Traffic MonitorまたはTraffic Viewerを使用すると、OpenText DASTによって送信されたすべてのHTTP要求と、Webサーバから受信した関連するHTTP応答を表示および確認できます。

スキャン実行前にTraffic Monitorのログ記録が有効になっていなかった場合、Traffic MonitorとTraffic Viewerは使用できません。この機能は、デフォルト設定で有効にするか(**編集(Edit)] > デフォルト設定(Default Settings)] > 設定(Settings)] > 全般(General)]**をクリック)、またはスキャンウィザードでスキャンを開始するときに有効にすることができます(詳細なスキャン設定(Detailed Scan Configuration)]ウィンドウの 設定(Settings)]で **Traffic Monitorの有効化(Enable Traffic Monitor)**]を選択)。

Traffic Viewerのトラフィックセッションデータ

元のTraffic Monitorは、スタンドアロンのTraffic Viewerツールになりました。Traffic Viewerには、元のTraffic MonitorとWebProxyツールの両方の機能が組み込まれています。スタンドアロンのTraffic Viewerのトラフィックセッションファイルの形式は、Traffic Monitorの形式とは異なります。スタンドアロンのTraffic Viewerツールの詳細については、Traffic Viewerツールのオンラインヘルプまたは『*OpenText™ Dynamic Application Security Testingツールガイド*』を参照してください。

Traffic Viewerでのトラフィックの表示

Traffic Viewerでトラフィックセッションデータを表示するには:

- 開いているスキャンの [スキャン情報(Scan Info)]パネルで、 **Traffic Monitor**]をクリックします。

  Traffic Viewerツールが開き、ビューにトラフィックセッションデータが表示されます。

参照情報

" [スキャン情報(Scan Info)]パネル" ページ73

Server Profiler

Server Profilerを使用してWebサイトの事前テストを行い、OpenText DASTの特定の設定を変更する必要があるかどうかを判断します。変更が必要だと思われる場合、Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

たとえば、Server Profilerは、サイトに入るために権限付与が必要であるものの、有効なユーザ名とパスワードが指定されていないことを検出するかもしれません。そのままスキャンを続行して著しく質の低い結果を得るのではなく、Server Profilerのプロンプトに従って、続行する前に必要な情報を設定することができます。

同様に、設定では、OpenText DASTが「ファイルが見つからない」の検出を実行しないように指定されていることもあります。このプロセスは、存在しないリソースをクライアントから要求されてもステータス「404 Not Found」を返さないWebサイトで役に立ちます(代わりにステータス「200 OK」が返される場合がありますが、応答にはファイルが見つからないというメッセージが含まれます)。Profilerは、このような手法がターゲットサイトに実装されていると判断した場合、この特徴に対応できるようにOpenText DAST設定を変更することを推奨します。

Server Profilerは、ガイド付きスキャン中に選択することも、[アプリケーション(Application)]設定で有効にすることもできます。特定の情報については、"アプリケーション設定: Server Profiler" ページ488を参照してください。

ツールとしてのServer Profilerの起動

プロファイラをスキャンウィザードの外部でツールとして起動するには、次の手順に従います。

1. OpenText DASTの[**ツール(Tools)**]メニューをクリックし、[**サーバ(Server)プロファイラ(Profiler)**]を選択します。
2. [**URL**]ボックスで、URLまたはIPアドレスを入力または選択します。
3. (オプション)必要に応じて、[**サンプルサイズ(Sample Size)**]を変更します。大規模なWebサイトでは、要件を十分に分析するために、デフォルトのセッション数を超えるセッションが必要な場合があります。
4. [**分析(Analyze)**]をクリックします。
   Profilerは、提案の一覧(または変更が不要であるというステートメント)を返します。
5. 提案を拒否するには、関連するチェックボックスのチェックを外します。
6. ユーザ入力が必要な提案については、要求された情報を入力してください。
7. (オプション)変更した設定をファイルに保存するには:
   a. [**設定の保存(Save Settings)**]をクリックします。
   b. 標準のファイル選択ウィンドウを使用して、設定をSettingsディレクトリのファイルに保存します。

スキャンの開始時にServer Profilerを起動する

スキャンの開始時にProfilerを起動するには、次の手順に従います。

1. 次のいずれかの方法でスキャンを開始します。
   - OpenText DASTの [**開始ページ(Start Page)**] で、 [**基本スキャンの開始(Start a Basic Scan)**] をクリックします。
   - [**ファイル(File)**] > [**新規(New)**] > [**基本スキャン(Basic Scan)**] をクリックします。
   - (ツールバーの) [**新規(New)**] アイコンでドロップダウン矢印をクリックして、 [**基本スキャン(Basic Scan)**] を選択します。
   - OpenText DASTの [**開始ページ(Start Page)**] で、 [**スケジュールされたスキャンの管理(Manage Scheduled Scans)**] をクリックし、 [**追加(Add)**] をクリックしてから [**基本スキャン(Basic Scan)**] を選択します。
2. スキャンウィザードのステップ4(詳細スキャン設定)で、 [**プロファイル(Profile)**] をクリックします([**Profilerを自動的に実行する(Run Profiler Automatically)**] が選択されている場合を除く)。

   Profilerは、提案の一覧(または変更が不要であるというステートメント)を返します。
3. 提案を拒否するには、関連するチェックボックスのチェックを外します。
4. ユーザ入力が必要な提案については、要求された情報を入力してください。
5. [**次へ(Next)**] をクリックします。

結果の検査

スキャンを開始するとすぐに、OpenText DASTではWebアプリケーションのスキャンが開始し、各セッションを示すアイコンがナビゲーションペインに表示されます([**サイト(Site)**] ビューまたは [**シーケンス(Sequence)**] ビューのいずれかを使用)。また、存在する可能性のある脆弱性もサマリペインの [**検出事項(Findings)**] タブで報告されます。詳細については、「"ナビゲーションペイン" ページ61」および「" [**検出事項(Findings)**] タブ" ページ104」を参照してください。

注記: WebサービスおよびAPIスキャンの場合、サイトツリーには、Web Services Definition Language (WSDL)ドキュメントまたはAPI定義ファイルの操作とパラメータを示すアイコンが表示されます。

サマリペインに一覧表示されているURLをクリックすると、関連するセッションがナビゲーションペインで強調表示され、関連する情報が情報ペインに表示されます。詳細については、「"情報ペイン" ページ72」を参照してください。

脆弱なセッションを検出した攻撃が攻撃情報に一覧表示されない場合があります。つまり、ナビゲーションペインで脆弱なセッションを選択してから、 [**セッション情報(Session Info)**] パネルで [**攻撃情報(Attack Info)**] をクリックしたときに、攻撃情報が情報ペインに表示されません。これは、攻撃情報は通常、攻撃が検出されたセッションではなく、攻撃が作成されたセッションに関連付けられているためです。このような場合は、親セッションを選択してから、 [**攻撃**

情報(Attack Info)]をクリックします。詳細については、「" セッション情報(Session Info)]パネル" ページ86」を参照してください。

1つ以上の脆弱性の操作

サマリペインで1つ以上の脆弱性を右クリックすると、ショートカットメニューを使用して次の操作を実行できます。

- **URLのコピー(Copy URL)** - URLをWindowsのクリップボードにコピーします。
- **選択した項目のコピー(Copy Selected Item(s))** -選択した項目のテキストをWindowsクリップボードにコピーします。
- **すべての項目のコピー(Copy All Items)** -すべての項目のテキストをWindowsクリップボードにコピーします。
- **エクスポート(Export)** -項目をCSVファイルにコピーします。
- **ブラウザで表示(View in Browser)** - 1つの脆弱性が選択されている場合に使用できます。ブラウザでHTTP応答をレンダリングします。
- **現在の値によるフィルタ(Filter by Current Value)** - 1つの脆弱性が選択されている場合に使用できます。選択した基準を満たす脆弱性だけを表示するよう制限します。たとえば、 [メソッド(Method)]列で「Post」を右クリックして、 **現在の値によるフィルタ(Filter by Current Value)**]を選択すると、Postメソッドを使用したHTTP要求を送信して検出された脆弱性だけがリストに表示されます。

  注記: フィルタ基準は、サマリペインの右上隅のコンボボックスに表示されます。または、このコンボボックスを使用してフィルタ基準を手動で入力または選択することもできます。追加の詳細および構文ルールについては、"サマリペインのフィルタとグループの使用" ページ290を参照してください。

- **重大度の変更(Change Severity)** -重大度レベルを変更できます。
- **脆弱性の編集** - 1つの脆弱性が選択されている場合に使用できます。 [脆弱性の編集(Edit Vulnerabilities)]ダイアログが表示され、脆弱性のさまざまな特性を変更できます。詳細については、「"脆弱性の編集" ページ296」を参照してください。
- **脆弱性のロールアップ(Rollup Vulnerabilities)** -複数の脆弱性が選択されている場合に使用できます。選択した脆弱性を、OpenText DAST、Fortify WebInspect Enterprise、およびレポート内で「[Rollup]」というタグの接頭部を持つ単一インスタンスにロールアップできます。詳細については、「"脆弱性のロールアップ" ページ299」を参照してください。

  注記: ロールアップされた脆弱性を選択した場合、このメニューオプションは **[脆弱性のロールアップを元に戻す(Undo Rollup Vulnerabilities)]**になります。

- **再テスト(Retest)** - 選択した1つ以上の検出事項、すべての検出事項、または特定の重大度の検出事項の再テストを実行します。詳細については、「"脆弱性の再テスト" ページ271」を参照してください。
- **マーク付けする(Mark as)** -脆弱性に誤検出(説明を追加可能)または無視のフラグを設定します。どちらの場合も、その脆弱性はリストから削除されます。 [スキャン情報(Scan Info)]パネルで **[抑制された検出事項(Suppressed Findings)]**を選択すると、すべての誤検出および無視された脆弱性のリストを表示できます。

注記: 抑制された検出事項を脆弱性に戻すことができます。詳細については、「"抑制された検出事項" ページ83」を参照してください。

- **送信(Send to)** -脆弱性を欠陥に変換し、OpenText Application Lifecycle Management (ALM)データベースに追加します。
- **場所の削除(Remove Location)** -選択したセッションをナビゲーションペイン([サイト(Site)]ビューと [シーケンス(Sequence)]ビューの両方)から削除し、関連する脆弱性もすべて削除します。

注記: 削除された場所(セッション)およびそれに関連する脆弱性を回復できます。詳細については、「"削除されたセッションの回復" ページ304」を参照してください。

- **Web探索(Crawl)** - 1つの脆弱性が選択されている場合に使用できます。選択したURLのWeb探索を再実行します。
- **ツール** - 1つの脆弱性が選択されている場合に使用できます。使用可能なツールのサブメニューを示します。
- **添付ファイル(Attachments)** - 1つの脆弱性が選択されている場合に使用できます。選択したセッションに関連するメモの作成、フォローアップのためのセッションへのフラグ付け、脆弱性のメモの追加、脆弱性スクリーンショットの追加を行うことができます。

グループの操作

グループを右クリックすると、ショートカットメニューで次の操作を実行できます。

- すべてのグループの縮小/展開(Collapse/Expand All Groups)
- グループの縮小/展開(Collapse/Expand Group)
- URLのコピー(Copy URL)
- 選択した項目のコピー(Copy Selected Item(s))
- すべての項目のコピー(Copy All Items)
- エクスポート
- 重大度の変更(Change Severity)
- 脆弱性のロールアップ(Rollup Vulnerabilities)
- マーク付けする(Mark as)
- 送信(Send to)
- 場所の削除(Remove Location)

重大度について

サマリペインに一覧表示されている脆弱性の相対的な重大度は、次の表で説明するように、関連付けられたアイコンによって識別されます。

アイコン	説明
重大	攻撃者がサーバ上でコマンドを実行したり、個人情報を取得および変

アイコン	説明
	更したりできる可能性がある脆弱性。
High	一般に、ソースコード、Webルート外のファイル、および機密性の高いエラーメッセージの表示が可能になります。
中間	機密性が高い可能性のあるHTML以外のエラーまたは問題を示します。
Low	注目すべき問題、またはより高いレベルの問題になる可能性のある問題。
情報	サイト内の興味深い点、または特定のアプリケーションやWebサーバの検出。
ベストプラクティス	Web開発で一般的に認められるベストプラクティスに関連した問題で、サイト品質とサイト開発のセキュリティに関する全体的なプラクティス(またはその欠如)を示す可能性があります。

ナビゲーションペインでの操作

ナビゲーションペインでオブジェクトまたはセッションを選択し、 [セッション情報(Session Info)]パネルで使用可能なオプションを使用してセッションを調査することもできます。詳細については、「"ナビゲーションペイン" ページ61」および「" [セッション情報(Session Info)]パネル" ページ86」を参照してください。

参照情報

"再テストと再スキャン" ページ271

"Webサービスの監査" ページ293

"脆弱性の編集" ページ296

"OpenText DASTユーザインタフェース" ページ46

"削除されたセッションの回復" ページ304

クライアント側ライブラリ分析

ハッカーレベルインサイトのチェックが強化され、National Vulnerability Database (NVD)およびDebrickedヘルスメトリクスからの両方の情報が含められるようになりました。

重要! {/b}スキャンダッシュボードのハッカーレベルインサイトの検出事項数は、サマリペインに一覧表示されているURLの数と一致しない場合があります。現在、ハッカーレベルインサイトの検出事項は悪用可能なものとして検証は行われず、スキャンダッシュボードにおいて個別の脆弱性に分割されません。

NVD情報

[HLI (ハッカーレベルのインサイト)検出ライブラリ(Hacker Level Insights (HLI) Detected Libraries)] のチェックが有効になっているポリシーを選択すると、クライアント側で脆弱なライブラリが検出された場合に、NVDのローカルコピーからCVE (Common Vulnerabilities and Exposures)に関する情報が脆弱性のサマリに含められます。

注記: NVDはOpenText DASTインストーラに同梱されています。NVDはリリースごとに1回更新され、リリースからリリースまでの間に更新されることはありません。

National Vulnerability Database (NVD)の詳細については、https://nvd.nist.gov/を参照してください。

Debrickedヘルスメトリクス

検出されたライブラリがオープンソースの場合、Debrickedのサブスクリプションをお持ちで、かつDebrickedアクセストークンを使ってOpenText DASTが設定してあるなら、そのライブラリの寄稿者、普及度、およびセキュリティに関する情報がDebrickedデータベースから取得され、脆弱性のサマリに含められます。Debrickedへのアクセスは、`WIConfig`プログラムを使用して設定します。詳細については、『OpenText™ Dynamic Application Security Testingインストールガイド』を参照してください。

ローカルNVDを拡張して、最新のCVEを含めるDebricked設定もあります。ローカルNVD内にCVEのレコードがない場合、CVEとその説明に関するデータはDebrickedデータベースから取得されます。

また、Debrickedの情報には、オープンソースプロジェクト用の関連するGitHubセキュリティアドバイザリ(GHSA)情報が含まれる場合があります。

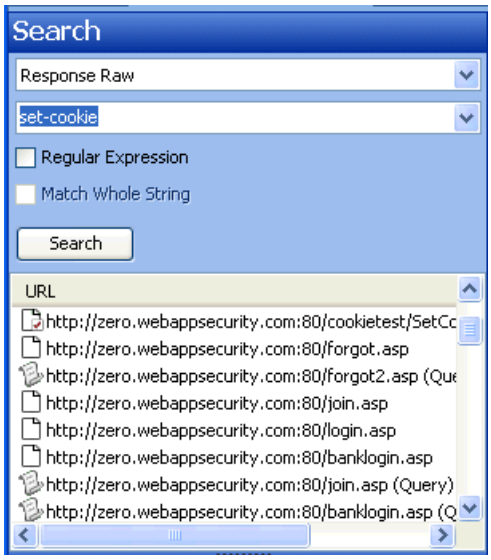
Debrickedヘルスメトリクスの詳細については、https://portal.debricked.com/project-health-45を参照してください。GitHubセキュリティアドバイザリの詳細については、https://docs.github.com/を参照してください。

アクセス状況がDebrickedコンテンツに及ぼす影響

スキャンの開始時にDebrickedサービスがダウンしている場合、または何らかの理由で到達不可能な場合、スキャンは続行します。しかし、スキャンの完了時にDebrickedサービスへのアクセスが確立していない場合は、Debricked情報がスキャン結果に含められません。

検索(Search)]ビュー

検索(Search)]ビューでは、すべてのセッションでさまざまなHTTPメッセージコンポーネントを検索できます。たとえば、ドロップダウンから **応答の生データ(Response Raw)**]を選択し、検索文字列として「**set-cookie**」を指定すると、HTTP応答の生データに「set-cookie」コマンドが含まれるすべてのセッションがOpenText DASTに一覧表示されます。



検索(Search)]ビューを使用するには:

1. ナビゲーションペインで、 **検索(Search)**]をクリックします(ペインの下部)。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。

   すべてのボタンが表示されてはいない場合は、ボタンリストの下部にある **ボタンの設定(Configure Buttons)**]ドロップダウンリストをクリックし、 **他のボタンを表示(Show More Buttons)**]を選択します。
2. 一番上のリストから、検索するエリアを選択します。
3. コンボボックスで、検索する文字列を入力または選択します。
4. 文字列が正規表現を表している場合は、 **正規表現(Regular Expression)**]チェックボックスをオンにします。詳細については、「"正規表現" ページ354」を参照してください。
5. 検索文字列と完全に一致する文字列全体をHTTPメッセージ内で検索するには、 **文字列全体を照合する(Match Whole String)**]チェックボックスをオンにします。完全一致では、大文字と小文字は区別されません。

   このオプションは、特定の検索ターゲットには使用できません。
6. **検索(Search)**]をクリックします。

参照情報

"OpenText DASTユーザインタフェース" ページ46

サマリペインのフィルタとグループの使用

このトピックでは、サマリペインでフィルタおよびグループを使用する方法について説明します。

フィルタの使用

指定した基準に一致する項目のサブセットを表示するには、次の2つの方法のいずれかを使用します。

- ペインの右上隅にあるコンボボックスを使用してフィルタ基準を入力します。

  注記: フィルタ基準ボックスをクリックして<CTRL> + <Space>を押すと、使用可能なすべてのフィルタ基準のポップアップリストが表示されます。次に、その基準の値を入力します。

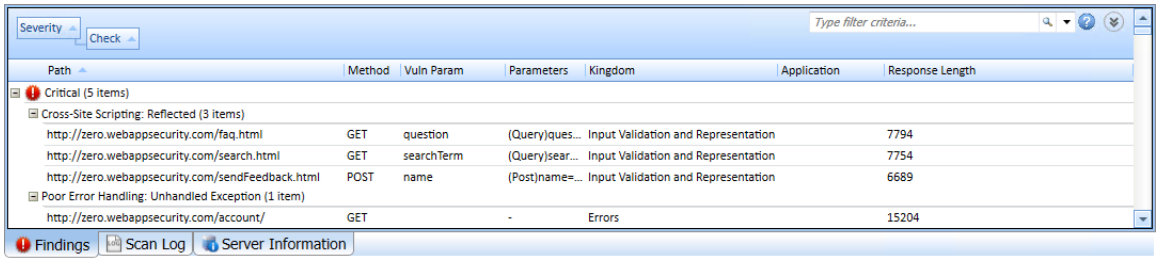
- 任意の列の値を右クリックし、ショートカットメニューから **[現在の値でフィルタ(Filter by Current Value)]** を選択します。

このフィルタ機能は、サマリペインの **[スキャンログ(Scan Log)]** を除くすべてのタブで使用できます。

フィルタなし

次の例は、 **[検出事項(Findings)]** タブで項目にフィルタが適用されていない状態を示しています。

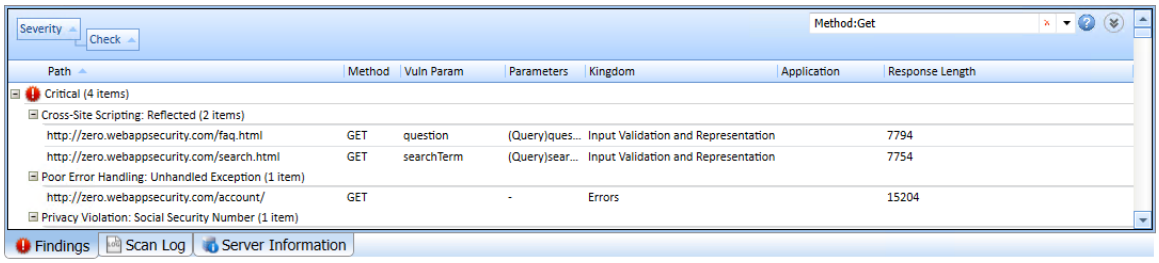
フィルタが適用されていないサマリペインのイメージ



「Method:Get」でフィルタされている場合

次の例は、フィルタ基準ボックスに「Method:Get」と入力した後に表示された内容です。

フィルタが適用されているサマリペインのイメージ



コンボボックスにフィルタ基準(Method:Get)が表示されており、ここに赤いXも表示されていることに注意してください。このXをクリックするとフィルタが削除され、フィルタ適用前のリストが再び表示されます。

複数のフィルタの指定

フィルタ基準コンボボックスに基準を入力するときに複数のフィルタを指定するには、フィルタをカンマで区切ります(「Parameter:noteid, Method:GET」など)。

フィルタ基準

次の識別子を入力できます。

- application -脆弱性が検出されたアプリケーションまたはフレームワーク
- check -チェック名
- checkid - SecureBaseからのチェックID番号
- cookienamerp - HTTP応答のクッキーの名前
- cookienamerq - HTTP要求のクッキーの名前
- cookievaluerp - HTTP応答のクッキーの値
- cookievaluerq - HTTP要求のクッキーの値
- cwe - CWE (Common Weakness Enumeration) ID
- duplicates - OpenText DAST Agentにより検出された重複
- filerq - HTTP要求のファイル名と拡張子
- headernamerp - HTTP応答ヘッダ名
- headernamerq - HTTP要求ヘッダ名
- headervaluerp - HTTP応答ヘッダ値
- headervaluerq - HTTP要求ヘッダ値
- kingdom - 7つの有害な界の値(詳細については、「"アプリケーション設定: 全般" ページ 480」を参照)。

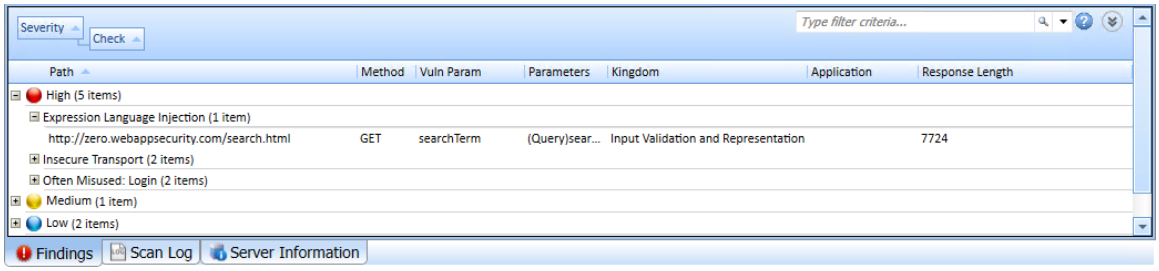
- location -リソースを識別するパスとパラメータ
- manual -手動で追加された場所(構文はmanual:Trueまたはmanual:False)
- method - HTTPメソッド(GET、POST)
- methodrq - HTTP要求で指定されたメソッド
- parameters - HTTP要求で指定されたパラメータ
- path -リソースを識別するパス(パラメータなし)
- pendstatus -スキャンがFortify Software Security Centerに発行される場合のステータス
- rawrp -生のHTTP応答
- rawrq -生のHTTP要求
- responselength -脆弱なセッションの応答サイズ(バイト単位)
- reteststatus -再テストステータスの値(値のリストについては、"脆弱性の再テスト" ページ 271を参照)。
- sessiondataid -セッションデータ識別子(ナビゲーションペインでセッションを右クリックし、 [現在のセッションでフィルタ(Filter by Current Session)]を選択します)
- severity -脆弱性に割り当てられた重大度(critical、high、medium、low)
- stack - OpenText DAST Agentから返されるスタックトレース(構文はstack:Trueまたはstack:False)
- statuscode - HTTPステータスコード
- typerq -要求のタイプ: query、post、またはSOAP
- vparam -脆弱性パラメータ

グループの使用

列ヘッダに基づいて、項目をカテゴリにグループ化できます。これを行うには、ヘッダをドラッグして、ペイン上部のグループエリアにドロップするだけです。

次の画像の検出事項は、重大度別にグループ化され、次にチェック名別にグループ化されています。

グループを使用したサマリペインのイメージ



列ヘッダを右クリックすると、グループ化とフィルタリングに関連する次のショートカットメニュー項目がOpenText DASTに表示されます。

- [フィールドでグループ化(Group by Field)] -選択したフィールドに基づいて脆弱性をグループ化します。

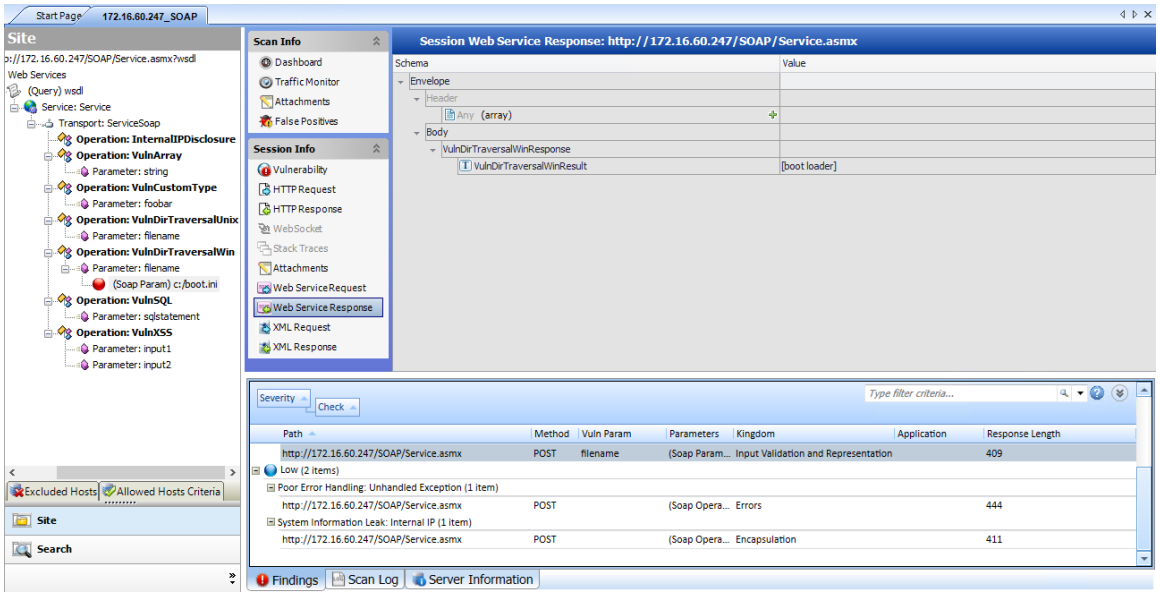
- [ボックスでグループ化(Group by Box)]-列ヘッダに基づいてグループを編成できる[グループ基準(Group By)]エリアが表示されます。
- [列(Column)]-表示する列を選択できます。
- [デフォルトビューとして保存(Save as Default View)]-現在のグループ化方法をすべてのスキャンのデフォルトとして保存します。
- [デフォルトビューにリセット(Reset Default View)]-グループ化方法を、作成したデフォルトビューに戻します。
- [出荷時設定にリセット(Reset Factory Settings)]-グループ化方法を元のビューに戻します([重大度(Severity)]>[チェック(Check)])。

Webサービスの監査

Webサービスは、(ユーザではなく)他のアプリケーションと通信し、情報の要求に応答するプログラムです。ほとんどのWebサービスは、SOAP (Simple Object Access Protocol)を使用して、Webサービスと、情報要求を開始したクライアントWebアプリケーションとの間でXMLデータを送信します。Webページの表示方法のみを説明するHTMLとは異なり、XMLは構造化されたデータを説明し、含むためのフレームワークを提供します。クライアントWebアプリケーションは、返されたデータを即座に理解し、その情報をエンドユーザに表示できます。

WebサービスにアクセスするクライアントWebアプリケーションは、WSDL (Web Services Description Language)ドキュメントを受け取り、サービスとの通信方法を理解します。WSDLドキュメントには、Webサービスに含まれるプログラミングされたプロシージャ、これらのプロシージャに必要なパラメータ、およびクライアントWebアプリケーションが受け取る戻り情報のタイプが記述されています。

Webサービススキャンのイメージ



[セッション情報(Session Info)]パネルで使用可能なオプション

次の表に、[セッション情報(Session Info)]パネルで使用可能なオプションを示します。

オプション	定義
脆弱性(Vulnerability)	ナビゲーションペインで選択されているセッションの脆弱性情報を表示します。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。
HTTP要求(HTTP Request)	OpenText DASTから、スキャン対象のサイトをホストするサーバに送信された生HTTP要求を表示します。
HTTP応答(HTTP Response)	OpenText DASTの要求に対するサーバの生HTTP応答を表示します。 **注記:** Flash (.swf)ファイルを選択した場合、OpenText DASTはバイナリデータの代わりにHTMLを表示します。これにより、OpenText DASTは読み取り可能なフォーマットでリンクを表示できます。
スタックトレース(Stack Traces)	この機能は、OpenText DAST Agentがターゲットサーバにインストールされ、実行されているときにこのエージェントをサポートするように設計されています。特定のチェック(SQLインジェクション、コマンド実行、クロスサイトスクリプティングなど)の場合、OpenText DAST AgentはOpenText DAST HTTP要求を傍受し、ターゲットモジュールでランタイム分析を実行します。この分析によって脆弱性が存在することが確認されると、OpenText DAST AgentはHTTP応答にスタックトレースを追加します。開発者は、このスタックトレースを分析して、改善が必要なエリアを調査できます。
添付ファイル(Attachments)	選択されているセッションに関連付けられているすべてのメモ、フラグ、およびスクリーンショットを表示します。 添付ファイルを作成するには、次のいずれかを実行します。 • ナビゲーションペインで操作または脆弱性を右クリックし、ショートカットメニューから **[添付ファイル(Attachments)]** を選択します。 • サマリペインの **[検出事項(Findings)]** タブでURLを右クリックし、ショートカットメニューから **[添付ファイル(Attachments)]** を選択します。詳細については、「"サマリペイン" ページ104」を参照してください。

オプション	定義
	• ナビゲーションペインで操作または脆弱性を選択し、 **セッション情報(Session Info)**]パネルから **添付ファイル(Attachments)**]を選択し、(情報ペインの) **追加(Add)**]メニューをクリックします。 OpenText Application Lifecycle Management (ALM)に問題を送信するたびに、OpenText DASTによってメモがセッション情報に自動的に追加されます。
Webサービス要求(Web Service Request)	要求のSOAPエンベロープ、ヘッダ、および本文要素を、開かれたビューで表示します。
Webサービス応答(Web Service Response)	応答のSOAPエンベロープ、ヘッダ、および本文要素を、開かれたビューで表示します。
XML要求(XML Request)	要求に埋め込まれている関連XMLスキーマが表示されます(Webサービススキャンで WSDLオブジェクトを選択した場合に使用可能)。
XML応答(XML Response)	応答に埋め込まれている関連XMLスキーマが表示されます(Webサービススキャンで WSDLオブジェクトを選択した場合に使用可能)。

Webサービス脆弱性スキャンの実行方法の詳細については、「"APIスキャンウィザードの使用" ページ165」を参照してください。

脆弱性スクリーンショットの追加と表示

脆弱性スクリーンショットを追加するには:

1. 次のいずれかを実行して脆弱性を選択します。
   - サマリペインの **検出事項(Findings)**]タブで、脆弱なURLを右クリックします。詳細については、「" 検出事項(Findings)]タブ" ページ104」を参照してください。
   - ナビゲーションペインで、脆弱なセッションまたはURLを右クリックします。詳細については、「"ナビゲーションペイン" ページ61」を参照してください。
2. ショートカットメニューで、 **添付ファイル(Attachments)] > 脆弱性スクリーンショットの追加(Add Vulnerability Screenshot)]**をクリックします。

   注記: もう1つの方法として、脆弱性を選択し、 **セッション情報(Session Info)**]パネルで **添付ファイル(Attachments)**]をクリックしてから、(情報表示エリアの) **追加(Add)**]メニューでコマンドを選択する方法があります。詳細については、「"情報ペイン" ページ72」を参照してください。

3. 複数の脆弱性があるセッションを選択した場合は、1つ以上の脆弱性の横にあるチェックボックスをオンにします。
4. [名前(Name)]ボックスにスクリーンショットの名前(最大40文字)を入力します。
5. 次のいずれかの方法でイメージファイルを選択します。
   - 参照ボタン...をクリックし、標準のファイル選択ウィンドウでファイルを選択します。
   - [クリップボードからコピー(Copy from Clipboard)]をクリックして、Windowsクリップボードの内容を保存します。

     注記: 複数の脆弱性を選択した場合でも、指定できるイメージファイルは1つだけです。
6. (オプション)選択した脆弱性スクリーンショットに関連するメモを入力します。
7. [OK]をクリックします。

選択したセッションのスクリーンショットの表示

[セッション情報(Session Info)]パネルの[添付ファイル(Attachments)]をクリックすると、選択したセッションのメモ、フラグ、およびスクリーンショットを表示できます。

すべてのセッションのスクリーンショットの表示

[スキャン情報(Scan Info)]パネルの[添付ファイル(Attachments)]をクリックすると、すべてのセッションのメモ、フラグ、およびスクリーンショットを表示できます。

参照情報

"脆弱性のメモ" ページ304

"フォローアップのためのセッションへのフラグ設定" ページ302

"スキャンメモの使用" ページ302

脆弱性の編集

OpenText DASTがアプリケーションの脆弱性を評価した後、以下のようなさまざまな理由で結果を編集および保存できます。

- **セキュリティ**- HTTP要求または応答にパスワード、アカウント番号、またはその他の機密データが含まれている場合は、スキャン結果を組織内の他のユーザが利用できるようにする前に、この情報を削除または変更できます。
- **訂正**- OpenText DASTが「誤検出」を報告する場合があります。これは、OpenText DASTが脆弱性の可能性を示す兆候を検出したが、開発者がさらに調査することにより、問題が実際には存在しないと判断された場合に発生します。セッションから脆弱性を削除するか、セッション全体を削除できます。または、その報告を誤検出として指定することもできます。([サイト(Site)]または[シーケンス(Sequence)]ビューでセッションを右クリックし、

[マーク付けする(Mark As)] > [誤検出(False Positive)] の順に選択)。

- **重大度の変更**- OpenText DASTの脆弱性のランク付けが適切ではないと思われる場合は、次のスケールを使用して別のレベルを割り当てることができます。

範囲	重大度
0 - 9	通常
10	情報
11 - 25	Low
26 - 50	中間
51 - 75	High
76 - 100	重大

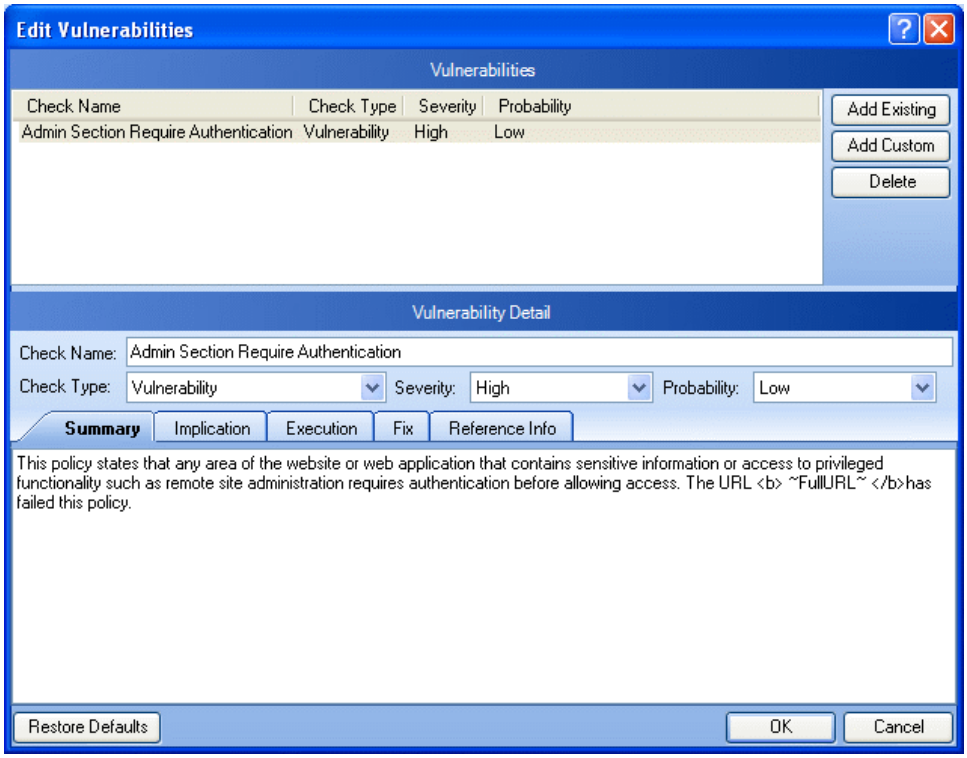
- **レコードの保持**-個々の脆弱性に関連付けられたレポートフィールド(サマリ(Summary)、実行(Execution)、推奨(Recommendation)、実装(Implementation)、修復(Fixes)、および参照(References))を変更できます。たとえば、実際に問題を修復した方法を説明するパラグラフを [修復(Fixes)] セクションに追加できます。
- **拡張**-新しい脆弱性を検出した場合、その脆弱性を定義して、カスタム脆弱性としてセッションに追加できます。

脆弱なセッションの編集

脆弱なセッションを編集するには:

1. 次のいずれかを実行してセッションを選択します。
   - **サマリ**ペインの [検出事項(Findings)] タブで、脆弱なURLを右クリックします。または、
   - ナビゲーションペインで、セッションまたはURLを右クリックします。
2. ショートカットメニューから [脆弱性の編集(Edit Vulnerability)] を選択します。

[脆弱性の編集(Edit Vulnerabilities)]ウィンドウが開きます。



3. セッションに複数の脆弱性が含まれる場合は、1つの脆弱性を選択します。
4. 既存の脆弱性(つまり、データベースに存在する脆弱性)をセッションに追加するには、**[既存のものを追加(Add Existing)]**をクリックします。
   a. [既存の脆弱性の追加(Add Existing Vulnerability)]ウィンドウで、脆弱性名の一部、または完全な脆弱性ID番号またはタイプを入力します。

      注記: *文字と%文字は、ワイルドカードとして使用でき、相互に交換可能です。ただし、ワイルドカードは、文字列の先頭、末尾、または先頭と末尾でのみ使用できます。文字列の中に含まれている場合(「mic*soft」など)、これらの文字はワイルドカードとして機能しません。

   b. **[検索(Search)]**をクリックします。
   c. 検索によって返される脆弱性を1つ以上選択します。
   d. [OK]をクリックします。
5. カスタム脆弱性を追加するには、**[カスタムの追加(Add Custom)]**をクリックします。
   次に、ステップ7の説明に従って脆弱性を編集できます。
6. 選択したセッションから脆弱性を削除するには、**[削除(Delete)]**をクリックします。
7. 脆弱性を変更するには、**[脆弱性の詳細(Vulnerability Detail)]**セクションから別のオプションを選択します。[サマリ(Summary)]、[意味(Implication)]、[実行(Execution)]、[修復(Fix)]、および[参照情報(Reference Info)]の各タブに表示される説明を変更することもできます。
8. [OK]をクリックして変更を保存します。

脆弱性のロールアップ

一部のサイトには、サイト全体に特有の脆弱性のクラスが含まれています。たとえば、入力の検証がないために、サイト全体にわたり、すべてのパラメータに対するすべてのPOSTおよびGETメソッドに、クロスサイトスクリプティングの脆弱性が存在する場合があります。これは、サマリペインの [検出事項(Findings)] タブにクロスサイトスクリプティングの脆弱性が多数一覧表示されるという意味です。OpenText DAST、Fortify WebInspect Enterprise、およびレポートでは、開発チームの負担を軽減するため、このような脆弱性をロールアップして、先頭に「[Rollup]」というタグを付けた単一のインスタンスにできます。

ロールアップされた脆弱性の挙動

複数の脆弱性を選択してロールアップ機能を使用すると、最初に選択した脆弱性を除くすべての脆弱性は「無視」としてマーク付けされます。最初に選択された脆弱性はそのまま表示されて、ロールアップを代表します。選択した残りの脆弱性は「無視」としてマーク付けされますが、 [削除された項目の回復(Recover Deleted Items)] ウィンドウに無視された脆弱性として表示されることはありません。

注意! {/b}脆弱性をロールアップすることは、それらの根本原因が同じであり、その根本原因を修復すればロールアップされたすべての脆弱性が修復されることを意味しています。以降のスキャンでは、ロールアップされた脆弱性が検出された場合、自動的に無視されます。ロールアップされた脆弱性の中に根本原因の異なるものがあっても、同様に無視されてしまいます。

ロールアップのガイドライン

脆弱性のロールアップには、次のガイドラインが適用されます。

- 脆弱性のロールアップを含むスキャンは、再スキャンと一括再テストができます。
- 一括再テストでは、表示されている脆弱性のみが再テストされます。残りの脆弱性は無視され、再テスト時にロールアップとして表示されません。
- ロールアップはスキャンに対してローカルであり、他のスキャンには伝播されません。
- ロールアップ機能は、ロールアップされていない複数の脆弱性を選択した場合にのみ使用できます。現在ロールアップされている脆弱性が誤って選択された場合、ショートカットメニューに [脆弱性のロールアップ(Rollup Vulnerability)] オプションは表示されません。
- ロールアップの取り消しは、現在ロールアップされている脆弱性を1つだけ選択した場合にのみ行うことができます。

脆弱性のロールアップ

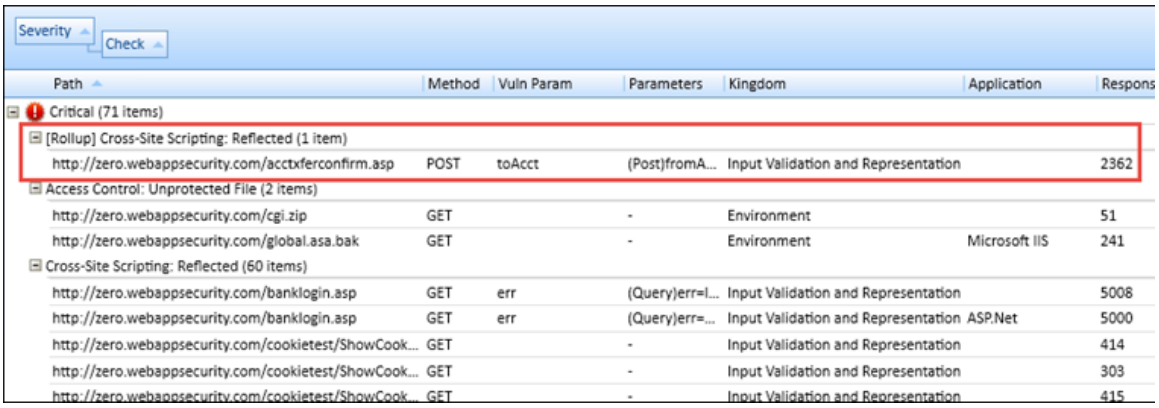
脆弱性をロールアップするには:

1. サマリペインの **検出事項(Findings)**]タブで、ロールアップする脆弱性を複数選択します。
2. 右クリックして、ショートカットメニューから **脆弱性のロールアップ(Rollup Vulnerabilities)**]を選択します。

   次の警告が表示されます。

   これらの脆弱性をロールアップすることは、それらの根本原因が同じであり、その根本原因を修復すればロールアップされたすべての脆弱性が修復されることを意味しています。以降のスキャンでは、ロールアップされた脆弱性が検出された場合、自動的に無視されます。これらの脆弱性の中に根本原因の異なるものがあっても、同様に無視されてしまいます。続行しますか? (Rolling up these vulnerabilities indicates that they share the same root cause, and that fixing the root cause will fix all rolled up vulnerabilities. Future scans will automatically ignore rolled up vulnerabilities if found. If any of these vulnerabilities do not share the same root cause, they will still be ignored. Do you wish to continue?)
3. 次のいずれかを実行します。
   - **OK**]をクリックして、脆弱性をロールアップします。
   - **キャンセル(Cancel)**]をクリックして、脆弱性をそのままにします。

   OK]をクリックすると、選択した脆弱性が1つのインスタンスにロールアップされ、次に示すように、チェック名の前に「[Rollup]」というタグが付きます。さらに、同じ脆弱性の影響を受ける、ロールアップされたURLの詳細を含むメモが、 **セッション情報(Session Info)**]パネルの添付ファイルに追加されます。詳細については、「"選択したセッションのメモの表示" ページ304」を参照してください。



ロールアップの取り消し

ロールアップ機能は、元に戻すことが可能です。ロールアップを取り消すには:

1. サマリペインの **[検出事項(Findings)]** タブで、ロールアップされた脆弱性を右クリックします。
2. **[脆弱性のロールアップを取り消す(Undo Rollup Vulnerabilities)]** を選択します。
   ロールアップが元に戻され、脆弱性が **[検出事項(Findings)]** タブに表示されます。さらに、ロールアップされた脆弱性の詳細を含むメモが **[セッション情報(Session info)]** パネルの添付ファイルから削除されます。

> **注記:** Fortify Software Security Centerに発行されたスキャンのロールアップを取り消す場合、 **[セッション情報(Session Info)]** パネルの添付ファイルに追加されたロールアップの詳細を含むメモはOpenText DASTから一時的に削除されますが、Fortify Software Security Centerとの同期後に再び表示されます。

参照情報

" **[検出事項(Findings)]** タブ" ページ104

誤検出としてマーク

セッションに脆弱性が含まれているとOpenText DASTが誤って判断したと思われる場合は、 **[誤検出としてマーク(Mark as False Positive)]** ダイアログを使用して、セッションからその脆弱性を削除できます。

誤検出としてマークするには:

1. 1つ以上のURLに関連付けられているチェックボックスをオンにします。
2. (オプション) **[説明]** ボックスにコメントまたは説明を入力します。
3. **[OK]** をクリックします。

> **ヒント:** 誤検出としてマークされたすべてのセッションの一覧を表示するには、 **[スキャン情報(Scan Info)]** パネルから **[抑制された検出事項(Suppressed Findings)]** を選択します。

脆弱性としてマーク

[脆弱性としてマーク(Mark As Vulnerability)] ダイアログを使用して、脆弱性を元のセッションに復元します。

1. 1つ以上のURLに関連付けられているチェックボックスをオンにします。
2. (オプション)コメントを入力します。
3. **[OK]** をクリックします。

フォローアップのためのセッションへのフラグ設定

フォローアップのためにセッションにフラグを付けるには:

1. 次のいずれかを実行してセッションを選択します。
   - サマリペインの [検出事項(Findings)] タブで、脆弱なURLを右クリックします。
   - ナビゲーションペインで、セッションまたはURLを右クリックします。
2. ショートカットメニューで、 [添付ファイル(Attachments)] > [フォローアップのためのセッションへのフラグ設定(Flag Session for Follow Up)] をクリックします。

   注記: フォローアップのためにセッションにフラグを設定するもう1つの方法として、脆弱性またはセッションを選択し、 [セッション情報(Session Info)] パネルで [添付ファイル(Attachments)] をクリックしてから、(情報表示エリアの) [追加(Add)] メニューをクリックする方法があります。
3. 選択したセッションに関連するメモを入力します。
4. [OK] をクリックします。

選択したセッションのフラグの表示

[セッション情報(Session Info)] パネルの [添付ファイル(Attachments)] をクリックすると、選択したセッションのメモ、フラグ、およびスクリーンショットを表示できます。

すべてのセッションのフラグの表示

[スキャン情報(Scan Info)] パネルの [添付ファイル(Attachments)] をクリックすると、すべてのセッションのメモ、フラグ、およびスクリーンショットを表示できます。

スキャンメモの使用

スキャンメモを追加するには:

1. [スキャン情報(Scan Info)] パネルで [添付ファイル(Attachments)] をクリックします。
2. [追加(Add)] をクリックして [スキャンメモ(Scan Note)] を選択します。
3. [スキャンメモの追加(Add Scan Note)] ダイアログボックスで、スキャンに関連するメモを入力します。
4. [OK] をクリックします。

スキャンメモ(または添付ファイル)を削除するには:

1. 添付ファイルを選択します。
2. [削除(Delete)] をクリックします。

参照情報

"脆弱性スクリーンショットの追加と表示" ページ295

"脆弱性のメモ" 次のページ

"フォローアップのためのセッションへのフラグ設定" 前のページ

セッションメモの操作

セッションのメモを追加するには:

1. 次のいずれかを実行してセッションを選択します。
   - サマリペインの [検出事項(Findings)]タブで、脆弱なURLを右クリックします。
   - ナビゲーションペインで、セッションまたはURLを右クリックします。
2. ショートカットメニューで、 **[添付ファイル(Attachments)] > [セッションのメモの追加(Add Session Note)]**をクリックします。

   注記: セッションのメモを追加するもう1つの方法として、脆弱性またはセッションを選択し、 [セッション情報(Session Info)]パネルで **[添付ファイル(Attachments)]**をクリックしてから、(情報表示エリアの) **[追加(Add)]**メニューをクリックする方法があります。
3. 選択したセッションに関連するメモを入力します。
4. **[OK]**をクリックします。

選択したセッションのメモの表示

[セッション情報(Session Info)]パネルの **[添付ファイル(Attachments)]**をクリックすると、選択したセッションのメモ、フラグ、およびスクリーンショットを表示できます。

すべてのセッションのメモの表示

[スキャン情報(Scan Info)]パネルの **[添付ファイル(Attachments)]**をクリックすると、すべてのセッションのメモ、フラグ、およびスクリーンショットを表示できます。

参照情報

" [検出事項(Findings)]タブ" ページ104

"情報ペイン" ページ72

"ナビゲーションペイン" ページ61

脆弱性のメモ

脆弱性のメモを追加するには:

1. 次のいずれかを実行して脆弱性を選択します。
   - サマリペインの [検出事項(Findings)]タブで、脆弱なURLを右クリックします。詳細については、"検出事項(Findings)]タブ" ページ104を参照してください。
   - ナビゲーションペインで、脆弱なセッションまたはURLを右クリックします。詳細については、"ナビゲーションペイン" ページ61を参照してください。
2. ショートカットメニューで、 [添付ファイル(Attachments)] > [脆弱性のメモの追加(Add Vulnerability Note)]をクリックします。

   注記: もう1つの方法として、脆弱性を選択し、 [セッション情報(Session Info)]パネルで [添付ファイル(Attachments)]をクリックしてから、(情報表示エリアの) [追加(Add)]メニューをクリックする方法があります。詳細については、"情報ペイン" ページ72を参照してください。
3. 複数の脆弱性があるセッションを選択した場合は、1つ以上の脆弱性の横にあるチェックボックスをオンにします。
4. 選択した脆弱性に関連するメモを入力します。
5. [OK]をクリックします。

選択したセッションのメモの表示

[セッション情報(Session Info)]パネルの [添付ファイル(Attachments)]をクリックすると、選択したセッションのメモ、フラグ、およびスクリーンショットを表示できます。選択したセッションにロールアップされた脆弱性が含まれている場合、 [説明(Description)]エリアのメモに、ロールアップされた、同一の脆弱性による影響を受けるURLの詳細が表示されます。詳細については、"脆弱性のロールアップ" ページ299を参照してください。

すべてのセッションのメモの表示

[スキャン情報(Scan Info)]パネルの [添付ファイル(Attachments)]をクリックすると、すべてのセッションのメモ、フラグ、およびスクリーンショットを表示できます。

削除されたセッションの回復

セッションを削除すると、OpenText DASTはそのセッションをナビゲーションペイン([サイト(Site)]ビューと [シーケンス(Sequence)]ビューの両方)、およびサマリペインの [検出事項(Findings)]タブから削除します。また、今後生成されるレポートからもそのセッションが除外されます。

削除されたセッションの数は、ダッシュボード([スキャン(Scan)]カテゴリの下)に表示されます。削除されたセッションを回復するには:

1. [**削除された項目(Deleted Items)**]ヘッダの横に表示される、強調表示された数字をクリックします。

   [削除された項目の回復(Recover Deleted Items)]ウィンドウには、削除された項目のリストが表示されます。
2. 回復する各セッションの横のチェックボックスをオンにします。
3. セッションの詳細情報を表示するには、 [**選択時に詳細を表示する(Show details when selected)**]を選択します。
4. [**回復(Recover)**]をクリックして、選択を確認するプロンプトが表示されたら [**はい**]をクリックします。

回復されたセッションは、ナビゲーションペイン([サイト(Site)]ビューと [シーケンス(Sequence)]ビューの両方)、およびサマリペインの [**検出事項(Findings)**]タブに親セッションとともに再び表示されます。

参照情報

" [セッション情報(Session Info)]パネル" ページ86

OpenText ALMへの脆弱性の送信

1つ以上の脆弱性を不具合に変更して、それらをOpenText Application Lifecycle Management (ALM)データベースに追加できます。

脆弱性を不具合トラッキングシステムに送信するには:

1. ナビゲーションペインまたはサマリペインで脆弱性を右クリックします。詳細については、「" ナビゲーションペイン" ページ61」および「"サマリペイン" ページ104」を参照してください。
2. [**送信先(Send to)**]を選択して、 [**OpenText ALM**]を選択します。
3. [送信先(Sendo to)]ダイアログボックスで、 [**プロファイル(Profile)**]リストからプロファイルを選択します。

   プロファイルを作成または編集する必要がある場合は、 [**管理(Manage)**]をクリックしてOpenText DASTの [アプリケーション設定(Application Settings)]にアクセスします。詳細については、「"アプリケーション設定: OpenText ALM" ページ507」を参照してください。

   注記: 選択したプロファイルがOpenText DAST脆弱性を(重大度レベルに基づいて)「発行しない(Do not publish)」にマップしている場合、脆弱性はエクスポートされません。
4. 以前に報告されている場合でも不具合を強制的に作成するには、 [**重複する不具合の割り当てを許可する(Allow duplicate defect assignment)**]を選択します。

   OpenText DASTは、同じスキャン内でのみ重複を認識します。サイトをスキャンして特定の脆弱性をALMに送信する際に、そのスキャン中に再び同じ脆弱性が検出された場合、OpenText DASTが同じ脆弱性を送信しないようにすることができます。ただし、そのサイトに再びスキャンを行い、OpenText DASTが同じ脆弱性を再度検出した場合、

OpenText DASTに以前のスキャンにおいて脆弱性がALMに送信されたことをプログラムによって認識させることはできません。

5. 不具合の送信後にこのダイアログボックスを閉じるには、 **完了したら閉じる(Close when finished)**]を選択します。
6. 複数の脆弱性を選択した場合、ID番号の横のチェックボックスを外して脆弱性を除外できます。
7. **送信(Send)**]をクリックします。

送信される追加情報

次の例が示しているように、OpenText DASTは、OpenText ALMに欠陥が送信されたことを示すメモをセッション情報に追加します。

Defect #30 was created in OpenText ALM. (Micro Focus ALMにおいて不具合#30が作成されました)
Check ID: 182(チェックID: 182)
CheckName: Dan-o Log Information Disclosure(チェック名: Dan-oログ情報公開)
Profile: QA-user1(プロファイル: QA-user1)
Server URL: http://myvm2023/qcbin(サーバURL: http://myvm2023/qcbin)
Project: test3(プロジェクト: test3)
Priority: 3-High(優先度: 3-高)
Severity: 1-Low (重大度: 1-低)

注記:「OpenText ALMの認証でエラーが発生しました(Error authenticating with OpenText ALM)」というエラーメッセージが表示される場合は、"データ実行防止の無効化" 下を参照してください。

データ実行防止の無効化

OpenText Application Lifecycle Management (ALM)と統合しようとすると、次のエラーメッセージが表示されることがあります。

```
Error authenticating with OpenText ALM.
```

その場合は、Microsoftのデータ実行防止(DEP)を無効にする必要があります。DEP設定の変更方法については、Windowsのマニュアルを参照してください。

レポートの生成

Report Generatorをさまざまな方法で起動できます。

- 開始ページ(Start Page)]のクライアントエリアで、左ペインにある **レポートの生成(Generate a Report)**]をクリックする。
- OpenText DASTのツールバーで、 **レポート(Reports)**]をクリックします。

- [**レポート(Reports)**]メニューをクリックし、[**レポートの生成(Generate Report)**]を選択する。
- [**スキャンの管理(Manage Scans)**]フォームでスキャン名を右クリックし、[**レポートの生成(Generate Report)**]を選択する。
- スキャンを開いた状態で、[**サイト(Site)**]ビューでセッションを右クリックし、[**セッションレポートの生成(Generate Session Report)**]を選択する。詳細については、「"サイトビュー" ページ63」を参照してください。
- スキャンをスケジューリングするときに。

レポートを生成するには:

1. 上記のいずれかのオプションを使用してReport Generatorを起動します。
2. [**スキャンの選択(Select a Scan)**]ウィンドウからスキャンを1つ以上選択します。
3. (オプション)[**詳細(Advanced)**](ウィンドウの下部にある)をクリックして、レポートの保存のオプションと、ヘッダとフッタのテンプレートを選択するためのオプションを選択します。
4. [**次へ(Next)**]をクリックします。
5. (オプション)[**お気に入り(Favorites)**]リストからレポートを選択します。

   ヒント:「お気に入り」は、1つ以上のレポートとその関連パラメータの単なる名前付きコレクションです。レポートおよびパラメータを選択した後でお気に入りを作成するには、[**お気に入り(Favorites)**]リストをクリックして、[**お気に入りに追加(Add to favorites)**]を選択します。
6. 1つ以上のレポートを選択します。レポートの説明については、「"標準レポート" ページ310」を参照してください。
7. 要求できるパラメータの情報を入力します。感嘆符は、必須パラメータを示します。
8. (1つのタブ上にすべてのレポートを結合するのではなく)個別のタブに各レポートを表示するには、[**レポートを別のタブで開く(Open Reports in Separate Tabs)**]を選択します。
9. [**完了(Finish)**]をクリックします。

レポートの保存

OpenText DASTによってレポートが生成および表示されたら、レポートビューアツールバーの[**名前を付けて保存(Save As)**]をクリックしてレポートを保存できます。

レポートは次の形式で保存できます。

- Adobe Portable Data Format (.pdf)
- ハイパーテキストマークアップ言語(.html)
- ネイティブOpenText DAST内部形式(.raw)
- リッチテキスト形式(.rtf)
- テキスト(.txt)
- Microsoft Excel (.xls)

参照情報

"標準レポート" ページ310

"詳細レポートのオプション" 下

"コンプライアンステンプレート" ページ312

"アプリケーション設定: レポート" ページ501

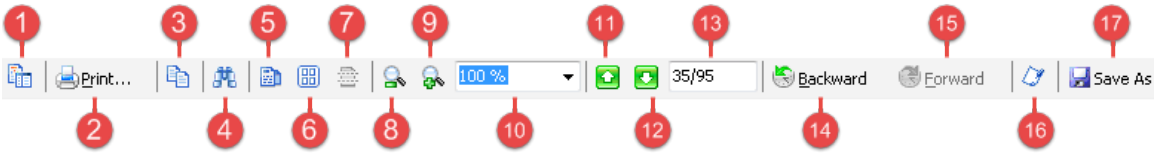
詳細レポートのオプション

次の表に、詳細レポートのオプションの説明を示します。

オプション	説明
レポートをディスクに保存する(Save reports to disk)	このオプションは、レポートをファイルに出力する場合に選択します。
ファイル名を自動的に生成する(Automatically generate file name)	レポートをディスクに保存するときにこのオプションを選択すると、レポートファイルに*<reportname> <date/time>.<extension>*という形式の名前が付けられます。 たとえば、pdf形式でコンプライアンスレポートを作成し、そのレポートが4月5日の6:30に生成される場合、ファイル名は「Compliance Report 04_05_2009 06_30.pdf」になります。これは、反復スキャンの場合に便利です。 • 複数のレポートタイプを選択した場合は、*<reportname>*が「Combined Reports」になります。 • レポートは、生成されるレポート用にアプリケーション設定で指定されたディレクトリに書き込まれます。 **ファイル名を自動的に生成する(Automatically generate filename)**]を選択しない場合は、デフォルト名「auto-gen-filename」をファイル名に置き換えます。
エクスポート形式(Export Format)	レポート形式を選択します。
ヘッダ/フッタレポート(Header/Footer Report)	レポートのヘッダとフッタの形式を選択してから、コンポーネントを入力または選択します。

レポートビューア

ツールバーを使用して、レポート内の移動、レポートの印刷と保存、、メモの追加を行います。



項目	説明
1	目次の表示/非表示
2	レポートの印刷
3	コピー
4	検索
5	単一ページビュー
6	複数ページビュー
7	連続スクロール
8	ズームアウト
9	ズームイン
10	倍率
11	前のページ
12	次のページ
13	現在のページ番号/ページの合計数
14	1ページ戻る
15	1ページ進む
16	注釈("メモの追加" 次のページを参照)
17	レポートの保存

注記: [戻る(Backward)]ボタンと [進む(Forward)]ボタンは、ブラウザの [戻る]ボタンと [進む]ボタンと同じように機能します。履歴リスト内の1ステップ分進むか、戻ります。

メモの追加

メモを追加するには:

1. [注釈(Annotation)]アイコンをクリックします。
2. 形式を選択します。
3. レポートにドラッグします。
4. メモを右クリックし、 **[プロパティ(Properties)]**を選択します。
5. [テキスト(Text)]プロパティを選択し、メモの内容を入力します。

標準レポート

次の表に、使用可能な標準レポートの説明を示します。

レポート	説明
集約(Aggregate)	このレポートは、複数スキャン向けに設計されています。報告する重大度のカテゴリ、レポートセクション(サーバのコンテンツと脆弱性の詳細)、およびセッション情報(応答および要求)を選択できます。スタックトレースが利用可能な場合には、スタックトレースも報告できます。
アラートビュー(Alert View)	このレポートでは、すべての脆弱性が重大度別に一覧にされ、脆弱性を発生させた各HTTP要求へのハイパーリンクが表示されます。また、各脆弱性を詳細に説明した付録も含まれています。
攻撃ステータス(Attack Status)	このレポートには、スキャン中に使用された各攻撃エージェント(チェック)について、脆弱性ID番号、チェック名、脆弱性の重大度、チェックがスキャンで有効になっていたかどうか、チェックが合格したかどうか(つまり、脆弱性が検出されたかどうか)、および(チェックが不合格の場合には)脆弱性が検出されたURLの数が一覧にされます。特定の重大度の脆弱性と、合格/不合格ステータスを報告することを選択できます。
コンプライアンス(Compliance)	このレポートには、政府が定めた特定の規制や企業が定義したガイドラインにアプリケーションがどの程度準拠しているかを評価した定性分析が含まれています。
Web探索済みURL	このレポートには、Web探索中に検出されたURLごとに、送信され

レポート	説明
(Crawled URL)	たすべてのクッキーと生のHTTP要求および応答が一覧にされます。
開発者リファレンス(Developer Reference)	Webサイトで検出された各フォーム、JavaScript、電子メール、コメント、非表示のコントロール、およびクッキーの総数と詳細な説明が示されます。これらの参照タイプから1つ以上を選択できます。
重複(Duplicates)	このレポートには、OpenText DAST Agentにより検出され、同じソースに行き着く脆弱性に関する情報が記載されています。最初に、相関関係のない脆弱性の総数と固有の脆弱性の数を比較する棒グラフが表示されます。
エグゼクティブサマリ(Executive Summary)	このレポートには、基本的な統計情報と、アプリケーションの脆弱性レベルを反映したグラフが表示されます。
誤検出	このレポートには、OpenText DASTによって最初は脆弱性として分類されたものの、後でユーザが誤検出と判断したURLに関する情報が表示されます。
QAの概要(QA Summary)	このレポートには、破損したリンク、サーバエラー、外部リンク、およびタイムアウトを含むすべてのページのURLが一覧にされます。これらのカテゴリから1つ以上を選択できます。
スキャンの差異(Scan Difference)	このレポートでは、2つのスキャンが比較され、脆弱性、ページ、ファイルが見つからないという応答などが一方のWebサイトでだけ見られるといった相違が報告されます。
スキャンログ(Scan Log)	スキャン中にOpenText DASTによって実行されたアクティビティを順に示すリストです(情報はサマリペインの **[スキャンログ(Scan Log)]** タブに表示されます)。
傾向(Trend)	このレポートでは、脆弱性の解決に向けた開発チームの進捗状況を監視できます。たとえば、最初のスキャンの結果が保存され、チームが問題の修復を開始します。その後、毎週1回サイトを再スキャンして結果をアーカイブします。進行状況を定量化するには、現在までに実行したすべてのスキャンの結果を分析する傾向レポートを実行します。このレポートには、各スキャンの実行日付によって定義されたタイムラインに、脆弱性の数を重大度別に示すグラフが含まれています。重要: 信頼できる結果を得るためには、同じポリシーを使用して各スキャンを実行してください。
脆弱性(レガシ)	各脆弱性と、改善に関する推奨事項を含む詳細なレポートです。

レポート	説明
(Vulnerability (Legacy))	
脆弱性 (Vulnerability)	このレポートにも、検出された脆弱性に関する詳細情報が重大度別に表示されます。

レポートの管理

レポート定義ファイルの名前変更、追加、削除、またはインポートを行うには、 [レポートの管理(Manage Reports)]を使用します。

標準レポートに対する名前変更、削除、またはエクスポートは実行できません。

コンプライアンステンプレート

ここでは、使用可能なコンプライアンステンプレートについて説明します。他のテンプレートは、使用可能になった段階でSmartUpdateを介してダウンロードできます。

注記: このリストは、お使いの製品に表示されるテンプレートと一致しない場合があります。このドキュメントの作成以降に、SmartUpdateによりテンプレートが追加されている可能性があります。

Template	説明
21CFR11	米国連邦規制基準第21編第11部(通常は「21 CFR 11」と略される)に、電子記録および電子署名に関する要件が記載されています。医療会社のコンプライアンスを支援するために、米国食品医薬品局(FDA)は、FDA規制によって保管および維持が義務付けられている記録の電子記録および電子署名の適切な使用に関するガイダンスを公開しています。このガイダンスには、「機関が、電子記録、電子署名、および電子記録に対して行われた手書きの署名が信用でき、信頼性が高く、紙の記録や紙に対して行われた手書きの署名と同等であると見なす基準」が記載されています。 法律とFDAガイダンスにより、機密性の高い医療情報を扱う医療会社や医療機関は、電子記録と電子署名が信用でき、信頼性が高く、紙の記録や手書きの署名の同等の代用品であることを保証することが義務付けられています。機器、オペレータ、およびコンピュータ間の相互作用が当たり前になる中、情報の通信と保存を行う安全な手段を確立

Template	説明
	することが重要です。
バーゼルII	バーゼルIIは、世界中の中央銀行による検討事項の一環であり、スイスのバーゼルにあるバーゼル銀行監督委員会(BCBS)の下で、銀行と金融当局が国境を越えてリスク管理に取り組む方法の統一を図ることを目的としています。BCBSは、銀行業務のコンプライアンスに関する国際的なルール作成部門です。2004年、中央銀行の総裁と10か国蔵相会議(G10)の各国銀行監督機関の長が、バーゼルIIとして広く知られている新しい自己資本の枠組みである「自己資本の計測と基準に関する国際的統一化:改訂された枠組み」の発行を承認しました。 バーゼルIIは、主に、銀行に対して、資本準備金を増やすか、信用リスクや運用リスクを組織的かつ効果的に管理できることを実証するように求めています。この枠組みでは、運用リスクを「不適切なまたは機能不全の内部プロセス、人、およびシステムによって、または、外部的事象によって発生する損失のリスク」と定義し、不適切なシステムセキュリティを介したハッキングや情報漏洩を損失事象として強調しています。世界中の銀行はグローバルな金融市場での運用リスクを管理する専門家ですが、オンライン銀行システムの運用と顧客データの安全性の確保に伴うリスクを理解して管理することには精通していません。 効果的な情報セキュリティとシステムセキュリティを実践している銀行は、監督機関に対して、運用リスクの低減を通して資本準備金を削減する資格があることを実証できます。バーゼルIIの枠組みは、情報を保護するためのポリシーとプロセスの効果的なシステムが設けられていることと、これらのポリシーとプロセスへのコンプライアンスが保証されていることを実証するよう銀行に対して繰り返し求めていますが、銀行がセキュリティポリシーおよびプロセスを実装する方法については規範を示していません。国際標準のISO/ICE 17799 Code of Practice for Information Security Managementは、情報セキュリティの実装と維持に関するガイドラインを提供しており、バーゼルIIの文脈で情報セキュリティに関連する運用リスクを管理および報告するためのモデルとして広く使用されています。
CA OPPA	カリフォルニア州オンラインプライバシー保護法(OPPA)は、2003年に制定され、カリフォルニア州の商用Webサイトのすべての企業と所有者に、個人情報の収集、使用、および共有に関するポリシーを明確に定めたプライバシーポリシーを目立つ場所に掲示し、遵守するように義務付けています。このポリシーは、サイト訪問者に関して収集された個人識別情報のカテゴリと、運営者が情報の共有先にできる第三者のカテゴリを識別します。

Template	説明
	カリフォルニア州の住人の非公開個人情報を収集するWebサイトを運営する企業、組織、または個人はこの法律の条項に制約されるため、カリフォルニア州OPPAは一般的な州の規制よりはるかに大きな影響を全国的に及ぼします。
CASB 1386	カリフォルニア州上院法案第1386号は、米国内の州の中で最も具体的で制限的なプライバシー侵害報告要件を定めています。この法律は、正当な業務目的で非公開個人情報を保有する企業、組織、および個人に対して、個人情報が漏洩した場合に直ちに消費者に通知することを強制するために制定されました。また、この法律は、情報の侵害を通して被った損害について、民事裁判所で企業を訴える権利を消費者に与えています。カリフォルニア州の住人の非公開個人情報を保持する企業、組織、または個人は、この法律の条項に制約されます。
COPPA	児童オンラインプライバシー保護法(COPPA)は、13歳未満の子供に関する個人情報をオンライン収集から保護するために2000年に制定されました。COPPAの目的は、子供がしばしば簡単にWebにアクセスできることを認識した上で、子供のプライバシーと安全をオンラインで保護することです。この法律は、Webサイトの運営者がサイト上にプライバシーポリシーを掲載し、特定の状況下で子供の個人情報を収集する場合は親の同意を求めるという要件の概要を示すように義務付けています。 この法律は、明らかに子供向けのWebサイトだけでなく、Webサイトの運営者が子供から個人情報を収集していることを自覚している、一般的な視聴者コンテンツを含むWebサイトにも適用されます。運営者は、自社のWebサイトまたはオンラインサービスのホームページと、子供から個人情報を収集する各エリアに、その情報取り扱いの通知へのリンクを掲載する必要があります。子供のエリアが別にある一般的な視聴者サイトの運営者は、子供のエリアのホームページにその通知へのリンクを掲載する必要があります。
CWE Top 25 *<version>*	CWE (Common Weakness Enumeration) Top 25 Most Dangerous Software Errors (CWE Top 25)は、MITREが作成した弱点のリストで、ソフトウェアの重大な脆弱性につながる可能性のある最も広がっている重大な弱点を示しています。MITREは、その方法論の概要を次のように説明しています。 「このリストを作成するために、CWEチームは、公開済みのCVE (Common Vulnerabilities and Exposures)データ、NIST (National Institute of Standards and Technology) のNVD (National

Template	説明
	Vulnerability Database)内にある関連CWEマッピング、および各CVEに関連付けられたCVSS (Common Vulnerability Scoring System)スコアを利用するデータ駆動型のアプローチを使用しました。その上で、採点式を適用して各弱点が示すまん延度と危険度を決定しました。反復可能でスクリプト化されたプロセスとしてこのデータ駆動型のアプローチを使用し、最小限の労力で定期的にCWE Top 25リストを生成することができます。」
DCID	この指令は、分類されたインテリジェンス情報を情報システムに保存、処理、および通信するためのセキュリティポリシーと手順を定めています。この指令の目的では、インテリジェンス情報とは、中央情報局長官の権限の下にある、隔離された機密情報とインテリジェンスへの特別なアクセスプログラムを指します。
DoD Application Security Checklist Version 2	DISA FSO (Field Security Operations)は、アプリケーションSRRを実施して、アプリケーションがミッションを脅かす可能性のある攻撃に対して合理的に安全であることの最低レベルの保証を、DISA、統合部隊、およびその他の国防総省(DoD)組織に提供します。ほとんどのミッションクリティカルなアプリケーションでは、その複雑さのせいで、アプリケーションSRRに割り当てられた時間枠内で考えられるすべてのセキュリティ機能と脆弱性の包括的なセキュリティレビューを行うことが不可能です。それにもかかわらず、最も一般的なアプリケーションの脆弱性に対処し、運用上許容できないリスクをもたらす情報保証(IA)問題を特定する上で、SRRは役立ちます。 IA制御が開発ライフサイクルのすべてのフェーズで統合されることが理想的です。アプリケーションレビュープロセスを開発ライフサイクルに統合すれば、アプリケーションのセキュリティ、品質、および回復力を保証できます。通常、アプリケーションSRRはアプリケーションリリースの近くまたは後に実施されるため、アプリケーションSRRの検出事項の多くは、アプリケーションインフラストラクチャに対するパッチまたは変更を通して修復する必要があります。脆弱性によっては修正に大幅なアプリケーション変更を要することがあります。アプリケーションレビュープロセスを開発ライフサイクルに統合するのが早いほど、改善プロセスの中断が少なくなります。
DoD Application Security and Development STIG *<version>*	このコンプライアンステンプレートでは、Application Security and Development Security Technical Implementation Guide (STIG)のバージョン3、リリース2の該当するWebアプリケーションコンポーネントのすべてが報告されます。STIGは、アプリケーション開発ライフサイクル全体を通して使用するためのセキュリティガイダンスを提供します。国防情報システム局(DISA)は、アプリケーション開発プロセスのできるだけ早い

Template	説明
	段階でこれらのガイドラインを使用するようにサイトに奨励しています。
DoD Control Correlation Identifier (CCI)	国防情報システム局(DISA)のFSO (Field Security Operations)がCCI仕様を作成し、現在は、CCI仕様とCCIリストの保守を担当しています。 CCI (Control Correlation Identifier)は、情報保証(IA)制御またはIAベストプラクティスを構成する単一のアクション可能な声明のそれぞれに標準の識別子と記述を提供します。 CCIは大まかなポリシー表現と詳細な技術実装の間のギャップを埋めます。CCIでは、大まかなポリシーフレームワークで表現されたセキュリティ要件を分解し、その特定のセキュリティ制御の目的の遵守を判断するために評価する必要がある詳細なセキュリティ設定と明示的に関連付けることができます。セキュリティ要件をその原点(規制やIAフレームワークなど)から詳細な実装までを追跡できるこの能力を使用すれば、組織は、複数のIAコンプライアンスフレームワークへのコンプライアンスを簡単に実証できます。また、CCIは、異種の技術をまたいで関連するコンプライアンス評価結果を客観的にロールアップして比較する手段も提供します。 このレポートは、OpenText Fortify 7PK分類をDISA CCIにマップします。
EUデータ保護	欧州委員会のデータ保護に関する指令は、個人データの処理に関するプライバシーに対する欧州連合市民の基本的権利を保護します。この指令の主な焦点は、受け入れ可能な個人データの使用と保護に置かれています。他のすべての欧州連合プライバシー立法と同様に、この指令でも、個人データを収集、保存、変更、または発信するにはデータの使用に関する市民の明確な同意と完全な開示を要求しています。また、欧州の組織から個人データの安全とプライバシーを適切に保護していない欧州連合以外の国や組織に個人データを転送することを禁じています。米国は、この指令に準拠する必要がある米国の組織向けのセーフハーバーフレームワークを策定しました。
プライバシーおよび電子通信に関するEU指令	プライバシーおよび電子通信に関する欧州連合指令は、欧州連合の電子通信部門に適用される法律の広範な「電気通信一括法案」の一部です。この指令は、すべての加盟国が、公衆通信ネットワーク上で行われた通信と、このような通信に本来備わっている個人データと非公開データの機密性を保証しなければならないという欧州連合の基本原則を補強するものです。この指令は、物理通信ネットワークとその上で伝送される個人データに適用されます。

Template	説明
FISMA	米国連邦政府は、米国の経済と国家安全保障の利益に対する情報セキュリティの重要性を認識して、2002年の電子政府法を通過させました。この法律の第III編は、連邦情報セキュリティマネジメント法(FISMA)と題され、すべての米国連邦政府機関が機密性、整合性、および可用性という3つのセキュリティ目標を掲げた適切な情報セキュリティを情報システムの一部として実装する際に使用する標準とガイドラインの策定を米国標準技術局に委ねています。FISMAは、各連邦機関の長に、情報と情報システムの不正アクセス、使用、開示、中断、変更、または破壊に伴うリスクと損害の大きさに見合った情報セキュリティ保護を提供するように要求しています。保護は、機関だけでなく、機関の代わりに働く請負業者や他の組織にも適用される必要があります。
一般データ保護規則(GDPR)	EU一般データ保護規則(GDPR)は、データ保護指令95/46/ECに代わるもので、欧州全体のデータプライバシー法を調和させ、すべてのEU市民のデータプライバシーを保護および強化し、地域全体の組織がデータプライバシーにアプローチする方法を見直すように設計されています。2018年5月25日に施行されたGDPRは、個人データの処理方法に関するフレームワークを組織に提供しています。 GDPR規制によると、個人データは「特定されたまたは特定可能な自然人(「データ主体」)に関連する情報を意味します。特定可能な自然人とは、特に、名前、識別番号、位置データ、オンライン識別子などの識別子を参照したり、その自然人の物理的、生理的、遺伝的、精神的、経済的、文化的、または社会的アイデンティティに固有の1つ以上の要素を参照したりすることによって直接的または間接的に識別できる人のことです。」 アプリケーションセキュリティに関連し、製品やサービスの設計や開発中に個人データを保護することを企業に要求するGDPRの条項を以下に示します。 • 第25条、設計およびデフォルトでのデータ保護-「デフォルトで、処理の特定の目的ごとに必要な個人データのみが処理されることを保証するための適切な技術的および組織的手段」の実施が必要です。 • 第32条、処理のセキュリティ-企業は「個人データの偶発的または不当な破壊、紛失、改変、不正開示、またはアクセスから」システムおよびアプリケーションを保護する必要があります。 このレポートは、アプリケーションセキュリティに関連して個人データの特定と保護を支援するためのフレームワークとして組織が使用する場合があります。

Template	説明
GLBA	グラムリーチブライリー法(GLBA)では、金融機関が消費者の個人の金融情報を保護するように義務付けています。金融業界のWebアプリケーションセキュリティに影響を与える主な規定は、GLBAセーフガードルールです。
HIPAA	Health Insurance Portability and Accountability Act (HIPAA: 医療保険の携行性と責任に関する法律)は、情報管理に関連するさまざまな脅威や脆弱性からの個人の健康情報のプライバシーとセキュリティを義務付けています。
ISO17799	これは、情報セキュリティ管理に関して最も広く受け入れられている国際標準です。このコンプライアンステンプレートは、組織とそのセキュリティポリシーのニーズを満たすコンプライアンスポリシーの策定のベースラインとして使用してください。
ISO27001 *<version>*	ISO/IEC 27001は、国際標準化機構および国際電気標準会議によって2005年10月に発行された情報セキュリティ管理システム標準です。基本的な目的は、継続的な改善アプローチを使用して、効果的な情報管理システムの確立と維持を支援することです。ISO 27001は、セキュリティ管理システム自体に関する要件を定めています。これは、ISO 17799とは対照的に、認定が提供される標準です。加えて、ISO 27001は、ISO 9001やISO 14001などの他の管理標準と「統一」されています。
JPIPA	日本は、2003年に、正当な目的のためにITと個人情報の有益性を保持しながら、個人の権利と個人情報を保護することを目的として、個人情報保護法(JPIPA)を施行しました。この法律は、日本の市民の個人情報を取り扱う企業の責任を規定し、準拠しない組織に対する罰金と罰則の可能性の概要を示しています。この法律は、企業に、個人情報の収集と使用の目的を伝達するように義務付けています。また、企業は、個人情報を開示、不正使用、または破壊から保護するための合理的な手順を講じる必要もあります。
NERC	北米電力信頼度協議会(NERC)は、米国の電力システムが信頼でき、適切で、安全であることを保証する使命を持って1968年に設立されました。1998年にBill Clinton大統領が米国の国家経済と公共の福祉に不可欠なインフラストラクチャ産業を定義するために大統領決定指令63を発行した後、米国エネルギー省は8つの重要なインフラストラクチャ産業の1つとして指名された電力業界の調整機関としてNERCを指定しました。
NIST 800-53	米国連邦政府は、米国の経済と国家の利益に対する情報セキュリ

Template	説明
<version>	ティの重要性を認識して、2002年の電子政府法を通過させました。この法律の第III編は、連邦情報セキュリティマネジメント法(FISMA)と題され、すべての米国連邦政府機関が機密性、整合性、および可用性という3つのセキュリティ目標を掲げた適切な情報セキュリティを情報システムの一部として実装する際に使用する標準とガイドラインの策定を米国標準技術局に委ねています。
OMB	このポリシーは、2004年12月に行政管理予算局が連邦政府機関の公式Webサイトに関して定義した主要なアプリケーションセキュリティ部門を対象とします。これらのWebサイトは、連邦政府が全部または一部の資金を提供し、機関、請負業者、または機関に代わるその他の組織が運営する情報リソースです。政府の情報を開示したり、一般または特定の非連邦ユーザグループにサービスを提供して、機関の機能の適切な遂行をサポートしたりします。
OWASP ASVS	OWASP (Open Web Application Security Project) ASVS (Application Security Verification Standard)は、設計者、開発者、テスト担当者、セキュリティプロフェッショナル、ツールベンダー、および消費者が安全なアプリケーションを定義、構築、テスト、および検証するために使用できるアプリケーションセキュリティ要件またはテストのリストです。 **注記:** OWASP ASVSドキュメントのCWEカテゴリへのマッピングの中には、カテゴリの目的と一致しないものや、限定範囲で一致するものがあります。このコンプライアンステンプレートを使用して生成されたレポート内の、報告されたCWEマッピングを確認してください。
OWASP Top Ten *<year>*	多くの政府機関が、Webアプリケーションのセキュリティの確保におけるベストプラクティスとして、OWASP Top Ten Webアプリケーション脆弱性のテストを推奨しています。
PCIデータセキュリティ*<version>*	クレジットカード業界(PCI)データセキュリティポリシーは、カード所有者データを保存、処理、または送信するすべてのPCIデータセキュリティのメンバー、業者、およびサービスプロバイダが、社内外のアプリケーションを含む、すべての購入したカスタムWebアプリケーションを検証するように義務付けています。
PCI SSF *<version>*	このコンプライアンステンプレートは、Payment Card Industry (PCI) Software Security Framework (SSF)で定義されている、Secure Software Requirements and Assessment Proceduresのアプリケーションセキュリティ部分に当てはまります。WebInspectでは、PCI SSFの制御目標セクション2、3、4、5、6、7、10、A.2、C.1、C.2、C.3、および

Template	説明
	C.4にわたる18件のアプリケーションセキュリティ関連制御目標をテストし、各制御目標が達成されているかどうかを報告して、要件が満たされているかどうかを示します。このレポートは、PCI SSFコンプライアンスと比較した場合の特定のアプリケーションの順守のレベルを測定することを目的としたもので、包括的なコンプライアンスレポート(ROC)として機能することを意図したものではありません。このレポートに含まれる情報は、プロジェクトマネージャ、セキュリティ監査担当者、およびコンプライアンス監査担当者を対象にしています。
PIPEDA	カナダの個人情報保護および電子文書法(PIPEDA)は、民間企業の管理下で個人情報を保護する新しい法律であり、商業活動の過程でのその情報の収集、使用、および開示に関するガイドラインを示しています。この法律は、カナダ規格協会が策定した10のプライバシー原則に基づいて、カナダのプライバシー委員会と連邦裁判所によって監視されています。2004年1月1日以降、カナダの企業はすべて、PIPEDAによって規定されたプライバシー原則を遵守する必要があります。この法律は、従来の紙ベースのビジネスとオンラインビジネスの両方を対象とします。
セーフハーバー	欧州委員会のデータ保護に関する指令は、欧州の組織から個人データの安全とプライバシーを適切に保護していない欧州連合以外の国や組織に個人データを転送することを禁じています。この包括的な欧州の法律の通過により、欧州連合の組織とデータを共有する米国内のすべての企業および組織に規制の遵守が義務付けられ、これはさまざまな大西洋横断企業取引を混乱させかねませんでした。個人データのプライバシーの保護に対して米国と欧州連合の各国が取ったアプローチが異なるために、米国商務省は、欧州委員会と協力して、合理化された「セーフハーバー」フレームワークを策定しました。このフレームワークを通して、米国の組織はデータ保護に関する指令に準拠できます。 セーフハーバーに参加している組織は、個人データが適切に使用、制御、および保護されていることを保証するために設計された7つの原則(通知、選択、転送、アクセス、セキュリティ、データ整合性、および実施)に準拠するように取り組む必要があります。ITにとって特に重要なのは次の点です。 • 通知の原則では、組織は、個人情報を収集する目的をプライバシーポリシーなどを通して個人に通知する必要があります。 • セキュリティの原則には、組織が個人データを保護するための合理的な予防措置を講じることが明記されています。 • 実施の原則では、組織が、包括的なセキュリティテストなどを通し

Template	説明
	て、セキュリティの義務が果たされていることを検証する手順を実施する必要があります。
SANS CWE Top 25 *<version>*	SANS (SysAdmin、Audit、Network、Security) Instituteは、1989年に共同研究および教育組織として設立されました。SANS CWE (Common Weakness Enumeration) Top 25 Most Dangerous Software Errorsは、深刻なソフトウェアの脆弱性につながる可能性のある最も普及している重大なプログラミングエラーのリストです。このようなエラーのせいで攻撃者がソフトウェアを完全に掌握して、データを盗んだり、ソフトウェアの機能を妨げたりすることが頻繁であるため、危険です。このコンプライアンステンプレートでは、このリストのすべての該当するWebアプリケーションコンポーネントが報告されます。 **注記:**「CWE」以外のSANSコンプライアンステンプレートも入手できます。
サーベンスオクスリー	米国証券取引委員会(SEC)の管理下にあるサーベンスオクスリー法は、2002年7月30日に制定されました。この法律は、顧客の機密情報のプライバシーやセキュリティを強化するのではなく、財務記録の保護のための企業行動を規制することに焦点が当てられています。
英国のデータ保護	欧州委員会のデータ保護に関する指令は、個人データの処理に関するプライバシーに対する欧州連合市民の基本的権利を保護します。この指令の主な焦点は、受け入れ可能な個人データの使用と保護に置かれています。英国は、1998年のデータ保護法を通して、指令が定める保護を実施してきました。この法律の概要を以下に示します。 • 個人データは、同意がある場合にのみ、公正かつ合法的に処理する必要があります。 • 個人データは、特定の合法的な目的でのみ取得し、それらの目的と相容れない方法では処理しないようにする必要があります。 • 個人データは、処理される目的に関して適切で、関連があり、過剰ではない必要があります。 • 個人データは、正確で、最新の状態に保つ必要があります。 • いかなる目的のために処理される個人データも、必要以上に長く保持しないようにする必要があります。 • 個人データは、データ主体の権利に従って処理する必要があります。 • 個人データの不正なまたは不当な処理や個人データの偶発的な紛失、偶発的な破壊、または損害に対して、適切な技術的および組

Template	説明
	織的対策を講じる必要があります。 • 個人データは、欧州経済地域外の国または地域に転送しないようにする必要があります。ただし、その国または地域が個人データの処理に関連してデータ主体の権利および自由に対する適切なレベルの保護を保証していない場合に限られます。
WASC *<version>*	このコンプライアンステンプレートは、Web Application Security Consortiumの脅威クラスに基づいて作成されています。WASCの脅威分類は、Webサイトのセキュリティに対する脅威を明確にして整理するための共同の取り組みです。全チェックポリシーと組み合わせて使用することにより、SecureBaseに付属の各脆弱性チェックを含むコンプライアンスレポートを生成できます。

設定の管理

[設定の管理(Manage Settings)]ウィンドウを使用すると、スキャン設定ファイルを作成、編集、削除、インポート、およびエクスポートできます。

注記: また、[デフォルト設定(Default Settings)]ウィンドウから設定をロードして保存し、出荷時のデフォルト設定を復元することもできます。[**編集(Edit)**]をクリックし、[**デフォルトのスキャン設定(Default Scan Settings)**]を選択します。

[設定の管理(Manage Settings)]ウィンドウへのアクセス

[設定の管理(Manage Settings)]ウィンドウにアクセスするには、次の方法を実行します。

- [**編集(Edit)**]メニューから[**設定の管理(Manage Settings)**]を選択します。
  [設定の管理(Manage Settings)]ウィンドウが開きます。

設定ファイルの作成

設定ファイルを作成するには:

1. [**追加(Add)**]をクリックします。
2. [新規設定の作成(Create New Settings)]ウィンドウで設定を変更します。
3. 終了したら、[OK]をクリックします。
4. 標準のファイル選択ダイアログボックスを使用して、ファイルに名前を付けて保存します。

設定ファイルの編集

設定ファイルを編集するには:

1. ファイルを選択します。
2. [**編集(Edit)**]をクリックします。
3. [**新規設定の作成(Create New Settings)**]ウィンドウで設定を変更します。
4. 終了したら、[**OK**]をクリックします。

設定ファイルの削除

設定ファイルを削除するには:

1. ファイルを選択します。
2. [**削除(Delete)**]をクリックします。

設定ファイルのインポート

設定ファイルをインポートするには:

1. [**インポート(Import)**]をクリックします。
2. 標準のファイル選択ダイアログボックスを使用して設定ファイルを選択し、[**開く(Open)**]をクリックします。

設定ファイルのエクスポート

設定ファイルをエクスポートするには:

1. ファイルを選択します。
2. [**エクスポート**]をクリックします。
3. 標準のファイル選択ダイアログボックスを使用して、ファイルに名前を付け、場所を選択します。
4. [**Save**]をクリックします。

保存した設定ファイルを使用したスキャン

保存した設定ファイルを使用してスキャンするには:

1. [**編集(Edit)**]メニューから[**デフォルト設定(Default Settings)**]を選択します。
2. [デフォルト設定(Default Settings)]ウィンドウの下部の左側の列で、[**ファイルから設定をロード(Load settings from file)**]をクリックします。

3. 標準のファイル選択ダイアログボックスを使用して、利用したい設定ファイルを選択し、[開く(Open)]をクリックします。

これで、選択したファイルがデフォルトの設定ファイルになります。

SmartUpdate

インターネットに接続しているインストール環境では、SmartUpdate機能がOpenTextデータセンターと通信して、新規または更新されたアダプティブエージェント、脆弱性チェック、およびポリシー情報を確認します。SmartUpdateでは、OpenText DASTの最新バージョンを使用しているかどうかも確認され、新しいバージョンがダウンロード可能な場合には通知されます。

アプリケーションを起動するたびにSmartUpdateを実行するようにOpenText DASTを設定できます([**編集(Edit)**]メニューから[**アプリケーション設定(Application Settings)**]を選択し、[**スマートアップデート(Smart Update)**]を選択します)。

OpenText DASTユーザインタフェースからSmartUpdateをオンデマンドで実行することもできます。このためには、OpenText DASTの[**開始ページ(Start Page)**]から[**SmartUpdateを開始(Start SmartUpdate)**]を選択するか、[**ツール(Tools)**]メニューから[**SmartUpdate**]を選択するか、または標準ツールバーの[**SmartUpdate**]ボタンをクリックします。詳細については、「"ツール(Tools)]メニュー" ページ53」および「"ツールバー" ページ57」を参照してください。

インターネットに接続していないインストール環境の場合は、"オフラインのSmartUpdateの実行" 次のページを参照してください。

注意! {/b}エンタープライズインストールの場合、OpenText DASTが使用する特定のファイルがSmartUpdateによって変更または置換されると、センササービスが停止し、センサで「オフライン」ステータスが表示されることがあります。OpenText DASTアプリケーションを起動し、サービスを再起動する必要があります。手順は次のとおりです:

1. **[編集(Edit)] > [アプリケーション設定(Application Settings)]**をクリックします。
2. **[センサとして実行(Run as a Sensor)]**を選択します。
3. [センサステータス(Sensor Status)]エリアの**[開始(Start)]**ボタンをクリックします。

SmartUpdateの実行(インターネットに接続している場合)

OpenText DASTがインターネットに接続している場合にSmartUpdateを実行するには:

1. 次のいずれかを実行します。
   - ツールバーで[**SmartUpdate**]をクリックします。
   - [**ツール(Tools)**]メニューから[**SmartUpdate**]を選択します。
   - OpenText DASTの[**開始ページ(Start Page)**]から[**SmartUpdateの開始(Start SmartUpdate)**]を選択します。

アップデートが利用可能な場合は、 [SmartUpdater]ウィンドウが開き、 [サマリ(Summary)]タブが表示されます。 [サマリ(Summary)]タブには、次のアイテムをダウンロードするための折りたたみ可能な別個のペインが最大3つ表示されます。

- 新規チェックおよび更新されたチェック
- OpenText DASTソフトウェア
- SmartUpdateソフトウェア

2. 1つ以上のダウンロードオプションに対応するチェックボックスをオンにします。
3. (オプション)更新されるチェックの詳細を表示するには
   a. [**チェックの詳細(Check Detail)**]タブをクリックします。
      左側のペインには、更新されるチェックのID、名前、およびバージョンを示すリストが表示されます。リストは [追加(Added)]、 [更新(Updated)]、および [削除(Delete)]でグループ化されます。
   b. 更新される特定のチェックを含むポリシーを確認するには、リストでそのチェックを選択します。
      影響を受けるポリシーのリストが [関連ポリシー(Related Policies)]ペインに表示されます。
4. (オプション)影響を受けるポリシーの詳細を表示するには:
   a. [**ポリシーの詳細(Policy Detail)**]タブをクリックします。
      左側のペインに、更新の影響を受けるポリシーが英字順で一覧表示されます。

      注記: このリストには、更新されるチェックの影響を受けるポリシーだけが表示されます。 [ポリシーの詳細(Policy Detail)]タブには、アップデートに含まれている可能性があるその他のポリシー変更(ポリシーへの新しいチェックの関連付けまたはポリシー名の変更など)は表示されません。

   b. 特定のポリシーで更新されるチェックを表示するには、リストからポリシーを選択します。
      [関連チェック(Related Checks)]ペインに、更新されるチェックのID、名前、およびバージョンを示すリストが表示されます。リストは [追加(Added)]、 [更新(Updated)]、および [削除(Delete)]でグループ化されます。
5. アップデートをインストールするには、 [**ダウンロード(Download)**]をクリックします。

OpenText DASTを更新せずにチェックをダウンロードする

スキャン中に特定のチェックを実行するには、エンジンの更新が必要です。最新バージョンのOpenText DASTを使用していない場合、スキャン中にSecureBaseのチェックの一部を実行できない可能性があります。すべて最新のチェックを使用してアプリケーションをテストするには、最新バージョンのOpenText DASTを使用している必要があります。

オフラインのSmartUpdateの実行

オフラインのOpenText DASTに対してSmartUpdateを実行するには、次の手順に従います。

ステージ	説明
1.	サポートケースを作成します。カスタマサポート担当者から、オフラインFTPサーバのURLとログイン資格情報が提供されます(必要な場合)。詳細については、「"序文" ページ25」を参照してください。
2.	インターネットにアクセスできるマシンで、オフラインFTPサーバにアクセスします。
3.	OpenText DASTのスタティックSmartUpdate ZIPファイルをダウンロードします。
4.	OpenText DASTがインストールされているマシンで、ZIPファイルからすべてのファイルを解凍します。
5.	OpenText DASTを閉じます。
6.	解凍した**SecureBase.db**ファイルおよび**version.txt**ファイルを、SecureBaseデータがあるディレクトリにコピーします。デフォルトの場所: `C:\ProgramData\HP\HP WebInspect\SecureBase` **ヒント:** Windowsでは、デフォルトではこれらのフォルダは表示されません。フォルダオプションを変更して隠しファイルを表示してください。

WebSphere Portalに関するFAQ

WebSphere Portalでアプリケーションが実行されているかどうかをどのように確認できますか?

通常、WebSphere Portalアプリケーションの URLは非常に長く、/wps/portalまたは/wps/myportalで始まり、その後にエンコードされたセクションが続きます。例:

```
http://myhost.com/wps/portal/internet/customers/home/!ut/p/b1/fY7BcoIwFAC_
xS94T4QCx6Rpk6qlo20x5tIJShEIJoID0q-vnfFq97Yze1hQIEEddV8W-lzaozZ_rh6-
HjkRfrhERBZ4-EKESBmde5ggzEEVxmbXNGW7-sIsKdgTW3c_
B3xmpzBfnacLv6QuIfxVHKJGhmNfzToue8nWdKg4fx8jtaT9MJpB2zQPgqLp9GrADyey0tvvL1F9Sn
ftm_
y0cbuw8Xbmvg2NN6412wlsQP27GAa3AO9AEBJhmxxcnWHlk8kverBIBQ!!/dl4/d5/L2dBISEvZ0FB
IS9nQSEh/
```

サポートされているWebSphere Portalのバージョンを教えてください。

バージョン6.1以降がサポートされています。

OpenText DASTでWebSphere Portalアプリケーションをスキャンするために特別な設定が必要な理由は何ですか?

URLのエンコードセクションには、「ナビゲーション状態」が含まれています。これは、現在のページで要素を表示する方法に関する情報(.NetのVIEWSTATEに似ています)と、ナビゲー

ション履歴です。このナビゲーション履歴は、自動Web探索プログラムを使用するときに問題となります。Web探索プログラムが各リンクにアクセスすると、ナビゲーション状態が更新されます。これにより、Web探索プログラムがすでにアクセスした可能性のあるページ上のリンクが継続的に変化します。新しいリンクのように見えるので、Web探索プログラムはこれらのリンクにアクセスします。このようにして動作が無限に循環することになります。

WebSphere Portalオーバーレイが選択されている場合、OpenText DASTはURLのナビゲーション状態をデコードし、URLがすでにアクセス済みかどうかを判断できます。これにより、Web探索プログラムが同じページを何度も続けてアクセスすることが防げます。

OpenText DASTはナビゲーション状態をどのようにデコードしますか?

WebSphere Portal 6.1以降には、URLデコードサービスが含まれています。WebSphere Portalオーバーレイが選択されている場合、OpenText DASTはURLをデコードサービスに渡し、応答を評価してこのURLがすでにアクセス済みであるかどうかを判断できます。デコードサービスはデフォルトでオンになっていますが、WebSphere Portalサーバの設定でオフにすることもできます。OpenText DASTでサイトを適切にスキャンできるようにするには、デコードサービスを有効にする必要があります。

ナビゲーション状態とは特別なセッションIDでしょうか?

いいえ。ナビゲーション状態には、セッション情報は含まれていません。セッションはクッキーにより維持されます。

ログインマクロを記録する際の特別な手順はありますか?

クッキーJSESSIONIDおよびLtpaTokenを状態パラメータとして設定するようにしてください。

サイトツリーに深くネストされたフォルダが含まれているのはなぜですか?

現時点では、「OpenText DAST」のサイトツリーは、WebSphere Portal URLのナビゲーション状態を解析する方法を認識しません。各セクションはディレクトリとして扱われます。もちろん、これらは実際にはディレクトリではありません。通常、各ブランチの最下位レベルにドリルダウンして、実際のコンテンツを確認する必要があります。

OpenText DASTがWebSphere Portalアプリケーションに対して実行できる攻撃のタイプに制限はありますか?

OpenText DASTは、WebSphere Portalアプリケーションに対してすべての操作攻撃を実行できます。これには、XSS、SQLインジェクション、CSRF、RFI、LFIなどが含まれます(ただし、これだけには限定されません)。OpenText DASTは、WebSphere Portalサイトをスキャンするときにサイト検索攻撃を実行しません。これには、バックアップファイル(.bak、.old)、隠しファイル、隠しディレクトリ、およびプラットフォーム固有の環境設定ファイルの検索が含まれます。除外されている理由は、ほとんどの要求が、デフォルトのポータルビューに対して200応答を返す結果になり、エラー応答と有効な応答を区別する方法がないためです。

WebSphere PortalサイトでWeb探索プログラムが正しく動作しているかどうかをどのように確認できますか?

Web探索プログラムが最適な状態で動作できるようにするため、WebSphere Portalデコードサービスを有効にし、サーバ上で到達可能にする必要があります。動作しているかどうかを確認するには、URLを手動でデコードします。サイトからURLをコピーし、次のように変更します。

```
http://myhost.com/wps/poc?uri=state: path with navigation state>&mode=download
```

XML応答が返されます。あるいは、WebSphere Portalオーバーレイが選択されている状態でサイトのスキャンを開始します。Traffic Monitorを有効にするか、Web Proxy経由でスキャンを実行します。デコーダサービスに対する次の形式での周期的な要求が確認できます。

```
http://myhost.com/wps/poc?uri=state: path with navigation
state>&mode=download.
```

もう1つ考慮すべき点は、デコードサービスのパスをサーバ上で変更できる点です。これが当てはまる場合は、スキャン設定を手動で変更する必要があります。サポートについては、カスタマサポートにお問い合わせください。

ナビゲーション状態マーカーも変更できます。デフォルトではこれは`!ut/p`です。サーバでこれをデフォルトから変更した場合、スキャン設定を手動で変更する必要があります。サポートについては、カスタマサポートにお問い合わせください。

詳細については、「"序文" ページ25」を参照してください。

コマンドライン実行

OpenText DASTには、コマンドラインインタフェース(CLI)を通して使用できる次のアプリケーションが含まれています。

- WI.exe -既存のマクロを使用するスキャンの設定と実行、スキャンファイルとレポートのエクスポート、スキャンのマージ、スキャンの再利用、既存のスキャンのログインマクロのテストができます。詳細については、「"wi.exeの使用" 次のページ」を参照してください。
- WIScanStopper.exe -現在実行中のスキャンを停止することができます。詳細については、「"WIScanStopper.exeの使用" ページ347」を参照してください。
- MacroGenServer.exe -ログインマクロを作成することができます。詳細については、「"MacroGenServer.exeの使用" ページ348」を参照してください。

これらのアプリケーションは、OpenText DASTと同じディレクトリにインストールされます。デフォルトでは、インストールディレクトリは次の場所にあります。

```
C:\Program Files\Fortify\Fortify WebInspect
```

CLIの起動

CLIを起動するには、次のコマンドを実行します。

- Windowsの**コマンドプロンプト**(`cmd.exe`)アプリケーションを右クリックし、[**管理者として実行**]を選択します。

  管理者:コマンドプロンプト]ウィンドウが表示されます。

重要! {/b}コマンドプロンプトで、`cd`コマンドを使用して現在の作業ディレクトリをアプリケーションがインストールされているディレクトリに変更します。

OpenText DAST on DockerのCLIの制限

コマンドラインインタフェースからアクセス可能な一部のパラメータと機能は、OpenText DAST on Dockerでサポートされていません。サポートされていない項目は、そのように示されています。

wi.exeの使用

コマンドラインインタフェース(CLI)でプログラム`wi.exe`を使用して、各種のOpenText DAST機能を開始できます。コマンドを入力するときには次の構文を使用します。

```
wi.exe -u url [-api type] [-s file] [-ws file] [-Framework name]
       [-CrawlCoverage name] [-ps policyID | -pc path]
       [-ab|ac|an|ad|aa|ak|at creds] [-macro path] [-o|c] [-n name]
       [-e[abcdefghijklmnopst] file] [-x|xd|xa|xn] [-b filepath] [-db]
       [-d filepath -m filename] [-i[erxd] scanid | -ic scanid scanname
       | -im option scanid scanlist] [-r report_name -y report_type
       -w report_favorite -f report_export_file -g[phacxe]
       [-t compliance_template_file] [-v] [-?]
```

コマンドラインから複数のスキャンを実行するには、次のような形式でバッチファイルを作成して実行します。

```
c:
cd \program files\Fortify\Fortify WebInspect
wi.exe -u http://172.16.60.19 -ps 4
wi.exe -u http://www.mywebsite.com
wi.exe -u http://172.16.60.17
wi.exe -u http://172.16.60.16
```

オプション

次の表に、オプションの定義を示します。斜体で表示されている項目には値が必要です。

カテゴリ	オプション	定義
全般	`-?`	使い方のヘルプを表示します。
	`-u {url}`	開始URLまたはIPアドレスを指定します。 注意! {/b}`-u`パラメータを`-s`(設定ファイル)と一緒に使用する場合には、必要に応じて`-x`、`-xa`、`-`

カテゴリ	オプション	定義
		`xd`、または`-xn`パラメータを指定して、スキャンをフォルダに限定します。このように限定しないと、一定の条件下では無制限の監査が実行されることがあります。 URLにアンパサンド(&)が含まれている場合は、URLを引用符で囲む必要があります。
	`-api {type}`	スキャンするAPIタイプを指定します。*type*の有効な値は次のとおりです。 `GraphQL` `gRPC` `OData` `SOAP` `Swagger` 重要! {/b}次の例に示すように、SwaggerまたはOData定義ファイルのURLを指定する必要があります。 `-u http://172.16.81.36/v1 -api Swagger` 重要! {/b}`-u`オプションでは、次の例に示すように、サービスの定義ファイルまたはエンドポイントを指すことができます。 `-u http://172.16.81.36/v1 -api Swagger` 必要に応じて、認証やプロキシ設定などの追加情報を含めたスキャン環境設定ファイルを作成し、コマンドでその設定ファイルを指すことができます。詳細については、「"wi.exeを使用したAPIのスキャン" ページ186」を参照してください。

カテゴリ	オプション	定義
	`-s {filename}`	設定ファイルを指定します。設定ファイルのタイプはJSONとXMLです。 **注記:** コマンドラインパラメータは、設定ファイルの値よりも優先されます。
	`-db`	設定ファイルで定義されているデータベースを使用することを指定します。省略すると、OpenText DASTではアプリケーション設定に定義されているデータベース接続がデフォルトで使用されます。
	`-ws {filename}`	使用するWebサービス設計ファイルを指定します。
	`-o`	監査専用スキャンを指定します。
	`-c`	Web探索専用スキャンを指定します。
	`-n {name}`	スキャン名を指定します。
	`-b {filepath}`	使用するSecureBaseファイルを指定します。パスには、フルパスとファイル名を指定します。
	`-d {filepath}`	指定したファイルパスにデータベースを移動します。
	`-m {filename}`	指定したファイル名にデータベースを移動します。
	`-v`	詳細出力を作成します。
	`-tm`	Traffic Monitor (Traffic Viewer)のスキャンを有効にします。 重要! {/b}Traffic Monitorでは、スキャンからのトラフィックセッションファイル(`.tsf`)が必要です。Traffic Monitorを有効にしたス

カテゴリ	オプション	定義
		キャンをスキャンファイルに.scan フォーマットでエクスポートする必要がある場合は、-etオプションを使用して、トラフィックセッションファイルを含むすべてのスキャンログをエクスポートします。
	-ie {scanid}	指定したスキャンID (GUID)の設定済みスキャンを開始します。
	-ir {scanid}	指定したスキャンID (GUID)のスキャンを再開します。
	-ix {scanid}	指定したスキャンID (GUID)の既存スキャンを使用しますが、スキャンは続行されません。
	-id {scanid}	指定したスキャンID (GUID)のスキャンを削除します。
	-ii {scanid} {file path}	スキャンをインポートします。 **注記:** このパラメータは、OpenText DAST on Dockerではサポートされていません。
ルートフォルダに限定	-x	スキャンをディレクトリのみ(自己)に限定します。
	-xa	スキャンをディレクトリと親(先祖)に限定します。
	-xd	スキャンをディレクトリとサブディレクトリ(子孫)に限定します。
	-xn	参照されている設定ファイルの「フォルダに限定」ルールを無視します。 フォルダに限定パラメータ(x|xa|xb|xn)は、独自のカテゴリに含めることができます(レポートまたは出力として)。
フレームワーク	-framework	フレームワークの名前を指定します。

カテゴリ	オプション	定義
	`{framework_name}`	現在サポートされているのはOracle ADF Faces (Oracle)およびIBM WebSphere Portal (WebSpherePortal)のみです。いずれかのテクノロジを使用して構築されたアプリケーションのスキャンを最適化します。
Web探索のカバレッジ	`-CrawlCoverage {Coveragename}`	スキャンのカバレッジのタイプを指定します。*Coveragename*の値は次のとおりです。 `Thorough` =サイト全体を対象とした徹底的なWeb探索 `Default`=パフォーマンスよりもカバレッジに重点を置く `Moderate`=カバレッジと速度のバランスをとる `Quick`=範囲とパフォーマンスに重点を置く
監査ポリシー	`-ps {policy id}` **ヒント:** 複数のポリシーをポリシーIDのカンマ区切りリストとして指定できます。例: `-ps 1001,1002` 複数のポリシーを指定する場合、センサはスキャン中にポリシーを集約します。	使用する非カスタムポリシーを指定します。*policy id*の値は次のとおりです。 **ベストプラクティス** `1`=標準 `1012`= OWASP Top 10アプリケーションセキュリティリスク2013 `1024`= SANS Top 25 2011 `1025`= OWASP Top 10 2017 `1027`=一般データ保護規制(GDPR) `1034`= DISA-STIGV4R9 `1036`= DISA-STIGV4R10 `1037`= CWE Top 25 `1041`= OWASP Application Security Verification Standard (ASVS) `1043`= DISA-STIGV4R11 `1044`= API `1045`= DISA-STIGV5R1 `1046`= NIST-SP80053R5 `1047`= CWE Top 25 2020

カテゴリ	オプション	定義
		1048= CWE Top 25 2021 1049= OWASP Top 10 2021 **タイプ別** 3= SOAP 7=ブランク 1001= SQLインジェクション 1002=クロスサイト スクリプティング 1005=パッシブ 1008=重大および高の脆弱性 1010=アグレッシブSQLインジェクション 1011= NoSQLおよび Node.js 1013=モバイル 1015= Apache Struts 1016=トランスポート層セキュリティ 1020=権限のエスカレーション 1021=サーバサイド 1022=クライアント サイド 1026= DISA-STIG-V4R4 1029= DISA-STIG-V4R5 1030= DISA-STIG-V4R6 1031= DISA-STIG-V4R7 1032= DISA-STIGV4R8 1033= WebSocket 1035= PCI Software Security Framework 1.0 (PCI SSF 1.0) 1050= OAST 1055= PCI DSS 4.0 1056= OWASP API Top 10 - 2023 **非推奨** 2=攻撃(非推奨) 4=クイック(非推奨) 5=セーフ(非推奨) 6=開発(非推奨) 16= QA (非推奨) 17=アプリケーション(非推奨) 18=プラットフォーム(非推奨) 1009= OWASP Top 10アプリケーションセキュリティリスク2010(非推奨) 1014= OpenSSL Heartbleed (非推

カテゴリ	オプション	定義
		奨) 1018=標準(非推奨) 1019= 非推奨のチェック 1051= アグレッシブLog4Shell(非推奨) **危険** 1004=全チェック
	-pc {policy path}	使用するカスタムポリシーを指定します。パスには、フルパスとファイル名を指定します。例: C:\ProgramData\hp\HP WebInspect\MyCustomPolicy.policy
認証	-ab "userid:pwd"	基本モード(ユーザ名とパスワード)を指定します。
	-ac "userid:pwd"	ADFS CBTモード(ユーザ名とパスワード)を指定します。
	-an "userid:pwd"	NTLMモード(ユーザ名とパスワード)を指定します。
	-ad "userid:pwd"	ダイジェストモード(ユーザ名とパスワード)を指定します。
	-aa "userid:pwd"	自動モード(ユーザ名とパスワード)を指定します。
	-ak "userid:pwd"	Kerberosモード(ユーザ名とパスワード)を指定します。
	-am {macro path}	非推奨。-macroオプションを使用してください。
	-at "{type} {token}"	APIスキャンの認証モード(typeおよびtoken)を指定します。次に例を示します。 -at "Basic YWxh0GRpbjpvcGVuc2VzYW1l" *type*の認証モードは次のとおりです。

カテゴリ	オプション	定義
		Basic Bearer Digest HOBA Mutual Negotiate OAuth SCRAM-SHA-1 SCRAM-SHA-256 vapid **注記:** typeおよびtokenは、前に示したように二重引用符で囲む必要があります。
マクロ	-macro {macro path}	Webマクロ認証のマクロ名とディレクトリパスを指定します。
	-macro {url} {username} {password}	認証用の自動生成マクロを作成します。
ログインマクロパラメータ	-ls "userid:pwd"	SmartCredentialsのユーザ名とパスワードを指定された値に置き換えます。
	-lt "*name0:value0;name1:value1;...nameN:valueN*"	指定した名前に一致する既存のTruClientログインパラメータを置き換えます。
出力	-ea {filepath}	スキャンを従来の完全なXML形式でエクスポートします。
	-eb {filepath}	スキャンの詳細(完全)を従来のXML形式でエクスポートします。
	-ec {filepath}	スキャンの詳細(コメント)を従来のXML形式でエクスポートします。
	-ed {filepath}	スキャンの詳細(非表示フィールド)を従来のXML形式でエクスポートします。
	-ee {filepath}	スキャンの詳細(スクリプト)を従来のXML形式でエクスポートします。

カテゴリ	オプション	定義
	-ef {filepath}	スキャンの詳細(設定されているクッキー)を従来のXML形式でエクスポートします。
	-eg {filepath}	スキャンの詳細(Webフォーム)を従来のXML形式でエクスポートします。
	-eh {filepath}	スキャンの詳細(URL)を従来のXML形式でエクスポートします。
	-ei {filepath}	スキャンの詳細(要求)を従来のXML形式でエクスポートします。
	-ej {filepath}	スキャンの詳細(セッション)を従来のXML形式でエクスポートします。
	-ek {filepath}	スキャンの詳細(電子メール)を従来のXML形式でエクスポートします。
	-el {filepath}	スキャンの詳細(パラメータ)を従来のXML形式でエクスポートします。
	-em {folderpath}	スキャンの詳細(Webダンプ)を従来のXML形式でエクスポートします。
	-en {filepath}	スキャンの詳細(サイト外リンク)を従来のXML形式でエクスポートします。
	-eo {filepath}	スキャンの詳細(脆弱性)を従来のXML形式でエクスポートします。
	-ep {filepath}	指定したファイルにスキャンをFPR形式でエクスポートします。
	-eq {format} {filepath}	スキャンの詳細をサイトツリーからエクスポートします。詳細は次のとおりです。 • 要求が送信された日時(ミリ秒単位) • ホスト • パス • メソッド

カテゴリ	オプション	定義
		• ステータスコード • 要求から応答までの間の経過時間(ミリ秒単位) SPA (シングルページアプリケーション)スキャンの場合: • CSV形式では、SPADisplayName列とSPASelector列が含まれます。 • JSON形式では、SPADisplayNameおよびSPASelectorデータを含むSPAイベントが含まれます。 詳細については、「"SPAカバレッジ(SPA Coverage)" ページ66」を参照してください。 formatの値は次のとおりです。 `json` `csv` エクスポートする値に二重引用符が含まれている場合は、エスケープ文字(二重引用符)がCSV出力に追加されます。たとえば、セレクタ"Sign in"には二重引用符が含まれているので、CSVファイルには次のように表示されます。 `"//a[normalize-space(string(.))=""Sign in""]"` **ヒント:** このオプションを、`-ie`、`-ir`、`-ix`、またはいずれかのスキャン開始オプションと組み合わせて、データを取得するスキャンを指定します。例: `-ix {scan GUID} -eq {format} {filepath}`

カテゴリ	オプション	定義
	`-es {filepath}`	指定したファイルにスキャンを.scanフォーマットでエクスポートします。
	`-et {filepath}`	指定したファイルにスキャンとログを.scanフォーマットでエクスポートします。
	`-eu {filepath}`	他のすべての上書きを適用した後、指定したファイルにスキャン設定をエクスポートします。 **注記:** このパラメータではスキャンは実行されません。設定がエクスポートされ、終了します。
レポート	`-r {report_name}` **ヒント:** 複数のレポートを指定する場合は、レポート名をセミコロンで区切ります。すべてのレポートは1つのファイルにまとめられます。	実行するレポートの名前を指定します。*report_name*の有効な値は次のとおりです。 `Aggregate` `Alert View` `Attack Status` `Compliance` `Crawled URLs` `Developer Reference` `Duplicates` `Executive Summary` `False Positive` `QA Summary` `Scan Difference` `Scan Log` `Trend` `Vulnerability` `Vulnerability (Legacy)` **注記:** 空白を含むレポート名は引用符で囲む必要があります。
	`-w {favorite_name}`	実行するレポートのお気に入りの名前を指定します。
	`-ag`	レポートのお気に入りのレポートを集約します。

カテゴリ	オプション	定義
	`-y {report_type}`	レポートのタイプ(`Standard`または`Custom`)を指定します。
	`-f {export_file}`	レポートを保存するファイルのパスとファイル名を指定します。
	`-gp`	PDF (Portable Document Format)ファイルとしてエクスポートします。
	`-gh`	HTMLファイルとしてエクスポートします。
	`-ga`	生のレポートファイルとしてエクスポートします。
	`-gc`	RTF (リッチテキスト形式)ファイルとしてエクスポートします。
	`-gx`	テキストファイルとしてエクスポートします。
	`-ge`	Excelファイルとしてエクスポートします。
	`-t {filepath}`	使用するコンプライアンステンプレートファイルを指定します。
スキャンのマージ	`-ic {scan id}` `{scan name}`	マージターゲットスキャンを作成します。詳細については、このトピックの「"スキャンのマージ" ページ346」を参照してください。 **注記:** このパラメータは、OpenText DAST on Dockerではサポートされていません。
	`-im /o:{option}` `{merge target scan id}` `{source scan id1}` `{source scan id2}`	スキャンをマージします。詳細については、このトピックの「"スキャンのマージ" ページ346」を参照してください。*option*の選択肢は次のとおりです。 • `Replace` -ターゲットセッションおよび脆弱性をソースセッションおよび脆弱性に置き換えます。

カテゴリ	オプション	定義
		• ReplaceMergeVulns -ターゲットセッションをソースセッションに置き換え、ソース脆弱性をターゲットスキャンに追加します。 • Skip -両方のスキャンでセッションIDが同じ場合は、セッションや脆弱性をマージしません。 • SkipMergeVulns -両方のスキャンでセッションIDが同じ場合は、ターゲットセッションを置き換えず、ソースから脆弱性をコピーします。 • Smart -マージ時にソースおよびターゲットのポリシーと時刻を考慮します。 重要! {/b}-imパラメータを使用する前にマージターゲットスキャンを作成するには、-icパラメータを使用します。 **注記:** このパラメータは、OpenText DAST on Dockerではサポートされていません。
スキャンの再利用	-iz /o:{option} {source scan id} {settings filename}	スキャンの再利用の設定を作成します。*option*の選択肢は次のとおりです。 • Incremental -ソーススキャンと同じ設定を使用し、変更されたポリシーを適用します。これは、ソーススキャンでフラグを設定したチェックを無効にし、1回だけフラグを設定するポリシーです。このモードでは、新しいWeb探索対象部分のみが監査されます。新しいWeb探索が実行されますが、新しいセッションのみが監査されます。 • Remediation -ソーススキャンと同じ設定を使用し、変更されたポリ

カテゴリ	オプション	定義
		シーを適用します。これは、ソーススキャンでフラグを設定しなかったチェックを無効にするポリシーです。 *settings filename*は、作成する変更済み設定ファイルの名前です。 **注記:** このパラメータは、OpenText DAST on Dockerではサポートされていません。
スキャン検出事項の再テスト	`-iv <guid> {[<severity> | <vuln ID prefix>] ...} /s <file path>`	スキャンを開始して検出事項を再テストするときに使用できる設定ファイルを作成します。重大度または固有のsessionCheckFoundID (またはその両方)を使って検出事項を再テストできます。重大度もsessionCheckFoundIDも指定しない場合は、ベーススキャンのすべての検出事項が再テストされます。パラメータの構成要素は次のとおりです。 • *<guid>*はベーススキャンIDです。これは必須です。 • *<severity>*は、再テストする脆弱性の重大度です。一覧に指定されている重大度のフラグが付いている、ベーススキャンのすべての脆弱性が再テストされます。重大度のオプションは`Critical`、`High`、`Low`、および`Medium`です。 • *<vuln ID prefix>*は固有のsessionCheckFoundIDであり、SessionCheckFounds APIエンドポイントを使用して取得できます。詳細については、OpenText DAST REST API Swagger UIを参照してください。 **ヒント:** sessionCheckFoundIDのプレフィクスを指定できます。

カテゴリ	オプション	定義
		たとえば、`012f`は sessionCheckFoundID `012fa34124`と一致します。 • `/s <file path>`は、作成される脆弱性再テスト設定ファイルのディレクトリパスとファイル名です。このパラメータは必須であり、再テストを指定するため元のスキャンの設定を変更します。作成される新しい設定ファイルでは、再テストされる脆弱性が指定されます。 重大度とsessionCheckFoundIDを任意の順序で指定したリストを指定できます。次の例は、有効なリストを示しています。 `Critical 3156 High 1234`
ログインマクロのテスト	`-it {scan id}`	既存のスキャンのログインマクロをテストします。
Seleniumマクロ	`-selenium_workflow {ArrayOfSelenium Command object}`	Seleniumワークフロースキャンを作成します。 このコマンドを使用する際の完全なプロセスと手順については、「"Selenium WebDriverとの統合" ページ373」を参照してください。
	`-selenium_no_validation`	スキャンを実行する前にSeleniumコマンドの検証を無効にします。 重要! {/b}このパラメータを使用する場合は、1つ以上の許可ホストを指定する必要があります。 詳細については、「"Selenium WebDriverとの統合" ページ373」を参照してください。
	`-slm {SeleniumCommand`	スキャンのSeleniumログインマクロを

カテゴリ	オプション	定義
	object}または @"PathtoFilewithobject"	指定します。このオプションは、要素が1つのArrayOfSeleniumCommand objectか、SeleniumCommand objectを使用します。 SeleniumCommand objectまたはArrayOfSeleniumCommand objectを含むファイルのパスを指定するには、@"PathtoFilewithobject"を使用します。 「"Seleniumログインマクロの例" ページ346」を参照してください。 重要! {/b}LogoutCondition要素が必要です。
Postmanスキャン	-pwc {filename}	Postmanコレクションファイルを使用してスキャンを開始します。このオプションでは、カンマで区切られた複数のコレクションファイルが受け入れられます。次に例を示します。 -pwc pcOne,pcTwo,pcThree 詳細については、「"Postmanコレクションによるスキャン" ページ364」を参照してください。
	-pdac	Postmanの自動設定を無効にします。これによりPostmanコレクションの自動設定または分析がスキャンの前に実行されなくなります。
	-plc {Collection path}	Postmanログインコレクションのパスを指定します。
	-pls "logoutsignature"	ログアウト条件を指定します。このパラメータでは正規表現の拡張が受け入れられます。 重要! {/b}スペース文字は\sに置き換える必要があります。

カテゴリ	オプション	定義
	`-pec {filepath}`	スキャンで使用するPostman環境ファイルを指定します。
	`-pg {filepath}`	スキャンで使用するPostmanグローバル変数ファイルを指定します。
状態管理	`-rs {<ArrayOfResponseStateElement>} or "@{filepath}"`	応答状態ルールを指定します。このパラメータは、`ArrayOfResponseStateElement`要素またはファイルに保存されている応答状態ルールを受け入れます。これはBearerトークンおよびAPIキーに使用されます。 重要! {/b}ファイルに保存されている応答状態ルールを使用するには、@記号を使用してファイルパスを指定する必要があります。 例については、「"応答状態ルールの例" 次のページ」を参照してください。
その他の設定	`-ah {url} [,{url},...]`	許可ホストを一覧にします。URLは、スキーマ、ホスト、およびポート番号です。

例

次の例は、OpenText DASTホームディレクトリから実行される場合と同様のコマンドライン実行を示しています。

```
wi.exe -u www.anywebsite.com -ps 1 -ab MyUsername:Mypassword
```

```
wi.exe -u https://zero.webappsecurity.com
       -s c:\program files\webinspect\scans\scripted\
       -r "Executive Summary";Vulnerability -y Standard
       -f c:\program files\webinspect\scans\scripted\zero051105.xml -gx
```

ポリシーを指定しない場合、OpenText DASTはWebサイトのWeb探索を実行します(しかし監査は行いません)。

無効なポリシー番号を指定すると、OpenText DASTはスキャンを実行しません。

Seleniumログインマクロの例

Seleniumログインマクロオプションの例を次に示します。

```
-slm "<SeleniumCommand><Command>"wi command\"</Command>
   <AllowedHosts><string>http://hostname/</string>
   </AllowedHosts><LogoutCondition>Access\sDenied</LogoutCondition>
   </SeleniumCommand>"
```

応答状態ルールの例

応答状態ルールの例を次に示します。

```
-rs "<ArrayOfResponseStateElement><ResponseStateElement><name>
   AutoDetect</name><ReplaceRegexes><string>Authorization:\sBearer\s
   (?&lt;AutoDetect&gt;[^\r\n]*)\r\n</string></ReplaceRegexes>
   <SearchRegexes><string>""en"":""(?&lt;AutoDetect&gt; [-a-zA-Z0-9._
   ~+/]+?=*)""}$</string></SearchRegexes>
   </ResponseStateElement></ArrayOfResponseStateElement>"
```

ヒント: 応答状態ルールは、OpenText DASTユーザインタフェースの [スキャン設定: HTTP解析(Scan Settings: HTTP Parsing)] で作成できます。その後、スキャン設定XMLファイルを開き、`ResponseStateElement`を見つけてコピーし、`-rs`パラメータに貼り付けることができます。応答状態ルールの詳細については、「"スキャン設定: HTTP解析" ページ422」を参照してください。

次のコードは、ファイルに保存されている応答状態ルールを使用してPostmanスキャンを開始する例を示しています。

```
wi -pwc c:\BearerWorkflow.json -pdac -plc c:\BearerLogin.json -rs
   @c:\BearerResponseStateRule.txt -pls
```

スキャンのマージ

注記: この機能は、OpenText DAST on Dockerではサポートされていません。

既存のスキャンにマージすることはできません。最初に「ic」パラメータを使用してマージターゲットを作成する必要があります。

マージするスキャンはスキャン日の順にソートされ、その順序でマージされます。2つのスキャンでセッションIDが同一の場合には情報が失われるため、順序は重要です。この問題が発生した場合、デフォルトでは、前のセッションおよび脆弱性は後のセッションおよび脆弱性で上書きされます。マージ時にこの問題を防ぐには、同じセッションIDの処理に関する別のオプションを選択できます。

注記: マージは、2つのスキャンで同一のセッションIDが少数であるかまたはまったくない場合に最も有効に機能します。

すべてのマージスキャンオプションでは、ソーススキャンの監査ステータスが「完了(Complete)」のセッションだけがマージされます。セッション除外(監査から除外)はマージされません。詳細については、「"監査設定: 攻撃除外" ページ473」を参照してください。

コマンドライン引数のハイフン

コマンドライン引数(出力ファイルなど)でハイフンを使用できるのは、次のコマンドの「エクスポートパス」引数に示すように、引数を二重引用符で囲んだ場合だけです。

```
wi.exe -u http://zero.webappsecurity.com -ea "c:\temp\command-line-test-export.xml"
```

注記: プロセスは、タスクマネージャに表示されるWI.exeです。スキャンデータは一時的に作業ディレクトリにキャッシュされ、その後スキャンディレクトリに移動されます。

終了コード

WI.exeアプリケーションは、次の表に示す終了コードの1つを返します。

コード	説明
0	コマンドはエラーなしで完了しました。
-1または-3	エラーが発生しました。

WIScanStopper.exeの使用

WIScanStopper.exeアプリケーションを使用して、現在実行中のスキャンを停止できます。

注記: この機能は、OpenText DAST on Dockerではサポートされていません。

実行中のスキャンを停止するには、コマンドラインで次のコマンドを入力します。

```
WIScanStopper {scanid}
```

WIScanStopper.exeアプリケーションは、指定されたスキャンID (GUID)のスキャンを停止します。このアプリケーションは、次の表に示す終了コードの1つを返します。

コード	説明
0	スキャンは正常に停止しました。
1	指定された引数はGUIDではありません。有効なスキャンID (GUID)を使用してコマンドを再試行してください。

コード	説明
2	指定されたGUIDのスキャンがマシンで実行されていることが検出されませんでした。スキャンID (GUID)を検証し、コマンドを再試行してください。
3	スキャンの停止を待機中にタイムアウトが発生しました。 タイムアウトは60秒です。停止コマンドが送信されると、プロセスはスキャンが停止するまで待機します。60秒経過してもスキャンステータスが変わらない場合は、タイムアウトが発生し、プロセスからこのコードが返されます。
4	その他の例外が発生しました。

ヒント: `-ir {scanid}`パラメータを指定したWI.exeアプリケーションを使用して、停止したスキャンを再開できます。詳細については、「"オプション" ページ329」を参照してください。

MacroGenServer.exeの使用

MacroGenServer.exeアプリケーションにより、コマンドラインインタフェース(CLI)で開始URL、ユーザ名、およびパスワードを指定して、ログインマクロを作成できます。次のテキストは、CLIでこのアプリケーションを使用するためのサンプル構文を示しています。

```
macrogenserver.exe -u http://zero.webappsecurity.com/login.html -mu username -
mp password
```

オプション

次の表で、使用可能なオプションを定義します。

パラメータ	定義
`-u`	開始URLを指定します。このパラメータは必須です。
`-mu`	ログインフォームのユーザ名を指定します。このパラメータは必須です。 重要! {/b}ユーザ名に特殊文字が含まれている場合は、文字列を二重引用符で囲む必要があります。ユーザ名に二重引用符文字が含まれている場合は、エスケープ文字を使用して、引用符をユーザ名の一部として渡す必要があります。エスケープ文字を判別するには、使用している特定のコマンドラインインタフェースのマニュアルを参照してください。
`-mp`	ログインフォームのパスワードを指定します。このパラメータは必須です。

パラメータ	定義
	重要! {/b}パスワードに特殊文字が含まれている場合は、文字列を二重引用符で囲む必要があります。パスワードに二重引用符文字が含まれている場合は、エスケープ文字を使用して、引用符をパスワードの一部として渡す必要があります。エスケープ文字を判別するには、使用している特定のコマンドラインインタフェースのマニュアルを参照してください。
-m	ログインマクロの保存先のファイルパスを指定します。
-ps	プロキシサーバのIPアドレスまたはホスト名を指定します。 例: `macrogenserver.exe -u http://zero.webappsecurity.com -mu username -mp password -ps 127.0.0.1 -pp 8080` `macrogenserver.exe -u http://zero.webappsecurity.com -mu username -mp password -ps myproxyhostname -pp 8080`
-pp	プロキシサーバポートを識別します。
-at	ネットワーク認証タイプを指定します。オプションは次のとおりです。 • Basic • Digest • Ntlm • ADFS_CBT
-au	ネットワーク認証のユーザ名を指定します。
-ap	ネットワーク認証のパスワードを指定します。
-h	MacroGenServerアプリケーションのヘルプを表示します。

WISwag.exeツールの使用

WISwag.exeツールは、高度な方法でREST APIのスキャンを行う場合に使用できます。たとえば、環境設定ファイルを指定して、そこにパラメータ値を含めること、それによってホスト情報を上書きすること、またはそれによってスキームを定義すること(特にODataの場合)が必要な場合などです。WISwag.exeツールは、REST API定義を解析し、それをOpenText DASTが理解できる形式に変換するコマンドラインツールです。

サポートされているAPI定義とプロトコル

WISwagツールは、次に挙げるREST APIの定義とプロトコルをサポートしています。

- Open API Specificationバージョン2.0および3.0 (旧称Swagger Specification)詳細については、Swagger Webサイト(http://swagger.io/)にアクセスしてください。
- Open Data (OData)プロトコル(バージョン2、3、および4)。詳細については、OData Webサイト(http://www.odata.org/)にアクセスしてください。

ヒント: WISwagツールをODataで使用して、POSTでエンティティセットの要求を正常に作成することができない場合は、Web Macro Recorderの [HTTP詳細(HTTP details)]タブでエラーを表示して、エンティティの要件を判別してください。

WISwag.exeツールを探す

WISwag.exeツールはOpenText DASTのインストールに含まれており、インストールディレクトリにコピーされます。デフォルトでは、インストールディレクトリは次の場所にあります。

```
C:\Program Files\Fortify\Fortify WebInspect\
```

プロセスの概要

REST APIをスキャンするプロセスは次のとおりです。

ステージ	説明
1.	開発チームからREST API定義を入手します。
2.	次のいずれかを実行します。 • 設定ファイルがない場合は、WISwag.exeツールを使用して、REST API定義をOpenText DAST設定ファイルに変換します。このオプションでは、ワークフローマクロおよびカスタムパラメータルールも生成され、それらが設定ファイルに埋め込まれます。「"API定義から設定ファイルへの変換" ページ353」を参照してください。 • 設定ファイルがある場合は、WISwag.exeツールを使用して、REST API定義をOpenText DASTワークフローマクロに変換します。「"API定義からマクロへの変換" ページ353」を参照してください。
3.	webmacroまたは設定ファイルを使用して、REST APIのスキャンを実行します。

WISwag.exeのパラメータ

次の表に、WISwag.exeのパラメータの定義を示します。

パラメータ	説明
-a	JSON形式で、人間が読み取り可能なバージョンのAPI定義を、指定の出力ファイルに生成します。出力ファイルは拡張子.jsonを使用します。生成された設定ファイル内のAPI定義はbase64でエンコードされているので、このパラメータはデバッグに役立つ可能性があります。詳細については、「"-s" 次のページ」を参照してください。 **例:** `-a ./<api-def_filename>.json`
-ab	提供された認証トークンを、AuthorizationヘッダでBearerタイプの認証として渡します。このパラメータは、API定義の説明欄で「Authorization: Bearer」が指定されている場合にのみ適用可能です。 **例:** `-ab QWxhZGRpbjpPcGVuU2VzYW1l`
-c	カスタムパラメータルールを文字列のリストとして指定の出力ファイルに生成します。出力ファイルは拡張子.txtを使用します。生成されたテキストファイルは、基本スキャンウィザードの [詳細設定(Advanced Settings)] のURL書き換え設定にインポートできます。詳細については、「"スキャン設定:カスタムパラメータ" ページ428」を参照してください。 **出力例:** `/odata-v4-test/Odata4Service.svc/Products({ID})` `/odata-v4-test/Odata4Service.svc/Categories({ID})`
-h	スキャンする各監査セッションに対するHTTP要求を指定の出力ファイルに生成します。出力ファイルは拡張子.txtを使用します。デバッグのために要求をコピーしてHTTP Editorに貼り付けることができます。 **出力例:** `GET http://bhillwin7.spidynamics.com:8080/odata-v4-test/Odata4Service.svc/Products HTTP/1.1` `Accept: application/json;odata.metadata=full` `Host: bhillwin7.spidynamics.com:8080`

パラメータ	説明
	`` X-WISwag-ID: GET_/odata-v4-test/Odata4Service.svc/Products OData-Version: 4.0 If-Match: * ```
-i	入力ファイルと場所を指定します。入力ファイルには、API定義ファイルまたは環境設定ファイルを指定できます。デフォルト設定を上書きし、処理するエンドポイントを制御するには、環境設定ファイルを使用します。詳細については、「"環境設定ファイルの使用" 次のページ」を参照してください。 場所には、URLまたはローカルファイルを指定できます。 **例:** `-i http://mysite.com/api_def.json` `-i C:/myapi.json`
-it	入力のタイプを指定します。有効な値は、`odata`および`swagger`です。 **例:** `-it swagger` `-it odata`
-m	OpenText DASTマクロを指定の出力ファイルに生成します。出力ファイルは拡張子`.webmacro`を使用します。 **例:** `-m ./<macro_filename>.webmacro`
-ma	API定義ファイルの要求に権限付与ヘッダを挿入します。 **注記:** 環境設定ファイルで権限付与ヘッダを使用し、同じ権限付与ヘッダをAPI定義ファイルの要求に挿入する必要がある場合に便利です。
-s	OpenText DAST設定ファイルを指定の出力ファイルに生成します。設定ファイルには、API定義に加えて、設定の上書きがあればそれも追加されます。REST APIをスキャンする際には、このオプションを使用することをお勧めします。出力ファイルは拡張子`.xml`を使用します。 **例:** `-s ./<settings_filename>.xml`

API定義からマクロへの変換

API定義をOpenText DASTワークフローマクロに変換し、次いでこれをREST APIのスキャンに使用できます。これを行うには、コマンドラインプロンプトで次のコマンドを入力します。

```
WISwag.exe -it swagger –i http://<input_file_location> -m ./<macro_filename>.webmacro
```

その後、Web Macro Recorderツールでマクロを開き、その内容を確認します。

API定義から設定ファイルへの変換

API定義を、OpenText DASTの設定ファイルに変換できます。設定ファイルは監査専用として実行されるように設定され、REST API定義から派生したワークフローマクロおよびカスタムパラメータルールが含められます。

これを行うには、コマンドラインプロンプトで次のコマンドを入力します。

```
WISwag.exe -it swagger –i http://<input_file_location> -s ./<settings_filename>.xml
```

OpenText DASTでスキャン設定を開き、内容を確認します。ワークフローマクロおよびカスタムパラメータルールがすでに定義されているはずです。

環境設定ファイルの使用

REST API定義ファイルを使用してワークフローマクロと設定ファイルを作成する場合、マクロと設定ファイルにはデフォルトの値と設定だけが含まれることになります。WISwagツールによって生成されるHTTP要求をより詳細に制御するには、REST API定義の代わりに環境設定ファイルをWISwagツールに渡すことができます。この高度な設定は、特定の操作やパラメータを制御する必要がある場合に役立ちます。たとえば、ログアウトまたは削除操作などの特定の操作を、OpenText DASTスキャンから除外する必要があるかもしれません。「`excludeOperations`」プロパティに操作IDのリストを含めることでこれを実現できます。操作IDは、REST API定義で定義されています。テストする必要のある操作が少数に過ぎない場合は、allow-listによるアプローチの方が簡単な場合があります。その場合は、「`includeOperations`」リストを使用します。

詳細については、「"APIスキャン環境設定ファイルについて" ページ188」を参照してください。

環境設定ファイルの形式

環境設定ファイルは次のような形式になっています。

```
{ apiDefinition : 'http://mysite.com/api_def.json', /* ローカルファイルでもよい (例: C:/myapi.json) */ host : 'localhost:8080', /* 生成される要求ごとにホストを置き換える */ schemes : ['https', 'http'], /* これらのスキーマの両方に対して出力を
```

```
生成する */ preferredContentType : 'application/json', /* 選択できる場合は、
jsonを優先する */ excludeOperations : [ 'logoutUser', 'deleteUser' ], /* これ
らの操作に対しては出力を生成しない */ parameterRules : [ { name : 'userId',
value : 42, location : 'path', type : 'number', includeOperations :
['createNewUser', 'getUser'] /* このルールをこれらの操作にのみ適用する */ }, {
name : 'file', value : 'my file payload', filename : 'myfile.txt', location
: 'body', type : 'file' }, { name : 'Authorization', value : 'Basic
QWxhZGRpbjpPcGVuU2VzYW1l', location : 'header', inject : true /* 生成される
すべての要求にこのヘッダを追加する */ } ] } C:/myapi.json) */ host :
'localhost:8080', /* replace the host in every generated request */ schemes
: ['https', 'http'], /* generate output for both of these schemes */
preferredContentType : 'application/json', /* if given a choice, prefer
json */ excludeOperations : [ 'logoutUser', 'deleteUser' ], /* generate no
output for these operations */ parameterRules : [ { name : 'userId', value
: 42, location : 'path', type : 'number', includeOperations :
['createNewUser', 'getUser'] /* only apply this rule to these operations */
}, { name : 'file', value : 'my file payload', filename : 'myfile.txt',
location : 'body', type : 'file' }, { name : 'Authorization', value :
'Basic QWxhZGRpbjpPcGVuU2VzYW1l', location : 'header', inject : true /* add
this header to every generated request */ } ] }
```

正規表現

正規表現のパターンを作成する際には、特殊なメタ文字とシーケンスが使用されます。次の表に、これらの文字の一部を示し、その簡単な使用例を示します。推奨する他の参照先として「Regular Expression Library」(http://regexlib.com/Default.aspx)があります。

ヒント: 作成した正規表現の構文を確認するには、Regular Expression Editorを使用してください(システムにインストールされている場合)。

文字	説明
\	次の文字を特殊文字としてマークします。/n/は文字「n」に一致します。シーケンス/\n/は、改行文字に一致します。
^	入力または行の先頭に一致します。 文字クラスとともに使用すると、否定文字を意味します。たとえば、contentディレクトリ内の/content/enおよび/content/caを除くすべてを除外するには、/content/[^(en|ca)].*/.*を使用します。\S \D \Wも参照してください。

文字	説明
$	入力または行の末尾に一致します。
*	先行する文字の0回以上の反復と一致します。/zo*/は「z」とも「zoo」とも一致します。
+	先行する文字の1回以上の反復と一致します。/zo+/は「zoo」に一致しますが、「z」には一致しません。
?	先行する文字の0回または1回の出現と一致します。/a?ve?/は「never」の「ve」に一致します。
.	改行文字を除く任意の1文字に一致します。
[xyz]	文字セット。括弧内の任意の1文字に一致します。/[abc]/は「plain」の「a」に一致します。
\b	スペースなどの単語境界に一致します。/ea*r\b/は、「never early」の「er」に一致します。
\B	非単語境界に一致します。/ea*r\B/は「never early」の中の「ear」と一致します。
\d	1つの数字に一致します。[0-9]と同じです。
\D	数字以外の1文字に一致します。[^0-9]と同じです。
\f	改ページ文字に一致します。
\n	改行文字に一致します。
\r	キャリッジリターン文字に一致します。
\s	スペース、タブ、改ページなどの空白に一致します。[\f\n\r\t\v]と同じです。
\S	空白文字以外の文字に一致します。[^ \f\n\r\t\v]と同じです。
\w	アンダースコアを含む任意の単語文字に一致します。[A-Za-z0-9_]と同じです。
\W	任意の非単語文字に一致します。[^A-Za-z0-9_]と同じです。

通常の正規表現構文に対する拡張もOpenText DASTのエンジニアにより作成および実装されています。詳細については、「"正規表現の拡張" 次のページ」を参照してください。

正規表現の拡張

通常の正規表現(regex)構文に対する拡張がOpenTextのエンジニアにより開発および実装されています。正規表現を作成する場合は、以下で説明するタグと演算子を使用できます。

正規表現タグ

- [STATUSCODE]
- [BODY]
- [ALL]
- [URI]
- [HEADERS]
- [COOKIES]
- [STATUSLINE]
- [STATUSDESCRIPTION]
- [SETCOOKIES]
- [METHOD]
- [REQUESTLINE]
- [VERSION]
- [POSTDATA]
- [TEXT]

正規表現演算子

- AND
- OR
- NOT
- [ ]
- ( )

例

- (a)ステータス行にステータスコード「200」が含まれており、かつ(b)メッセージ本文のどこかに「logged out」という語句が含まれている応答を検出するには、次の正規表現を使用しま

す。

```
[STATUSCODE]200 AND [BODY]logged\sout
```

- 要求されたリソースが一時的に別のURI (リダイレクト)に存在することを示しており、かつ応答のどこかにパス「/Login.asp」への参照が含まれる応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]302 AND [ALL]Login.asp
```

- (a)ステータスコードが「200」、かつ「logged out」または「session expired」という語句が本文のどこかに含まれている、または(b)ステータスコード「302」、かつ応答のどこかにパス「/Login.asp」への参照が含まれている応答のいずれかを検出するには、次の正規表現を使用します。

```
( [STATUSCODE]200 AND [BODY]logged\sout OR [BODY]session\sexpired ) OR
( [STATUSCODE]302 AND [ALL]Login.asp )
```

注記: 「開き」括弧または「閉じ」括弧の前後にスペース(ASCII 32)を含める必要があります。そうしないと、括弧が誤って正規表現の一部と見なされます。

- リダイレクトLocationヘッダのどこかに「login.aspx」が現れるリダイレクト応答を検出するには、次の正規表現を使用します。

```
[STATUSCODE]302 AND [HEADERS]Location:\slogin.aspx
```

- ステータス行のReason-Phrase部に特定の文字列(「Please Authenticate」など)が含まれる応答を検出するには、次の正規表現を使用します。

```
[STATUSDESCRIPTION]Please\sAuthenticate
```

参照情報

"正規表現" ページ354

OpenText DAST REST API

このトピックでは、OpenText DAST REST APIに関する情報を提供します。

OpenText DAST REST APIとは

OpenText DAST REST APIは、プロキシとスキャナをリモート制御するための、システムとOpenText DAST間のRESTfulインターフェイスを提供します。OpenText DASTのインストール時に自動的にインストールされる、軽量Windowsサービス(WebInspect APIと呼ばれる)として動作します。Fortify Monitorツールを使用して、サービスを設定、開始、および停止します。OpenText DAST REST APIを使用して、既存の自動化スクリプトにセキュリティ監査機能を追加できます。

OpenText DAST REST APIは、業界標準のSwagger RESTful API Documentation Specificationバージョン2.0 (現在はOpenAPI Specificationとして知られている)を使用して完全に記述され、文書化されています。Swaggerのマニュアルに、REST APIの使用を簡素化するための詳細なスキーマ、パラメータ情報、およびサンプルコードが記載されています。また、エンドポイントを運用環境で使用する前にテストする機能も提供されます。

推奨

OpenTextでは、スキャンを一度に1回だけ実行することをお勧めします。SQL Expressを使用する場合は特に、サイトのサイズによっては、同時(または並行)スキャンを実行すると、OpenText DASTホスト上のRAM、CPU、およびディスクリソースの使用率が高くなる場合があります。

OpenText DAST REST APIの設定

OpenText DAST REST APIを使用する前に、それを設定する必要があります。

1. Windowsの [スタート]メニューから、 **[すべてのプログラム] > [OpenText] > [OpenText DAST Monitor]** の順にクリックします。
   OpenText DAST Monitorアイコンがシステムトレイに表示されます。
2. **[OpenText DAST Monitor]**アイコンを右クリックして、 **[DAST APIの設定(Configure DAST API)]**を選択します。
   [DAST APIの設定(Configure DAST API)]ダイアログボックスが表示されます。
3. 次の表の説明に従って、APIサーバの設定を行います。

設定	値
ホスト	OpenText DASTとOpenText DAST REST APIの両方が同じマシン上に存在する必要があります。デフォルト設定の [+]は、OpenText DAST REST APIに、 [ポート(Port)]フィールドで指定されたポート上のすべての要求を傍受するように指示するワイルドカードです。同じポート上で別のサービスを実行しており、APIサービス専用の特定のホスト名を定義したい場合は、この値を変更できます。
ポート	指定された値を使用するか、上/下矢印を使用して使用可能なポート番号に変更します。
認証(Authentication)	[認証(Authentication)]ドロップダウンリストから、 **[なし(None)]**、 **[Windows]**、 **[基本(Basic)]**、または **[クライアント証明書(Client Certificate)]**を選択します。 認証に対して **[基本(Basic)]**を選択した場合は、ユーザ名とパスワードを指定する必要があります。これには次の操作を行いま

設定	値
	す。 a. [パスワードの編集(Edit passwords)]ボタンをクリックし、テキストエディタを選択します。 wircserver.keysファイルがテキストエディタで開きます。このファイルには、サンプルのユーザ名とパスワードのエントリが含まれています。 username1:password1 username2:password2 b. サンプルを、サーバにアクセスするためのユーザ資格情報で置き換えます。追加の資格情報が必要な場合は、認証するユーザごとにユーザ名とパスワードをコロンで区切って追加します。1行あたりのユーザ名とパスワードは1つずつにする必要があります。 c. ファイルを保存します。 認証に対して[クライアント証明書(Client Certificate)]を選択した場合は、まず、信頼された認証局(CA)から発行されたルートSSL証明書に基づいてクライアント証明書を生成してから、クライアントマシンにインストールする必要があります。 **ヒント:** Windowsソフトウェア開発キット(SDK)のMakeCertユーティリティなどのツールを使用して、クライアント証明書を作成できます。
Use HTTPS (HTTPSを使用する)	HTTPS接続を介してサーバにアクセスする場合に、このチェックボックスをオンにします。 HTTPSを介してサーバを実行するには、サーバ証明書を作成してAPIサービスにバインドする必要があります。HTTPSを介してAPIをテストする自己署名証明書を素早く作成するには、Administrator PowerShellコンソールで次のスクリプトを実行します。 `$rootcertID = (New-SelfSignedCertificate -DnsName "DO NOT TRUST - WIRC Test Root CA","localhost", "$($env:computername)" -CertStoreLocation "cert:\LocalMachine\My").Thumbprint` `$rootcert = (Get-Item -Path "cert:\LocalMachine\My\$($rootcertID)")` `$trustedRootStore = (Get-Item -Path`

設定	値
	"cert:\LocalMachine\Root") $trustedRootStore.open("ReadWrite") $trustedRootStore.add($rootcert) $trustedRootStore.close() netsh http add sslcert ipport=0.0.0.0:8443 certhash=$($rootcertID) appid="{160e1003-0b46-47c2-a2bc-01ea1e49b9dc}" 前述のスクリプトは、ローカルホストの証明書とコンピュータ名を作成して、その証明書を個人用ストアとルート認証局に配置し、ポート8443にバインドします。別のポートを使用する場合は、スクリプトで使用されるポートを指定します。 重要! {/b}前述のスクリプトによって作成された自己署名証明書は、テストにのみ使用してください。この証明書はローカルマシンでのみ機能し、認証局からの証明書のセキュリティは提供しません。運用環境では、認証局によって生成された証明書を使用してください。
ログレベル	収集するログ情報のレベルを選択します。 **ヒント:** APIログファイルは、Windowsイベントビューアを使用して表示できます。ログファイルは、 **[アプリケーションとサービスのログ(Applications and Services Logs)] > [WebInspect API]** にあります。

4. 次のいずれかを実行します。
   - OpenText DAST REST APIサービスを開始し、API設定をテストするには、 **[APIのテスト(Test API)]** をクリックします。
     サービスが開始され、ブラウザが開いて、OpenText DAST REST API Swagger UIページに移動します。このページの詳細については、"OpenText DAST API Swagger UIへのアクセス" 下を参照してください。
   - API設定をテストせずにOpenText DAST REST APIサービスを開始するには、 **[開始(Start)]** クリックします。

OpenText DAST API Swagger UIへのアクセス

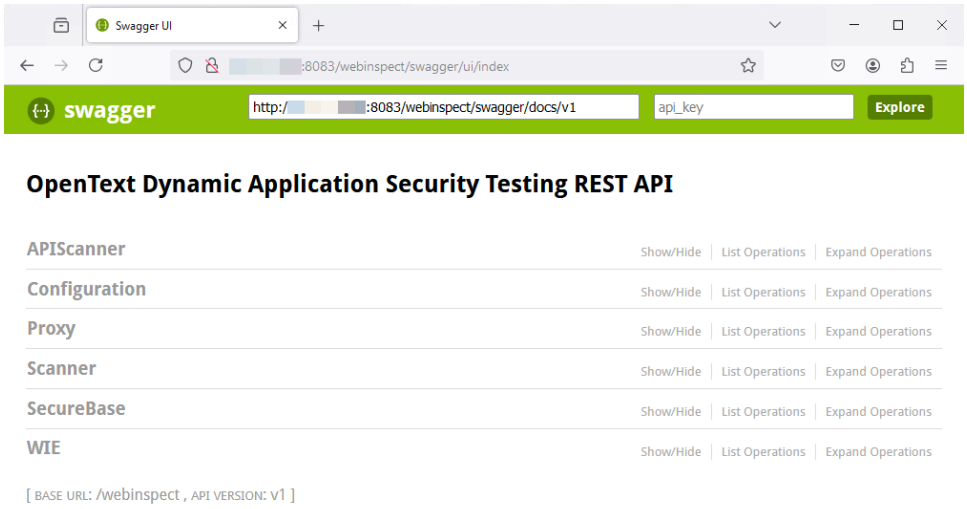
OpenText DAST API Swagger UIには、詳細なスキーマ、パラメータ情報、サンプルコード、およびエンドポイントのテスト機能を含む完全なマニュアルが付属しています。

この情報にアクセスするには:

1. OpenText DAST APIサービスを設定して起動したら、ブラウザを開きます。
2. アドレスフィールドに「`http://<hostname>:<port>/webinspect/api`」と入力し、**<Enter>**を押します。

   例: OpenText DAST REST APIの設定時にデフォルト設定を使用した場合は、「`http://localhost:8083/webinspect/api`」と入力します。

   OpenText DAST REST API Swagger UIページが表示されます。



APIバージョン間の切り替え

デフォルトでは、Swagger UIはOpenText DAST REST APIのバージョン1 (v1)で開きます。APIのバージョン2 (v2)には、完了に長い時間がかかる非同期バージョンのエンドポイントが含まれています。これらのエンドポイントを使用すると、ジョブのステータスと結果を取得するためにv2 `Job`エンドポイントと一緒に使用できるジョブトークンが生成されます。

OpenText DAST REST API v2に切り替えるには:

- Swagger UIで、URLの末尾にある**v1**を**v2**に変更します。

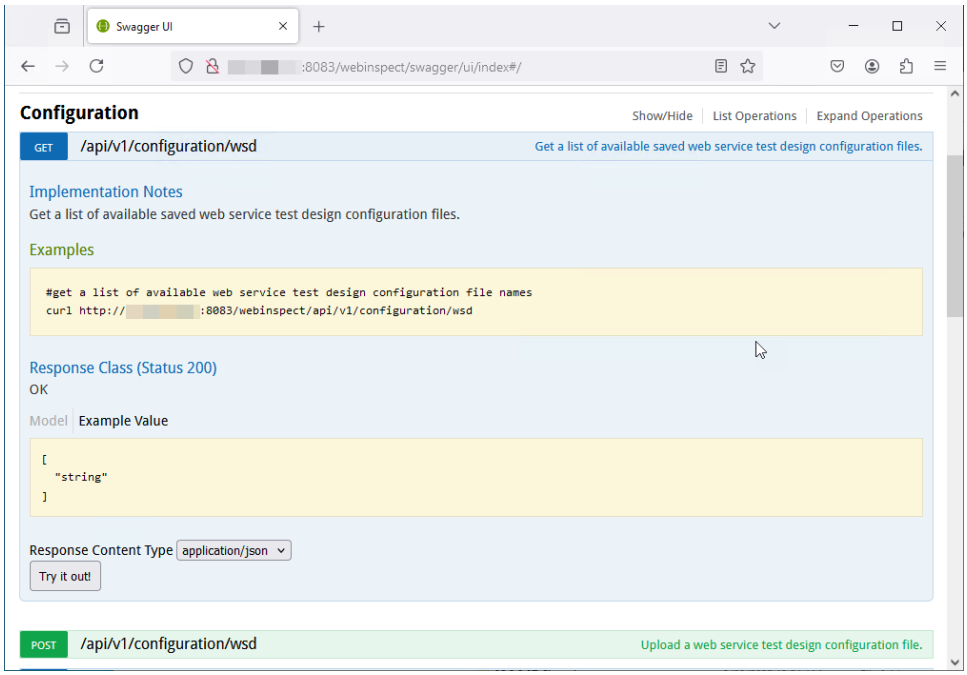
OpenText DAST REST API v1に戻るには:

- Swagger UIで、URLの末尾にある**v2**を**v1**に変更します。

Swagger UIの使用

Swagger UIを使用するには:

1. Swagger UIで、エンドポイントカテゴリをクリックします。
2. 使用するエンドポイントメソッドをクリックします。
   詳細なスキーマ、パラメータ情報、サンプルコード、およびエンドポイントのテスト機能が表示されます。

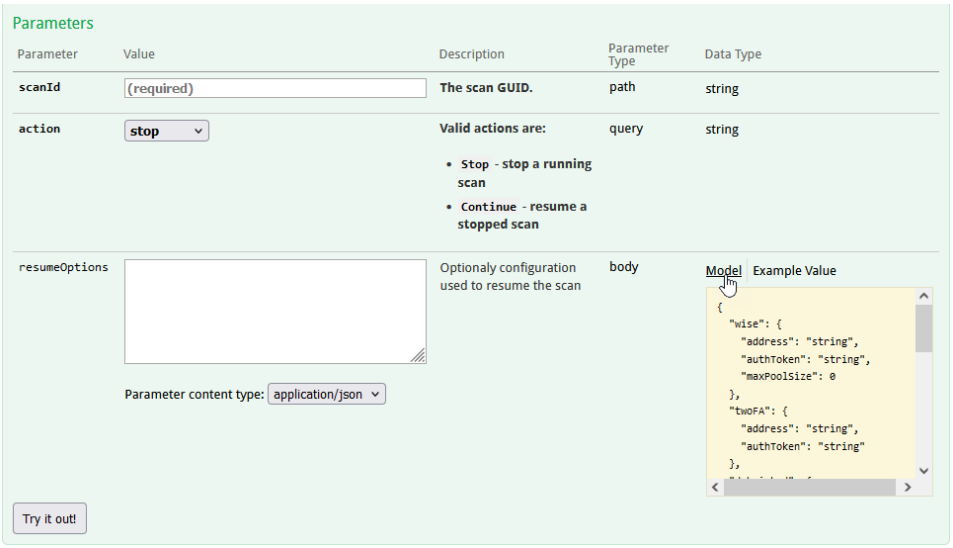


フィールドレベルの詳細の取得

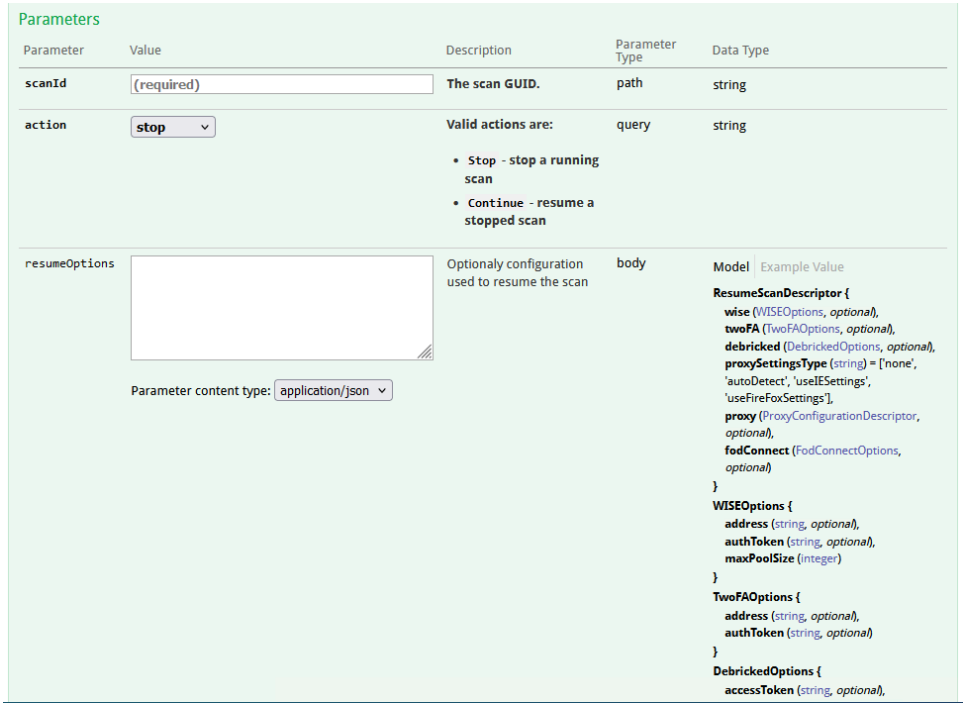
一部のAPIエンドポイントには、設定可能な多数のフィールドがあります。これらのフィールドの詳細については、Swagger UIを参照してください。

フィールドレベルの詳細を表示するには:

- エンドポイントの **[パラメータ(Parameters)]** セクションで、 **[データ型(Data Type)]** 見出しの下の **[モデル(Model)]** をクリックします。



すべてのエンドポイントフィールドの追加の詳細が表示されます。



OpenText DASTの自動化

OpenText DAST APIを使用して、既存の自動化スクリプトにOpenText DASTを追加できます。ユーザエージェントがサービスルータにアクセスできる限り、スクリプトをOpenText DASTとはまったく異なる環境に置くことができます。

OpenText DASTのアップデートとAPI

OpenText DASTをアップデートしたら、OpenText DASTユーザインタフェースを開いてからスキャンを開き、データベーススキーマの変更をスキャンデータベースに適用する必要があります。そうでない場合は、特定のAPIコマンドを実行するとエラーが表示される可能性があります。

Postmanコレクションによるスキャン

既存のPostman自動化テストスクリプト(コレクションとも呼ばれる)を使用して、REST APIアプリケーションのスキャンを実行できます。このトピックでは、Postmanおよび必要な追加のサードパーティソフトウェアに関する全般的な情報を提供します。

Postmanとは何か

PostmanはAPIの開発環境であり、APIの設計、協同、およびテストを実行できます。Postmanでは、API呼び出しのコレクションを作成することができ、各コレクションはサブフォルダおよび複数の要求に整理できます。コレクションをインポートおよびエクスポートできるため、開発環境とテスト環境間でファイルを簡単に共有できます。NewmanなどのCollection Runnerを使用すると、テストを複数回反復して実行できるため、繰り返しテストに要する時間を短縮できます。

Postmanコレクションの利点

REST APIアプリケーションでは、ブラウザや自動ツールを操作する人間が使用できる形式ですべてのエンドポイントが公開されるわけではありません。多くの場合、特定の要求データのセットが指定されたさまざまなpost、put、およびgetを受け入れるエンドポイントのコレクションに過ぎません。これらのエンドポイントを正常に監査するには、APIに関する重要な詳細をOpenText DASTが把握する必要があります。明確に定義されたPostmanコレクションでは、これらのエンドポイントを公開して、OpenText DASTでAPIアプリケーションを監査できるようにします。

Postman変数に関する既知の制限事項

OpenText DASTでは、Postmanのデータ変数はサポートされていません。ただし、コレクション変数、グローバル変数、および環境変数と、コレクション内にあるローカル変数はサポートされています。

回避策として、データ変数を環境で指定できます。環境とは、Postman要求で使用できる変数のセットです。

Postmanスキャンのオプション

次のいずれかのオプションを使用して、Postmanスキャンを実行できます:

- APIスキャンウィザード (「"APIスキャンウィザードの使用" ページ165」を参照してください)
- WI.exeまたはOpenText DAST REST API (「"WI.exeまたはOpenText DAST REST APIを使用したPostman APIスキャン" ページ371」を参照してください)

Postmanの前提条件

OpenText DASTでスキャンを実行するには、Postmanコレクションバージョン2.0または2.1が必要です。さらに、NewmanコマンドラインCollection Runner、Node.js、およびNode Package Manager (NPM)をインストールする必要があります。特定のバージョンに関する情報および追加の手順については、『*OpenText™ Application Securityソフトウェアのシステム要件*』を参照してください。

Postmanでのクライアント証明書の使用

Postmanスキャンの認証としてクライアント証明書を使用するには、証明書ファイル形式がWindowsでサポートされている必要があります。クライアント証明書がWindowsと互換性がない場合、証明書をWindowsと互換性のある形式に変換して、変換後のファイルをPostmanスキャンに使用できます。

次の表で、Postmanでクライアント証明書を変換および使用するプロセスについて説明します。

ステージ	説明
1.	OpenSSLなどのツールを使用して、証明書をWindows形式に変換します。
2.	OpenText DASTがインストールされているマシン上のWindows証明書ストアに、変換済みの証明書をインストールします。
3.	[スキャン設定:認証(Scan Settings: Authentication)]に証明書を追加します。詳細については、「"スキャン設定:認証" ページ440」を参照してください。

Postmanコレクションの準備のヒント

このトピックでは、優れたPostmanコレクションを作成するためのヒントを説明します。

有効な応答の確保

有効な応答を得るには、コレクションが完全で実行可能である必要があります。要求には次のものが含まれる必要があります:

- 有効な要求URL
- 正しいHTTPメソッド(POST、GET、PUT、PATCH、またはDELETE)
- APIを正しく実行するために必要な、有効なパラメータデータ

たとえば、「name」パラメータがある場合、デフォルトのデータ型「string」ではなく、「King Lear」または「Hamlet」のような実際のサンプルデータを指定する必要があります。

要求の順序

操作または要求の順序は重要であることに注意してください。たとえば、データに対してGET操作やDELETE操作を実行するには、事前にパラメータに対してサンプルデータを作成(またはPOST)する必要があります。

ヒント: OpenText DASTでコレクションの実行中にURLエラーが発生しないようにするには、コレクション内に正しい順序でAPI要求をバンドルした後、各要求をクリックしてから **保存(Save)**]をクリックして、要求を個別に保存します。

認証の処理

APIで認証が必要な場合は、Postmanコレクションで設定する必要があります。認証を設定する場合は、次のガイドラインに従います:

- ユーザ資格情報は最新でなければならず、有効期限が切れていてはなりません。
- 環境を使用して認証情報を指定する場合は、Postmanコレクションで認証環境のタイプを選択します。
- コレクション内のすべての要求で認証が必要とは限らず、すべての要求で同じタイプの認証が必要であるとは限りません。ご使用のコレクションにこれが該当する場合は、コレクション内の各要求に適切な認証タイプを指定してください。

  重要! {/b}スキャンでさまざまな認証タイプを使用中にセッション状態が失われた場合、正しく復元されません。セッション状態を適切に復元するには、単一の認証タイプでログインマクロまたはPostmanログインコレクションを使用します。

スタティック認証の使用

スタティック認証を使用する場合、Postmanコレクションでユーザ資格情報を名前と値のペアとしてハードコードする必要があります。OpenText DASTでは、コレクションファイルの解析時に、使用される認証タイプが判断され、コレクションからキー名と値が取得されます。その後、これらの値はスキャン設定に追加されます。

OpenText DASTでは、次のタイプのスタティック認証がサポートされています:

- APIキー
- 基本
- Bearerトークン
- ダイジェスト
- NTLM
- Oauth 1.0
- Oauth 2.0

ダイナミック認証の使用

ダイナミック認証を使用する場合、Bearerトークン認証変数またはAPIキー認証変数を、Postman環境ファイルまたはコレクションファイルのいずれかに保存する必要があります。たとえば、Bearerトークンでは`{{bearerToken}}`などの変数を使用できます。

応答状態ルールで正規表現を使用して、スキャン中にBearerトークンまたはAPIキーをダイナミックに指定する必要があります。応答状態ルールでは検索と置換のオプションが用意されており、トークンまたはキーを応答から取得して将来のセッションで使用することができます。詳細については、「"スキャン設定: HTTP解析" ページ422」を参照してください。

Postmanログインマクロの使用

OpenText DAST REST APIまたはWi.exeで、Postmanコレクションファイルの形式のログインマクロとワークフローマクロを指定できます。たとえば、`LoginBearer.json`のようなログインマクロファイルを指定できます。ただし、ログインマクロを使用する場合は、正規表現`The\stoken\sis\snot\svalid`などのログアウト条件も指定する必要があります。

Postmanの自動設定

スタティック認証の自動設定は、ユーザ名とパスワードがコレクションの認証セクションでハードコードされている場合など、認証値が既知の場合にサポートされています。自動設定が無効でない場合、OpenText DASTによってコレクションファイルの認証部分で有効な値が確認され、その値がスキャン設定に適用されます。

ダイナミック認証の自動設定では、ログインマクロと応答状態ルールの指定が自動的に試行されます。これは、BearerトークンまたはAPIキーが変数に保存されている場合に便利です。成功すると、Postmanコレクションの認証が検出されたことを示すメッセージが表示されます。Bearerトークンが検出されていても、安定した設定が作成されていない場合、自動設定に失敗したというメッセージが表示され、その理由が示されます。

重要! {/b}ダイナミック認証の自動設定は、Bearerトークン認証を使用する単純なケースでのみ機能します。

自動設定が失敗した場合は、認証を手動で設定する必要があります。詳細については、「"ダイナミックトークン用のPostmanログインの手動設定" 次のページ」を参照してください。

Postmanのサンプルスクリプト

Postman APIを活用するためのサンプルコードを https://github.com/fortify/WebInspectAutomationで入手できます。

PostmanコレクションのサンプルをGitHubのFortifyリポジトリ (https://github.com/fortify/WebInspectAutomation/tree/master/PostmanSamples)でダウンロードできます。

ダイナミックトークン用のPostmanログインの手動設定

このトピックでは、Postmanスキャンで自動設定が失敗した場合に、ダイナミック認証を手動で設定する方法について説明します。ダイナミック認証ではダイナミックトークンが使用されます。

ダイナミックトークンとは何か

ダイナミックトークンは、ソフトウェアによって生成される認証トークンであり、認証のインスタンスごとに固有です。トークンは短時間で作成でき、各インスタンスは個別に更新されます。

作業を開始する前に

手動ログインを設定するには、次の情報を把握している必要があります:

- アプリケーションで使用される認証のタイプ(Bearer、APIキー、OAuth1.0、OAuth 2.0、クッキーなど)
- 正規表現の検索引数の作成方法

プロセスの概要

ログインを手動で設定するプロセスは、次の表のとおりです。

ステージ	説明
1.	1つ以上のログイン要求を識別して、別々のPostmanコレクションに分離します。詳細については、「"ログイン要求を識別して分離する" 次のページ」を参照してください。
2.	ログアウト条件の正規表現を作成します。詳細については、「"正規表現を使用したログアウト条件の作成" 次のページ」を参照してください。
3.	応答状態ルールを作成します。詳細については、次を参照してください。 • "Bearerトークンの応答状態ルールの作成" 次のページ • "APIキーの応答状態ルールの作成" ページ370 **注記:** クッキーセッション管理では、応答状態ルールは必要ありません。

ログイン要求を識別して分離する

ログイン要求を識別して分離するには:

1. Postmanコレクションの内容を調べて、ログイン要求を識別します。

   ヒント: 通常、ログイン要求はPostmanコレクションの最初の要求であり、認証トークンを取得するものです。ただし、認証には複数の要求が含まれる場合があります。

2. この要求または複数の要求をコピーします。
3. 要求を別々のファイルに貼り付けます。
4. ファイルをPostmanコレクションとして保存します。

正規表現を使用したログアウト条件の作成

ログアウト条件を作成するには:

1. 認証を必要とする複数の要求を検索します。
2. 次のいずれかを実行します。
   - Bearerトークンの場合は、認証トークンを間違った値に置き換え、アプリケーションに送信する。
   - APIキーの場合は、アプリケーションに間違ったAPIKey値を送信する。
3. これらの要求からの応答を使用して、これらの応答に一致し、かつ有効なセッションと一致しない正規表現を作成します。

   たとえば、ほとんどの場合に「unauthorized」という単語が表示される場合は、正規表現でその語を使用するのが最適です。次に例を示します。

   ```
   [STATUSCODE]200 AND [BODY]unauthorized
   ```

   間違ったAPIKey値を送信して、「{"status": "Access Deny"}」という応答が得られた場合、最適な正規表現は次のようなものかもしれません。

   ```
   [BODY]Access\sDeny
   ```

Bearerトークンの応答状態ルールの作成

Bearerトークンの応答状態ルールを作成するには、2つの正規表現を作成する必要があります。

1つ目の正規表現では、すべての応答で認証トークンの更新を検索します。通常、このトークンは、プロセスのステージ1で識別されたログイン要求に対応するものです。

たとえば、次の応答には、「token」への参照があります。

```
"{"success":true,"message":"Authentication
   successful!","token":"eyJhbGciOiJIUzI1NiIs
```

```
    InR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluI
    iwiaWF0IjoxNTg1NzQzNzkzLCJleHAiOjE1ODU3NDc
    zOTN9.i8uXa20JQt00tlOjd1twRD76jTnsG-0xiU97 QWy6jkg"}"
```

この応答に対して、次の正規表現を作成できます:

```
"token":"(?<Token>[-a-zA-Z0-9._~+/]+?=*)"}$
```

この正規表現では、`(?<Token>[-a-zA-Z0-9._~+/]+?=*)`によってトークンの値が識別されます。

注記: XMLでは文字のエスケープが使用されます。XML形式で<および>を含む正規表現を使用する場合、<記号は`<`を使用してエスケープし、>記号は`>`を使用してエスケープします。

2つ目の正規表現で、このトークンを保存する場所を示します。Bearerトークンの場合、「Authorization: Bearer ...」ヘッダ内に配置されます。

Bearerトークンの例を次に示します:

```
Authorization:\sBearer\s(?<Token>[^\r\n]*)\r\n
```

この2つ目の正規表現では、1つ目の正規表現の値で置き換える値が`(?<Token>[^\r\n]*)`によって識別されます。

APIキーの応答状態ルールの作成

APIキーの応答状態ルールを作成するには、2つの正規表現を作成する必要があります。

1つ目の正規表現では、すべての応答で認証トークンの更新を検索します。通常、このトークンは、プロセスのステージ1で識別されたログイン要求に対応するものです。

たとえば、authのAPIキータイプのヘッダがあるとします。要求によって、ユーザ名とパスワードがパス「/Login」に送信され、次のような応答が返されます。

```
"{"success":true,"APIToken": "tp8989ieupgrjynsfbnfgh9ysdopfghsprohjo"}"
```

すべての保護された要求から、アクセスを承認するために「APIKey: ....」ヘッダが送信されます。

この応答に対して、次の正規表現を作成できます:

```
"APIToken":"(?<APIToken>[a-zA-Z0-9]+?)"}$
```

注記: XMLでは文字のエスケープが使用されます。XML形式で<および>を含む正規表現を使用する場合、<記号は`<`を使用してエスケープし、>記号は`>`を使用してエスケープします。

2つ目の正規表現で、このトークンを保存する場所を示します。APIKeyの場合、カスタムヘッダの名前と値、またはカスタムクエリパラメータの名前と値を指定できます。

```
APIKey:\s(?<APIToken>[^\r\n]*)\r\n
```

WI.exeまたはOpenText DAST REST APIを使用したPostman APIスキャン

このトピックでは、OpenText DAST REST APIまたはWi.exeでPostmanコレクションを使用してスキャンを実行するプロセスについて説明します。APIスキャンウィザードを使用してスキャンを実行するには、"APIスキャンウィザードの使用" ページ165を参照してください。

推奨

OpenTextでは、スキャンを一度に1回だけ実行することをお勧めします。SQL Expressを使用する場合は特に、サイトのサイズによっては、同時(または並行)スキャンを実行すると、OpenText DASTホスト上のRAM、CPU、およびディスクリソースの使用率が高くなる場合があります。

プロセス

次の表で、Postmanコレクションを使用してスキャンを実行するプロセスについて説明します。

ステージ	説明
1.	Postmanで次の操作を実行します: 1. このトピックでこれまでに説明したガイドラインに従って、Postmanコレクションファイルを作成します。 2. Postman内の各API呼び出しを個別に保存します。 3. [**ランナ(Runner)**]をクリックして、NewmanコマンドラインCollection Runnerを開きます。
2.	NewmanコマンドラインCollection Runnerで次の操作を実行します: 1. Collection Runnerでコレクションを開いた状態で、API呼び出しが正しい実行順序であることを確認します。 2. [***<Collection Name>*を実行(Run <Collection Name>)**]をクリックします。 3. 各呼び出しからの応答を検査して、要求が成功したことを確認します。
3.	OpenText DASTで次のいずれかを実行します: • OpenText DAST REST APIを使用するには:

ステージ	説明
	a. OpenText DAST APIを設定して起動します。「"OpenText DAST REST APIの設定" ページ358」を参照してください。 b. Swagger UIでPostman APIエンドポイントにアクセスします。「"OpenText DAST API Swagger UIへのアクセス" ページ360」を参照してください。 c. Swagger UIの指示に従ってエンドポイントを設定します。 d. Swagger UIまたは任意のAPIツールからエンドポイントサンプルスクリプトを実行します。 重要! {/b}スキャン設定ファイルには、Postmanコレクション内のサイトへのアクセスを提供する適切な設定を含めます。たとえば、正しい許可ホスト、プロキシ設定などを含めます。設定ファイルを指定しない場合、OpenText DASTのデフォルトのスキャン設定がスキャンに適用されます。 • Wi.exeを使用するには: a. "コマンドライン実行" ページ328の説明に従って、CLIを起動します。 b. "wi.exeの使用" ページ329で説明されているPostmanスキャンオプションを使用して、コマンドを作成します。
4.	エンドポイントまたはCLIコマンドによって、スキャンID (GUID)およびPostmanコレクションの結果が返されます。

Postmanスキャンのトラブルシューティング

Postmanコレクションを使用したスキャンの実行中に問題が発生した場合は、次のトラブルシューティングのヒントを使用します:

1. スキャン設定でプロキシ設定を確認し、常にPostmanがプロキシ経由で実行され、テスト用のサイトにアクセスできるようにします。1つの方法として、プロキシ設定を使用して手動でNewmanを実行してみるという方法があります。
2. 要求の結果を確認します。
   a. 送信された要求の総数を表示して、Postmanファイル内の要求数と一致していることを確認します。
   b. 失敗した要求がないことを確認します。

Selenium WebDriverとの統合

OpenText DASTをSelenium WebDriver (Selenium 2.0とも呼ばれる)と統合して、次の操作を実行できます。

- `WI.exe`コマンドラインツールを使用してスキャンを実行する
- OpenText DAST REST APIを使用してワークフローマクロを作成する

既知の制限事項

OpenText DASTをSelenium WebDriverを統合する場合の既知の制限事項は次のとおりです。

- OpenText DASTは、Selenium WebDriverのみをサポートしています。
- OpenText DASTは、RemoteWebDriverクラスなどのリモートサーバ設定を使用するSelenium WebDriverをサポートしていません。
- Selenium WebDriverマクロは、ワークフローマクロとしてのみ使用できます。ログインマクロまたは起動マクロとして使用することはできません。
- コマンドラインインタフェース(CLI)またはAPIからのみ、Selenium WebDriverマクロを使用してスキャンを開始できます。ユーザインタフェースからスキャンを開始することはできませんが、Selenium WebDriverマクロの再スキャンおよびインポート/エクスポートは可能です。
- Fortify WebInspect Enterpriseのサポートは限定的です。CLIまたはAPIから作成したマクロファイルを使用できますが、それはセンサマシン上でSelenium WebDriver環境のセットアップを完了した場合に限られます。

プロセスの概要

次の表では、OpenText DASTとSelenium WebDriverを統合するプロセスについて説明します。

ステージ	説明
1.	OpenText DASTは、OpenText DASTプロキシを使用してWebブラウザからトラフィックをキャプチャできる必要があります。プロキシキャプチャを有効にするには、次のいずれかを実行します。 • "Seleniumスクリプトへのプロキシの追加" ページ375の説明に従って、コード内で直接Seleniumスクリプトにプロキシを追加するか、コマンドラインインタフェースのプレースホルダを使用してプロキシを追加します。 • Firefoxを使用する場合は、"OpenText DAST geckodriver.exeの使用" ページ378の説明に従って、OpenText DAST geckodriver.exeを使用してトラフィッ

ステージ	説明
	クをキャプチャします。
2.	"Selenium WebDriver環境のインストール" ページ379の説明に従って、OpenText DASTを実行しているマシンにSelenium WebDriver環境をインストールします。
3.	"コマンドラインからのテスト" ページ379の説明に従って、コマンドラインからSelenium WebDriverスクリプトを起動し、許可ホストを定義できることを確認します。
4.	必要に応じて、"OpenText DASTへのファイルのアップロード" ページ382の説明に従って、すべてのスクリプトとその依存関係をSelenium APIにアップロードするか、OpenText DASTを実行しているマシンに手動でコピーします。
5.	"Seleniumコマンドの使用" ページ383の説明に従って、ステージ3のコマンドを使用し、WI.exeを使用してスキャンを実行するか、OpenText DAST REST APIを使用してマクロを作成します。
6.	発生したエラーを修復します。 WI.exeでスキャンを実行するか、APIでマクロを作成すると、マクロが検証されます。Seleniumコマンドごとにエラーと警告が返されます。この機能はデフォルトで有効になっています。無効にするには: • WI.exeで、引数 `-selenium_no_validation`パラメータを使用します。詳細については、「"wi.exeの使用" ページ329」を参照してください。 • APIで、`VerifyMacro`パラメータを`false`に設定します。詳細については、OpenText DAST REST API Swagger UIを参照してください。 問題をトラブルシューティングするには、スキャンログでエラーを確認し、StateRequestorログで警告を確認します。 **ヒント:** 通常、ログは次のディレクトリパスに書き込まれます。 • デフォルトユーザであるSYSTEM USERでAPIスキャンが実行されている場合、ログは次の場所に書き込まれます。 `C:\ProgramData\HP\HP WebInspect\Schedule\logs\<scan_guid>\ScanLog` `C:\ProgramData\HP\HP WebInspect\Schedule\logs\<scan_guid>\StateRequestor` • すべてのCLIおよびUIスキャンのログと、APIスキャンが現在のユーザで実行されている場合のログは、次の場所に書き込まれます。

ステージ	説明
	C:\Users\<*user.name*>\AppData\Local\HP\HP WebInspect\Logs\<*scan_guid*>\ScanLog C:\Users\<*user.name*>\AppData\Local\HP\HP WebInspect\Logs\<*scan_guid*>\StateRequestor

Seleniumスクリプトへのプロキシの追加

Webブラウザからのトラフィックをキャプチャするこの方法を使用するには、Selenium初期化にプロキシを適用するOpenTextコードを自分のコードの中に直接追加するか、該当する場合はコマンドラインインタフェース(CLI)で引数として渡します。

長所

Seleniumがサポートする任意のブラウザから実行できるため、このアプローチには柔軟性があります。さらに、この方法ではいくらかのアップグレードプロテクションが提供されます。OpenTextコードはスクリプト内に存在するため、コードを少し変更するだけで、今後のバージョンのSeleniumでも引き続き使用することができます。

短所

この方法では、ブラウザを正しく初期化するために、OpenTextコードをスクリプトに一度手動で追加する必要があります。

サンプルコード

`Fortify_WI_Proxy`という名前の環境変数から値を取得し、それをWebブラウザと信頼証明書に対するHTTPおよびHTTPSのプロキシとして保存する必要があります。方法はプログラミング言語ごとに異なります。次のセクションでは、いくつかの言語のサンプルコードを示します。

注記: これらのコードサンプルは、Selenium WebDriverバージョン3.14に基づいています。ご使用の特定のバージョン用のコードは異なる場合があります。

C#

C#コードでは、ブラウザドライバが初期化されている場所を見つけて、それにブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
ChromeOptions chromeOptions = new ChromeOptions(); string proxy =
Environment.GetEnvironmentVariable("Fortify_WI_Proxy"); if
(!String.IsNullOrEmpty(proxy)) { chromeOptions.AcceptInsecureCertificates =
true; chromeOptions.Proxy = new Proxy(); chromeOptions.Proxy.HttpProxy =
proxy; chromeOptions.Proxy.SslProxy = proxy; } ….new ChromeDriver
```

```
(chromeOptions) // オプションはこのクラスに含める
```

Firefoxブラウザの例を次に示します。

```
FirefoxOptions config = new FirefoxOptions(); string proxy =
Environment.GetEnvironmentVariable("Fortify_WI_Proxy"); if
(!String.IsNullOrEmpty(proxy)) { config.AcceptInsecureCertificates = true;
config.Proxy = new Proxy(); config.Proxy.HttpProxy = proxy;
config.Proxy.SslProxy = proxy; } … new FirefoxDriver(config))
```

Java

Javaコードでは、ブラウザドライバが初期化されている場所を見つけて、それにブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
ChromeOptions options = new ChromeOptions(); String wi_proxy =
System.getenv("Fortify_WI_Proxy"); if (wi_proxy != null) { Proxy proxy =
new Proxy(); proxy.setHttpProxy(wi_proxy); proxy.setSslProxy(wi_proxy);
options.setProxy(proxy); options.setAcceptInsecureCerts(true); }
ChromeDriver driver=new ChromeDriver(options);
```

Firefoxブラウザの例を次に示します。

```
FirefoxOptions options = new FirefoxOptions(); String wi_proxy =
System.getenv("Fortify_WI_Proxy"); if (wi_proxy != null) { Proxy proxy =
new Proxy(); proxy.setHttpProxy(wi_proxy); proxy.setSslProxy(wi_proxy);
options.setProxy(proxy); options.setAcceptInsecureCerts(true); }
FirefoxDriver driver=new FirefoxDriver(options);
```

JavaScript

JavaScriptコードでは、ブラウザドライバが初期化されている場所を見つけて、ブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
const selProxy = require('selenium-webdriver/proxy'); …… (async function
example() { let env =process.env.Fortify_WI_Proxy; if (env) { let caps = {
acceptInsecureCerts: true }; //すべての証明書の受諾を許可する let proxy = {
http: env, https: env }; // env変数をプロキシとして適用する driver = await new
Builder().withCapabilities(caps).setProxy (selProxy.manual
(proxy)).forBrowser('chrome').build(); // プロキシとacceptInsecureCertsを設定
する }else driver = await new Builder().forBrowser('chrome').build();
```

Firefoxブラウザの例を次に示します。

```
const selProxy = require('selenium-webdriver/proxy'); …… let env
=process.env.Fortify_WI_Proxy; if (env) { let caps = { acceptInsecureCerts:
true }; //すべての証明書の受諾を許可する let proxy = { http: env, https: env
}; // env変数をプロキシとして適用する driver = await new Builder
().withCapabilities(caps).setProxy (selProxy.manual(proxy)).forBrowser
('firefox').build(); // プロキシとacceptInsecureCertsを設定する }else driver =
await new Builder().forBrowser('firefox').build();
```

Python

Pythonコードでは、ブラウザドライバが初期化されている場所を見つけて、それにブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
capabilities1 = DesiredCapabilities.CHROME.copy() Fortify = os.environ.get
('Fortify_WI_Proxy') if Fortify is not None: prox = Proxy() prox.proxy_type
= ProxyType.MANUAL prox.http_proxy = Fortify prox.ssl_proxy = Fortify
prox.add_to_capabilities(capabilities1) cls.driver = webdriver.Chrome
(executable_path='C:/chromedriver.exe', desired_capabilities=capabilities1)
```

Firefoxブラウザの例を次に示します。

```
import os from selenium.webdriver import DesiredCapabilities from
selenium.webdriver.common.proxy import Proxy, ProxyType …… capabilities1 =
DesiredCapabilities.FIREFOX.copy() Fortify = os.environ.get('Fortify_WI_
Proxy') if Fortify is not None: capabilities1['acceptInsecureCerts'] = True
prox = Proxy() prox.proxy_type = ProxyType.MANUAL prox.http_proxy = Fortify
prox.ssl_proxy = Fortify prox.add_to_capabilities(capabilities1) cls.driver
= webdriver.Firefox(executable_path='C:/geckodriver.exe',
capabilities=capabilities1)
```

Ruby

Rubyコードでは、ブラウザドライバが初期化されている場所を見つけて、それにブラウザオプションを追加する必要があります。Chromeブラウザの例を次に示します。

```
http_proxy = ENV['Fortify_WI_Proxy'] if http_proxy proxy =
Selenium::WebDriver::Proxy.new(http: http_proxy, ssl: http_proxy)
capabilities = Selenium::WebDriver::Remote::Capabilities.chrome (accept_
insecure_certs: true) capabilities.proxy = proxy; else capabilities =
Selenium::WebDriver::Remote::Capabilities.chrome() end driver =
Selenium::WebDriver.for :chrome, desired_capabilities: capabilities
```

Firefoxブラウザの例を次に示します。

```
http_proxy = ENV['Fortify_WI_Proxy'] if http_proxy proxy =
Selenium::WebDriver::Proxy.new(http: http_proxy, ssl: http_proxy)
capabilities = Selenium::WebDriver::Remote::Capabilities.firefox (accept_
insecure_certs: true) capabilities.proxy = proxy; else capabilities =
Selenium::WebDriver::Remote::Capabilities.firefox() end driver =
Selenium::WebDriver.for :firefox, desired_capabilities: capabilities
```

CLIの使用

スクリプトがプロキシを設定する引数を受け入れる場合は、この方法を使用してOpenText DASTプロキシをスクリプトに追加できます。たとえば、`-proxy "<host:port>"`という名前の引数がある場合、次のように、実行時にコマンドでプレースホルダ`{Fortify_WI_Proxy}`を使用できます。

```
-proxy "{Fortify_WI_Proxy}"
```

ホストとポートを個別に指定する必要がある場合は、次のようにそれぞれに対してプレースホルダを使用できます。

```
-proxy "{Fortify_WI_Proxy_Host}:{Fortify_WI_Proxy_Port}"
```

これらの引数は、実行時にスクリプト内のプレースホルダをOpenText DASTプロキシに置き換えます。

OpenText DAST geckodriver.exeの使用

GeckoDriverは、W3C WebDriver互換のクライアントがGeckoベースのブラウザと通信できるようにするプロキシです。`geckodriver.exe`アプリケーションはFirefoxブラウザ用にこのプロキシを提供します。この方法でWebブラウザからのトラフィックをキャプチャするには、既存の`geckodriver.exe`を、`<InstallationDirectory>\Extensions`フォルダにあるOpenText DAST `geckodriver.exe`に置き換える必要があります。

注記: デフォルトのインストールディレクトリは`C:\Program Files\Fortify\Fortify WebInspect\Extensions`です。

長所

この方法では必要な作業が少なくなります。

短所

最新バージョンのgeckodriver.exeを使用できません。また、Firefoxスクリプトだけを使用する必要があります。

Selenium WebDriver環境のインストール

OpenText DASTがインストールされているマシンに、Seleniumスクリプトを実行するために必要なすべてのソフトウェアとツールをインストールする必要があります。これには次のものが含まれますが、これに限定されません。

- ブラウザ
- テストランナ
- Seleniumスクリプトの実行をサポートするために必要なすべての前提条件ソフトウェア
  たとえば、.NET NUnitフレームワークの場合、`.NET`と、Seleniumスクリプトを実行する実行可能ファイルとして`nunit3-console.exe`をインストールする必要があります。

重要! {/b}必要なソフトウェアとツールは、プログラミング言語によって異なります。

コマンドラインからのテスト

コマンドラインからSelenium WebDriverスクリプトを起動して実行できるようにするには、Seleniumスクリプトを実行するコマンドを作成して使用する必要があります。使用するコマンドは、Seleniumテストの実行に使用するプログラミング言語およびテストフレームワークによって異なります。

たとえば、.NETでNUnitを実行するには、次のようなコマンドを実行できます。

```
D:\tmp\selenium_wd\bin\net35\nunit3-console.exe "D:\tmp\selenium_
wd\selenium_c_sharp-master\Selenium\bin\Debug\Selenium.dll"
```

この例では、`nunit3-console.exe`はユニットテストランナであり、`Selenium.dll`はユニットテストが含まれているDLLです。詳細については、「"Seleniumコマンドの作成" 下」を参照してください。

ヒント: `POST /configuration/selenium/folder`および`GET /configuration/selenium/file/{foldername}` APIエンドポイントを使用して、展開したファイルのフルパスを表示できます。この情報を使用して、CLIのコマンドを更新できます。詳細については、「"OpenText DASTへのファイルのアップロード" ページ382」を参照してください。

Seleniumコマンドの作成

Seleniumコマンドは、ユニットテストを実行するためにコマンドラインで使用します。ほとんどの場合、このコマンドはビルドサーバでのユニットテストの実行時またはデバッグ時に使用されます。このコマンドは、使用しているユニットテストフレームワークによって異なります。各フレームワークには専用のランナとコマンドライン引数があります。以降のセクションでは、さまざまな言語での各種フレームワークに関するヒントとサンプルコマンドについて説明します。

.NET MSTest

MSTestフレームワークは、Vstest.console.exeというツールを次の構文で使用します。

```
<Path_to_Vstest_Executable>\Vstest.console.exe <Path_to_Unit_Test_
dlls>\<TestFileNames> <Options>
```

ほとんどの場合、この実行可能ファイルを呼び出すときにはDLL (実行するテストファイル名)のリストを指定する必要があります。次のサンプルコードは、2つのテストファイルを実行します。

```
"C:\Program Files (x86)\Microsoft Visual Studio 14.0\Common7\IDE\
   CommonExtensions\Microsoft\TestWindow\vstest.console.exe"
   "C:\Projects\Tests\bin\TestHomepage_unittest.dll"
   "C:\Projects\Tests\bin\AddCart_unittest.dll"
```

.NET NUnit

NUnitフレームワークは、nunit3-console.exeというツール(バージョン3.*x*)を次の構文で使用します。

```
NUNIT3-CONSOLE <InputFiles> <Options>
```

この実行可能ファイルを呼び出すときにはDLL (実行するテストファイル名)のリストを指定する必要があります。次のサンプルコードは、2つのテストファイルを実行します。

```
C:\nunit\net35\nunit3-console.exe "C:\Projects\Tests\bin\TestHomepage_
   unittest.dll" "C:\Projects\Tests\bin\AddCart_unittest.dll"
```

xUnit.net

xUnit.netフレームワークには、xunit.console.exeおよびxunit.console.x86.exeという2つのコマンドラインランナがあります。次の構文を使用します。

```
xunit.console <assemblyFile> [configFile] [assemblyFile [configFile]...]
[options] [reporter] [resultFormat filename [...]]
```

xUnit.netでは環境設定ファイル(configFile)のファイル拡張子として.jsonおよび.xmlを使用できます。

該当する実行可能ファイルを呼び出すときには、DLL (実行するテストファイル名)のリストを指定する必要があります。次のサンプルコードは、2つのテストファイルを実行します。

```
C:\xunit\xunit.console.exe "C:\Projects\Tests\bin\TestHomepage_
   unittest.dll" "C:\Projects\Tests\bin\AddCart_unittest.dll"
```

Java TestNG

TestNGフレームワークには、クラスパス(-cp)オプションで指定したtestng.jarライブラリと、java.exeアプリケーションが必要です。-cpオプションに、プロジェクトを実行するために必要なすべてのライブラリクラスを一覧にする必要があります。次の構文を使用します。

```
java -cp "<Path_to_testngjar>/testng.jar:<Path_to_Test_Classes>"
org.testng.TestNG <Path_to_Test_xml>
```

次のサンプルコードは、XMLテストファイルを実行します。

```
C:\Program Files\Java\jdk-12.0.1\bin\java.exe -cp ".\libs\: C:\Program
   Files\jbdevstudio4\studio\plugins\*" org.testng.TestNG testng.xml
```

Java JUnit

JUnitフレームワークには複数のバージョンがあり、バージョンごとに独自のテスト実行コマンドがあります。`-cp`オプションに、プロジェクトを実行するために必要なすべてのライブラリクラスを一覧にする必要があります。

JUnitバージョン5.*x*では次の構文を使用します。

```
java -jar junit-platform-console-standalone-<version>.jar --class-path <Path_
to_Compiled_Test_Classes> --scan-class-path
```

JUnitバージョン4.*x*では次の構文を使用します。

```
java -cp .\libs\:<Path_to_Junitjar>\junit.jar org.junit.runner.JUnitCore [test
class name]
```

JUnitバージョン3.*x*では次の構文を使用します。

```
java -cp .\libs\:<Path_to_Junitjar>\junit.jar junit.textui.TestRunner [test
class name]
```

次のサンプルコードは、テストクラスを実行します。

```
C:\Program Files\Java\jdk-12.0.1\bin\java -cp
   C\java\libs\:C:\junit\junit.jar org.junit.runner.JUnitCore
   C:\project\test.class
```

Python unittestおよびPyUnit

Pythonには、ご使用のPythonのバージョンに応じてPython unittestまたはPyUnitという組み込みのユニットテストモジュールがあります(`-m`)。これらのフレームワークは、次の構文を使用します。

```
python -m unittest [options] [tests]
```

この構文の`[tests]`には、任意の数のテストモジュール、クラス、およびテストメソッドのリストを指定できます。次のコマンドは、Pythonのunittestのヘルプを表示します。

```
python -m unittest -h
```

次のサンプルコードは、unittestモジュールで`tests.py`という名前のテストファイルを実行します。

```
C:\Python\Python37-32\python.exe -m unittest
   C:\SampleProjects\POMProjectDemo\Tests\tests.py
```

Ruby RSpec

RSpecフレームワークでは、Rubyコードのユニットテストライブラリが提供されます。このフレームワークは、次の構文を使用します。

```
<Path_to_RSpec>\rspec.bat [options] [files or directories]
```

次のサンプルコードは、テストライブラリを実行します。

```
C:\Ruby26-x64\bin\rspec.bat -I C:\Ruby26-x64\Project\lib\ C:\Ruby26-
   x64\Project\spec\calculator_spec.rb
```

JavaScript Jest

Jestでは、JavaScriptコードでテストを作成および実行するためのJavaScriptライブラリが提供されます。このフレームワークは、次の構文を使用します。

```
<Path_to_Jest>\jest.js [--config=<pathToConfigFile>] [TestPathPattern]
```

次のサンプルコードは、テストライブラリを実行します。

```
C:\Users\admin\AppData\Roaming\npm\jest.cmd" --
   config=C:\Users\admin\AppData\Roaming\npm\jest.config.js
   C:/Users/admin/AppData/Roaming/npm/sum.test.js
```

OpenText DASTへのファイルのアップロード

コマンドラインインタフェース(CLI)でスキャンを実行するか、APIを使用してマクロを作成するには、OpenText DASTがインストールされているマシンにすべてのスクリプトとその依存関係をアップロードする必要があります。

CLIの使用

CLIからスキャンを実行するには、OpenText DASTがインストールされているマシンにファイルを手動でコピーする必要があります。

APIの使用

OpenText DAST REST APIでは、これらのファイルを展開するための次のエンドポイントが提供されます。

- `POST /configuration/selenium/folder` - ZIPファイルをアップロードおよび圧縮解除する
- `GET /configuration/selenium/folder` - すでにアップロードされているZIPファイルのリストを取得する
- `GET /configuration/selenium/file/{foldername}` - ZIPファイルに含まれているファイルのリストを取得する
- `DELETE /configuration/selenium/folder/{foldername}` - ZIPファイルを削除する

これらのエンドポイントの使用に関する詳細については、Swagger UIの特定のエンドポイントメソッドを参照してください。詳細については、「"OpenText DAST API Swagger UIへのアクセス" ページ360」を参照してください。

Seleniumコマンドの使用

Seleniumコマンドの作成とテストが完了したら、そのコマンドを使用して、WI.exeを使用してスキャンを実行するか、またはAPIを使用してマクロを作成することができます。

重要! {/b}Seleniumコマンドを使用してスキャンを実行すると、次のいずれかの場所にログディレクトリが作成されます。

`C:\Users\<UserName>\AppData\Local\Temp\`

`C:\Windows\Temp` (OpenText DAST REST APIがシステムユーザにより実行されている場合)

スキャンの実行中にgeckodriver.exeまたはchromedriver.exeプロセスを終了すると、これらの一時ファイルは削除されません。これらのファイルを手動で削除する必要があります。

WI.exeを使用したスキャンの実行

コマンドラインインタフェース(CLI)では、WI.exeに`-selenium_workflow`パラメータがあります。このパラメータは、`ArrayOfSeleniumCommand`というXMLオブジェクトをファイルまたは文字列として受け入れます。

重要! {/b}コマンドをファイルではなく文字列として実行し、コマンドに二重引用符(")が含まれている場合、これを`<Command>`タグに入れて保存するときに、二重引用符をバックスラッシュ文字(\)でエスケープする必要があります。たとえば、コマンドでパスに空白が含まれており、Command内で二重引用符を使用してこのパスを受け渡す場合、次のように引用符をエスケープする必要があります。

```
<Command>\"C:\Program Files\nunit\nunit3-console.ex\"
   C:\Projects\Tests\bin\TestHomepage_unittest.dll
   \"C:\Projects\Tests Main\bin\AddCart_unittest.dll\"</Command>
```

次の構文に従い、以前に作成したSeleniumコマンドをCommandタグに入れます。詳細については、「"Seleniumコマンドの作成" ページ379」を参照してください。

```
<ArrayOfSeleniumCommand> <SeleniumCommand> <Command>"Commands"</Command>
<AllowedHosts> <string>http://hostname/</string> </AllowedHosts>
<WorkingDirectory>C:\pathtoprojectfolder\</WorkingDirectory>
</SeleniumCommand> <SeleniumCommand> ... </SeleniumCommand> ...
</ArrayOfSeleniumCommand>
```

コマンドをファイルとして渡す場合は、次の構文を使用します。

```
-selenium_workflow "@PathToFile"
```

次のサンプルコードは、wd_firefox.txtというファイルをコマンドとして渡します。

```
-selenium_workflow "@D:\tmp\selenium_wd\wd_firefox.txt"
```

詳細については、「"wi.exeの使用" ページ329」を参照してください。

APIを使用したマクロの作成

APIを使用してマクロを作成するには、次のエンドポイントを使用します。

```
POST /configuration/selenium/macro
```

次のサンプルコードは、cURLを使用してマクロを追加します。

```
curl -X POST --header "Content-Type: application/json" -d "
   {\"VerifyMacro\":true,\"name\": \"test\",\"command\":
   \"D:\\tmp\\selenium_wd\\bin\\net35\\nunit3-console.exe
   \\\"D:\\tmp\\selenium_wd\\selenium_c_sharp-master\\Selenium\\
   bin\\Debug\\Selenium.dll\\\"\",\"allowedHosts\":
   [\"http://zero.webappsecurity.com\"]}"
   http://localhost:8083/webinspect/configuration/selenium/macro
```

次のサンプルコードは、cURLを使用してスキャンを開始します。

```
curl.exe -X POST --header "Content-Type: application/json" --header
   "Accept: application/json" -d "{\"settingsName\": \"Default\",
   \"overrides\": { \"startOption\": \"macro\", \"workflowMacros\": [\"test
   \"],\"AllowedHosts\":[\"\\*\"] , \"crawlAuditMode\": \"auditOnly\" } }"
   http://localhost:8083/webinspect/scanner/scans
```

使用法に関する詳細な情報とサンプルコードがSwagger UIに含まれています。オブジェクトは、"WI.exeを使用したスキャンの実行" 前のページで説明されているオブジェクトに似ています。詳細については、「"Swagger UIの使用" ページ362」を参照してください。

WorkingDirectoryおよびAllowedHosts引数はオプションです。場合によっては、AllowedHostsが自動的に判別されることがあります。ただし、OpenTextでは、マクロごとにAllowedHostsを設定することをお勧めします。

場合によっては、WorkingDirectory引数に「現在の作業ディレクトリ」である作業ディレクトリパスを設定する必要があります。

Burp API拡張機能について

Burp Suiteは、Webアプリケーションのセキュリティテストを実行するためのツールキットです。OpenText DASTには、Burp拡張機能が含まれています。この拡張機能を使用すれば、Burp Suiteユーザは、OpenText DAST APIを介してOpenText DASTをBurpに接続できます。

Burp API拡張機能を使用するメリット

OpenText DASTをBurpに接続すると、次のようなメリットが得られます。

- OpenText DASTスキャンから脆弱性のBurp問題を作成する
  - 現在実行中のまたは完了したスキャンで検出された脆弱性を要求する
  - 重大度などの指定された基準に基づいて脆弱性を要求する

  注記: OpenText DASTのチェックIDと名前は、Burp問題のIDと名前に対応しません。
- Burpでセッションを選択し、OpenText DASTに送信する

  注記: セッションを選択する理由は次のとおりです。
  - 実行中のスキャンでOpenText DASTのWeb探索に場所を追加する必要がある
  - 実行中のスキャンに新しい脆弱性を追加する必要がある
  - 完了したスキャンに新しい脆弱性を追加する必要がある
- OpenText DASTからスキャン情報を取得する
  - 特定のスキャンのステータスを取得する
  - 現在接続されているOpenText DASTデータベースで使用可能なスキャンのリストを取得する
  - スキャンのステータス(実行中/完了)に基づいてスキャンのリストを取得する

サポートされているバージョン

OpenText DAST Burp API拡張機能は、新しいBurp拡張機能APIと互換性があります。

参照情報

"OpenText DAST REST API" ページ357

"Burp API拡張機能の使用" 下

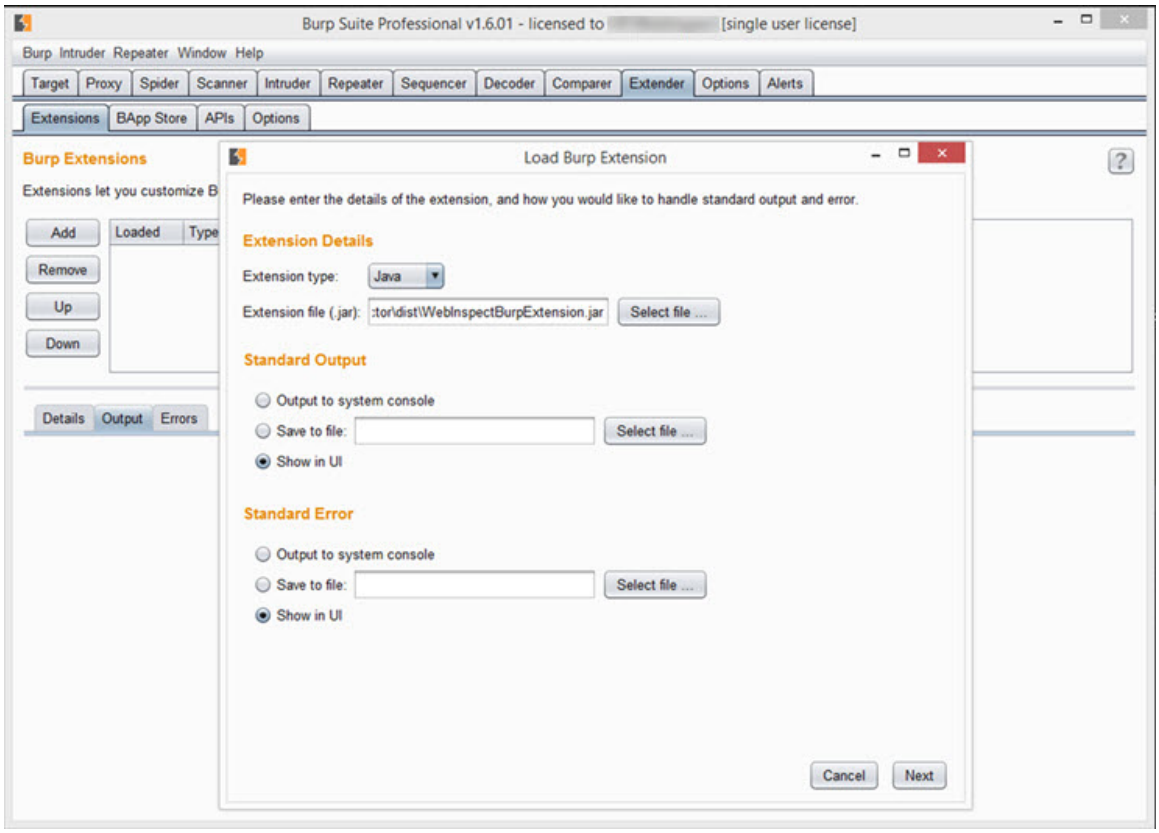
Burp API拡張機能の使用

このトピックでは、WebInspect Burp拡張機能を設定して使用する方法について説明します。

Burp拡張機能のロード

Burpで次のステップを実行して、WebInspect Burp拡張機能をロードします。

1. [エクステンダ(Extender)]タブで [拡張機能(Extensions)]を選択し、 [追加(Add)]をクリックします。
   [Burp拡張機能のロード(Load Burp Extension)]ウィンドウが表示されます。



2. [機能拡張ファイル(.jar) (Extension file (.jar))]フィールドで、 [ファイルの選択(Select file)]をクリックし、WebInspectBurpExtension.jarファイルに移動します。

   ヒント: WebInspectBurpExtension.jarファイルは、OpenText DASTがインストールされている場所のExtensionsディレクトリにあります。デフォルトの場所は次のいずれかです。

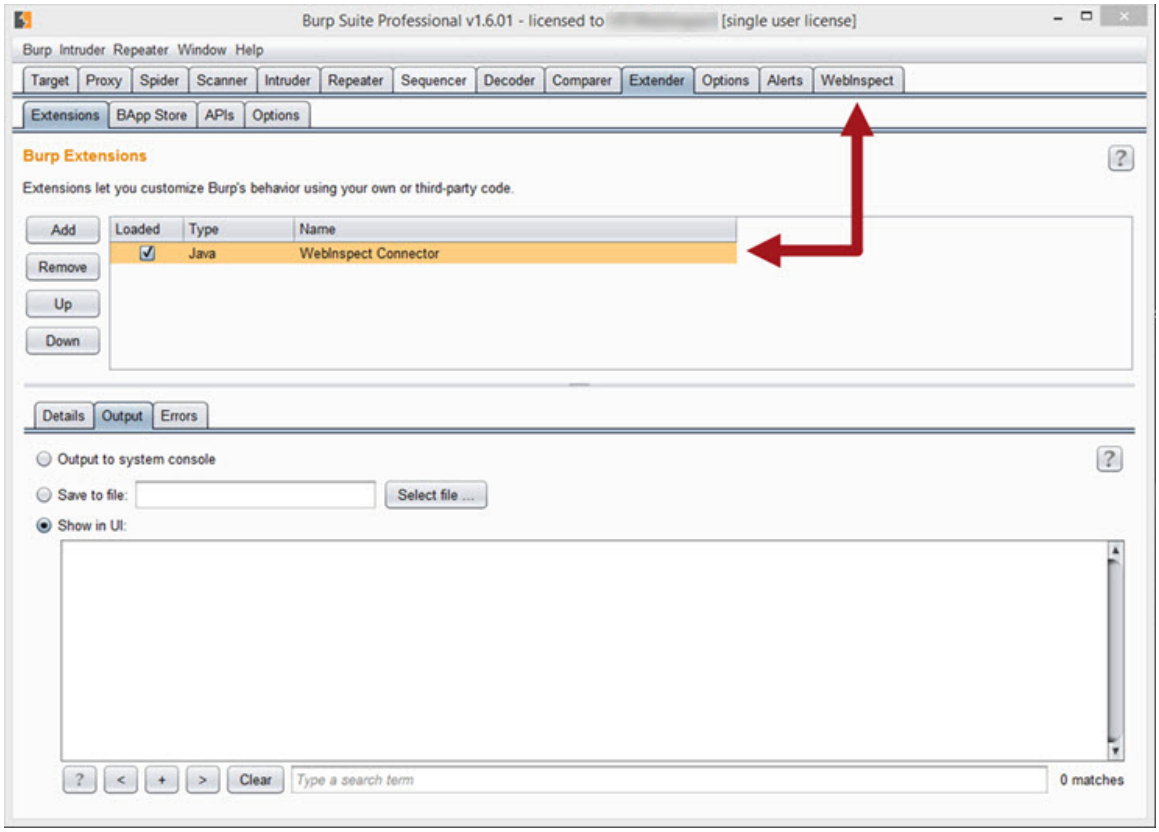
   C:\Program Files\Fortify\Fortify WebInspect\Extensions

   C:\Program Files (x86)\Fortify\Fortify WebInspect\Extensions

3. [標準出力(Standard Output)]セクションと [標準エラー(Standard Error)]セクションで、 [UIに表示(Show in UI)]オプションが選択されていることを確認します。
4. [次へ(Next)]をクリックします。

   WebInspect ConnectorがBurp拡張機能のリストに表示され、「WebInspect」というタブがBurpユーザインタフェースに追加されます。 [WebInspect]タブが表示されない場合は、

Burp拡張機能が正しくロードされていません。この場合は、[出力(Output)]タブと[エラー(Errors)]タブで、問題のトラブルシューティングに役立つ情報を確認してください。

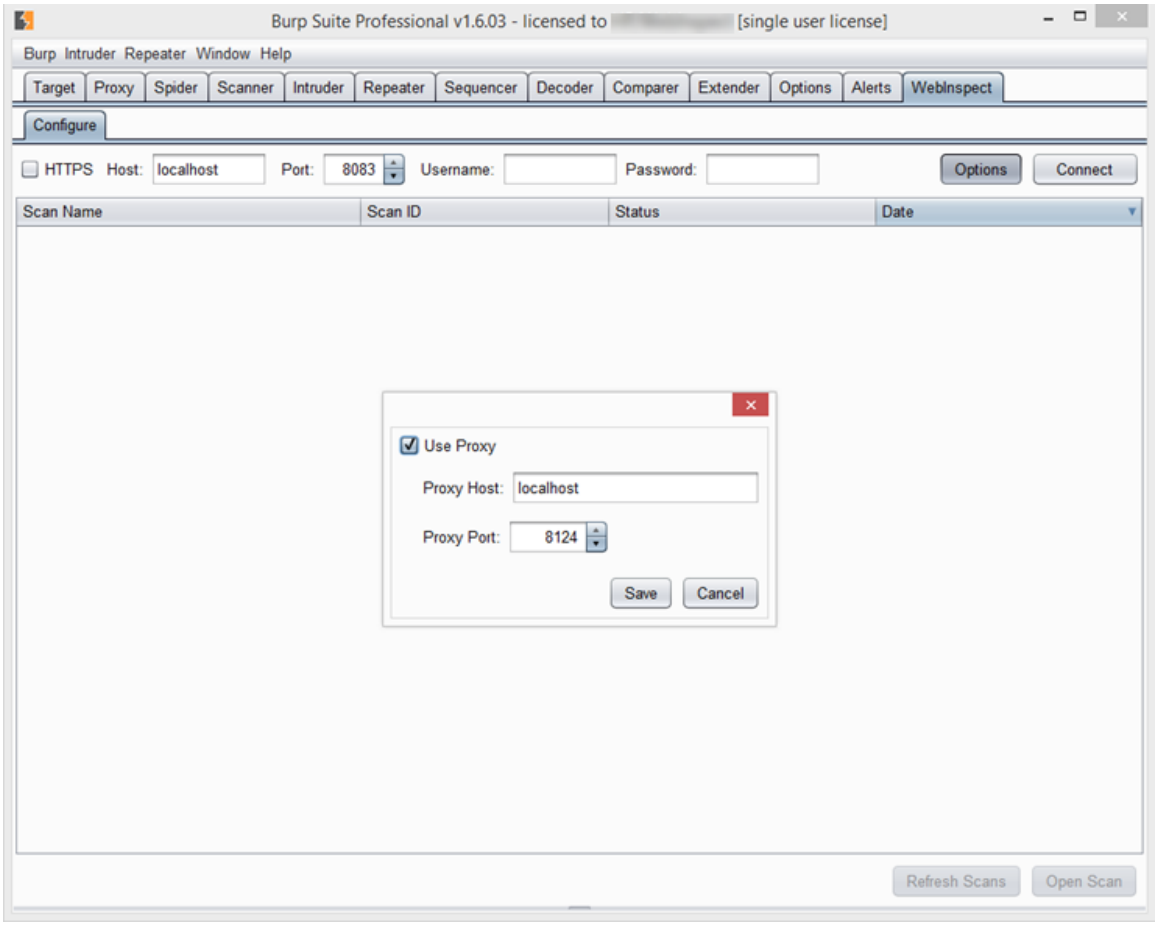


OpenText DASTへの接続

OpenText DASTに接続するには、Burpで次のステップを実行します。

1. OpenText DAST APIサービスが実行されていることを確認します。詳細については、「"OpenText DAST Monitor" ページ110」を参照してください。
2. **[WebInspect] > [設定(Configure)]**タブで次の操作を行います。
   a. APIでHTTPS認証が必要な場合は、**[HTTPS]**チェックボックスを**オン**にします。
   b. OpenText DAST APIサービスのホスト名を**[ホスト(Host)]**に、ポート番号を**[ポート(Port)]**に入力します。
   c. APIで認証が必須として設定されている場合は、**ユーザ名**と**パスワード**を入力します。
   d. **[オプション(Options)]**をクリックして、API HTTP要求のプロキシ設定を行います。

プロキシ設定ウィンドウが表示されます。

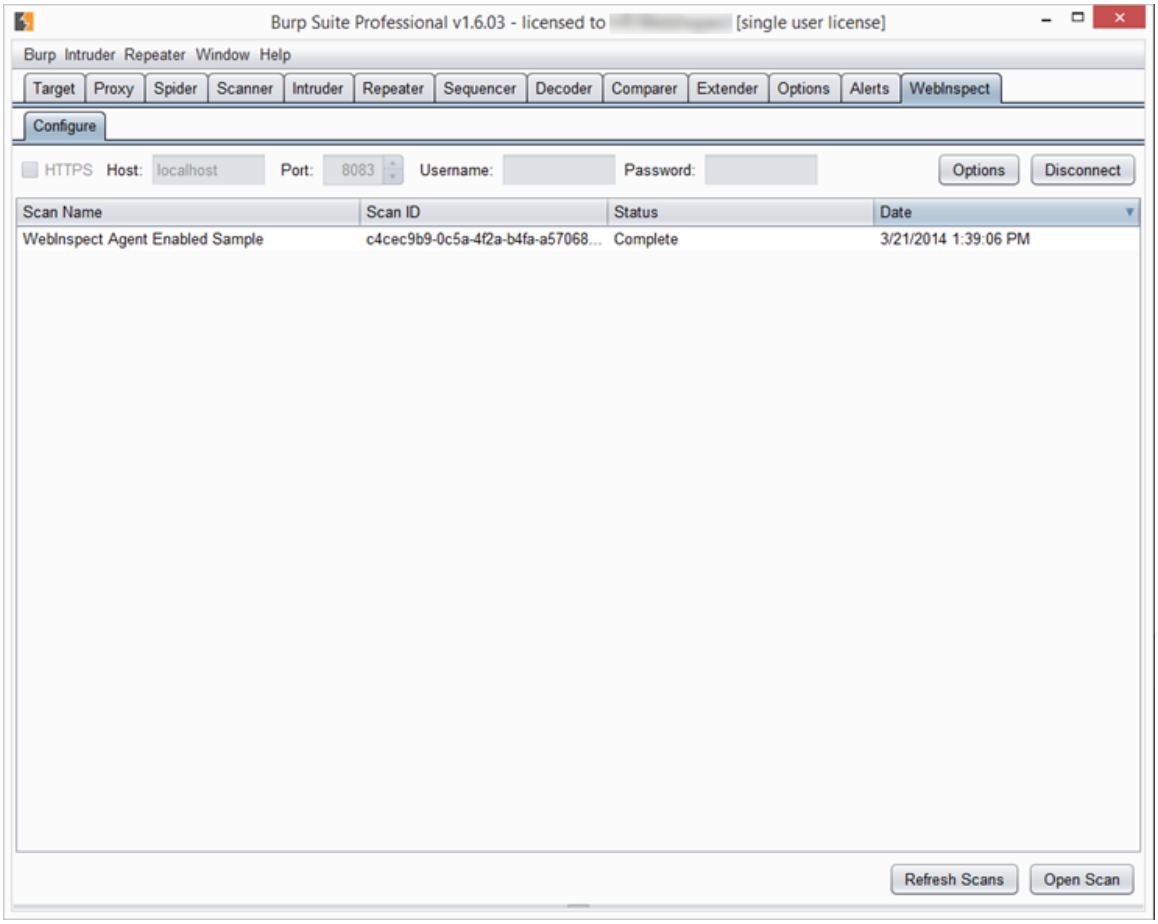


e. [**プロキシを使用する(Use Proxy)**]チェックボックスをオンにして、[**プロキシホスト(Proxy Host)**]に名前を入力し、[**プロキシポート(Proxy Port)**]に番号を入力します。

f. [**Save**]をクリックします。

3. [**接続(Connect)**]をクリックします。

[WebInspect]タブに、OpenText DASTスキャンのリストが表示されます。



スキャンのリストの更新

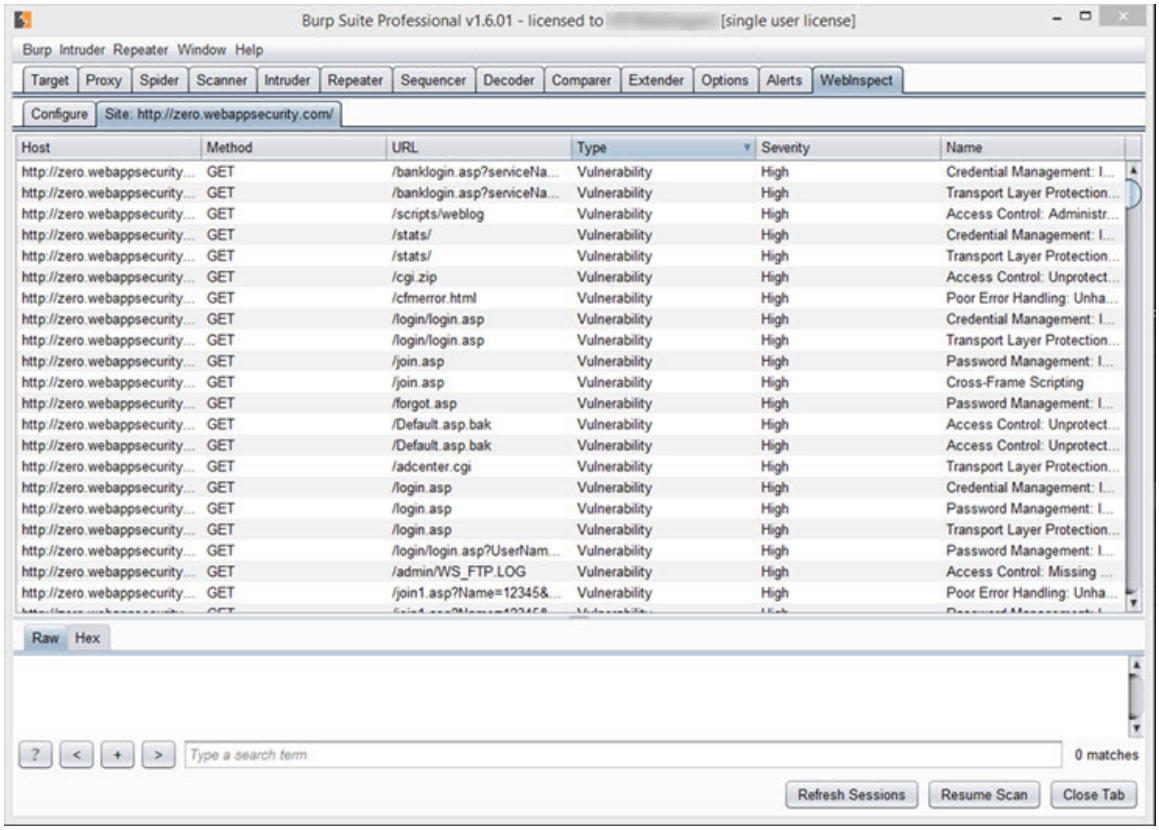
OpenText DASTスキャンのリストを更新するには、**[スキャンの更新(Refresh Scans)]**をクリックします。

Burpでのスキャンの操作

OpenText DASTスキャンを操作するには、Burpで次のステップを実行します。

1. 次のいずれかを実行してスキャンを開きます。
   - リスト内のスキャンをダブルクリックする。
   - リストからスキャンを選択し、**[スキャンを開く(Open Scan)]**をクリックする。

[WebInspect]タブの下の新しいタブでスキャンが開き、Web探索セッションと脆弱性セッションが一覧表示されます。セッションのリストは、タイプに基づいて脆弱性セッション、Web探索セッションの順に自動的にソートされます。



2. ソートされた列を逆の順序でソートするには、列ヘッダをクリックします。異なるソート基準を使用してリストをソートするには、ソート基準にする列のヘッダをクリックします。次の表で、いくつかのソートシナリオを説明します。

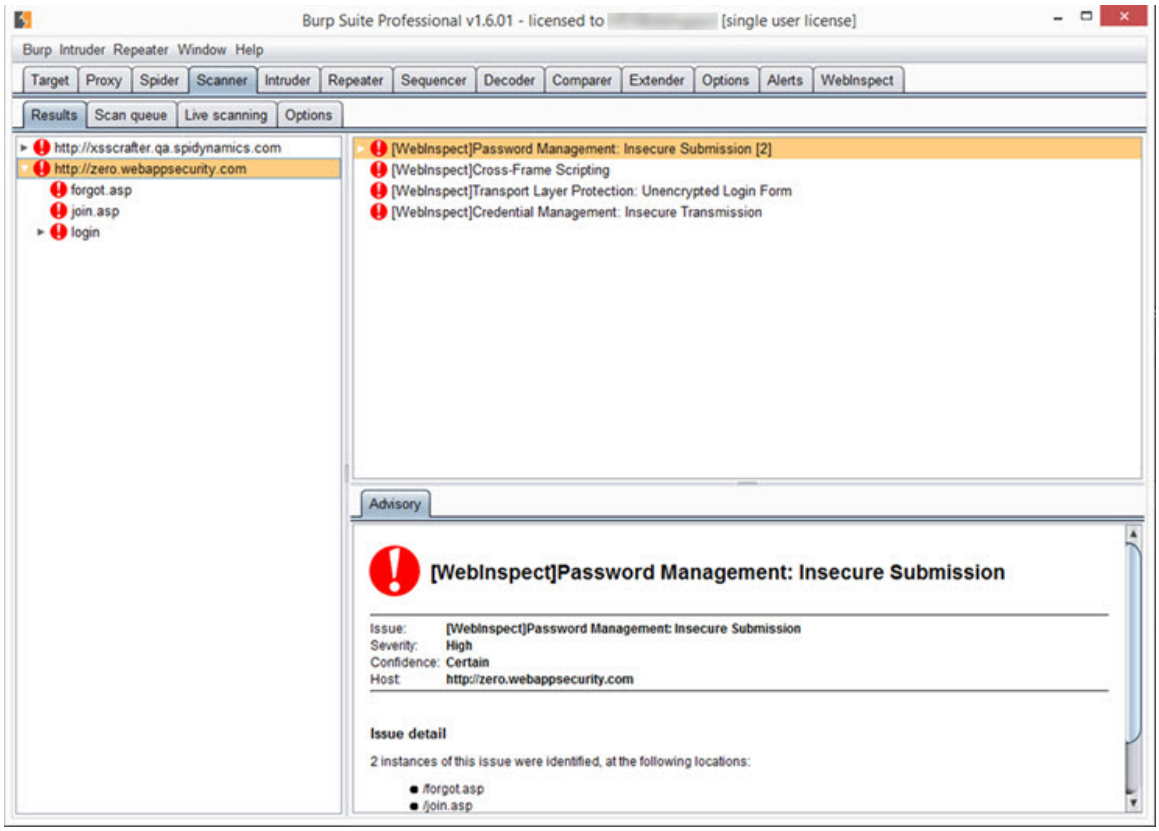
次の場合...	ソート基準...
スキャンに複数のホストが含まれており、セッションをホスト別にグループ化する場合	ホスト
特定のメソッドを使用しているすべてのセッションを表示する場合	メソッドでソートし、目的のメソッドまでスクロールする
Webサイト内の特定のページに影響するすべてのセッションを表示する場合	URLでソートし、目的のページまでスクロールする
重大度が[重大(Critical)]および[高(High)]のすべてのセッションを選択してBurpツールに送信する場合	重大度でソートし、重大度が[重大(Critical)]および[高(High)]のセッションまでスクロールする

次の場合...	ソート基準...
同じチェック名を持つすべてのセッションを選択する場合	名前でソートし、目的のチェック名までスクロールする

3. Burpがまだ実行中のスキャンに接続されている場合などにセッションのリストを更新するには、[セッションの更新(Refresh Sessions)]をクリックします。
4. セッションの要求を表示するには、リストでそのセッションをクリックします。
   セッション要求情報がウィンドウの下部に表示されます。要求をクリックすると、応答が表示されます。
5. 1つ以上のセッションをBurpツールに送信してさらに分析するには、セッションを選択し、右クリックして該当する[送信先(Send To)]オプションを選択します。

   注記: 現在のオプションは、[Spiderに送信(Send To Spider)]、[Intruderに送信(Send To Intruder)]、および[Repeaterに送信(Send To Repeater)]です。Burpツールの詳細については、Burp Suiteのマニュアルを参照してください。

6. 脆弱なセッションの問題を作成し、Burpの[スキャナ(Scanner)]タブに追加するには、セッションを右クリックして[問題の作成(Create Issue)]を選択します。
   この問題にはOpenText DASTのレポートデータが取り込まれ、問題名には[WebInspect]というタグが付いています。これは、外部リソースから問題が追加されたことを示します。



注記: [問題の作成(Create Issue)]オプションは、Burp Professional Editionでのみ使用可能であり、Web探索セッションでは使用できません。

7. 停止したスキャンを続行するには、 **[スキャンの再開(Resume Scan)]**をクリックします。
8. OpenText DASTスキャンを閉じるには、 **[タブを閉じる(Close Tab)]**をクリックします。

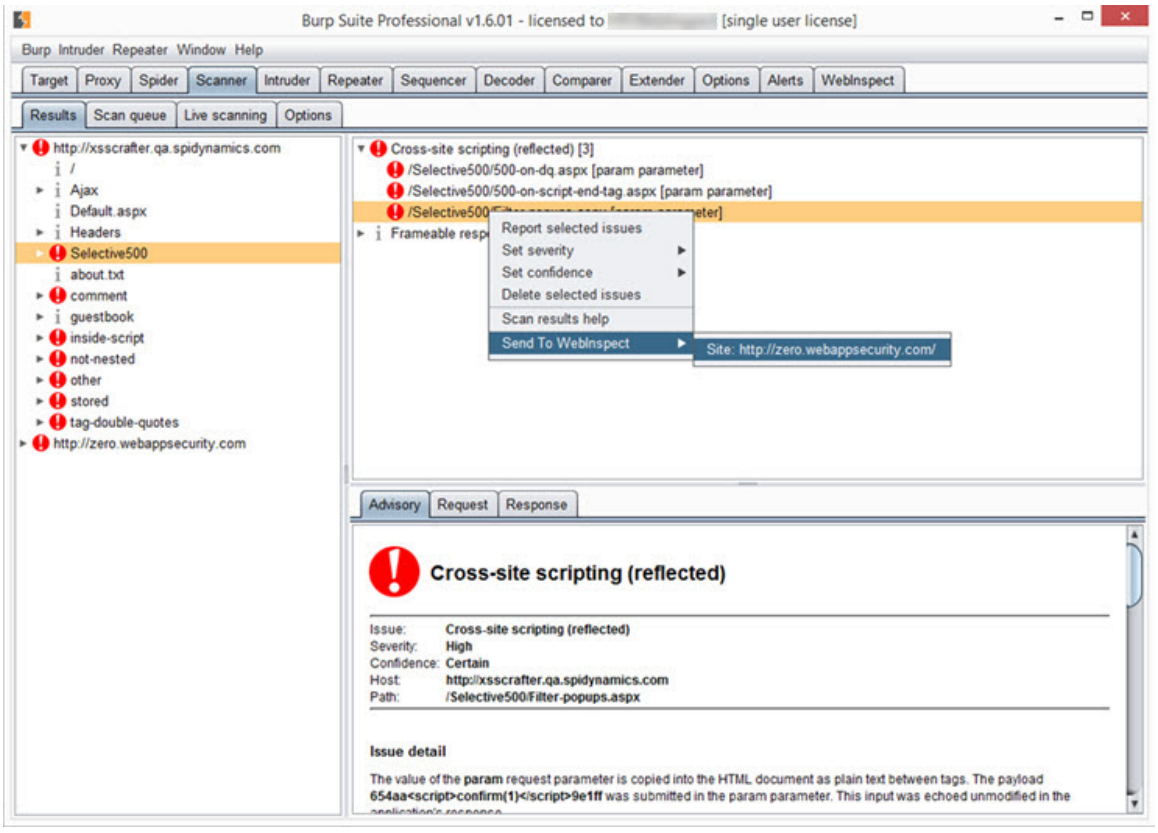
BurpからOpenText DASTへの項目の送信

Web探索対象の要求/応答および問題をOpenText DASTに送信するには、Burpで次のステップを実行します。

1. 目的のOpenText DASTスキャンが **[WebInspect]**タブで開いていることを確認します。

ヒント: BurpでOpenText DASTスキャンが開いていない場合、コンテキストメニューに[WebInspectに送信(Send to WebInspect)]オプションが表示されません。

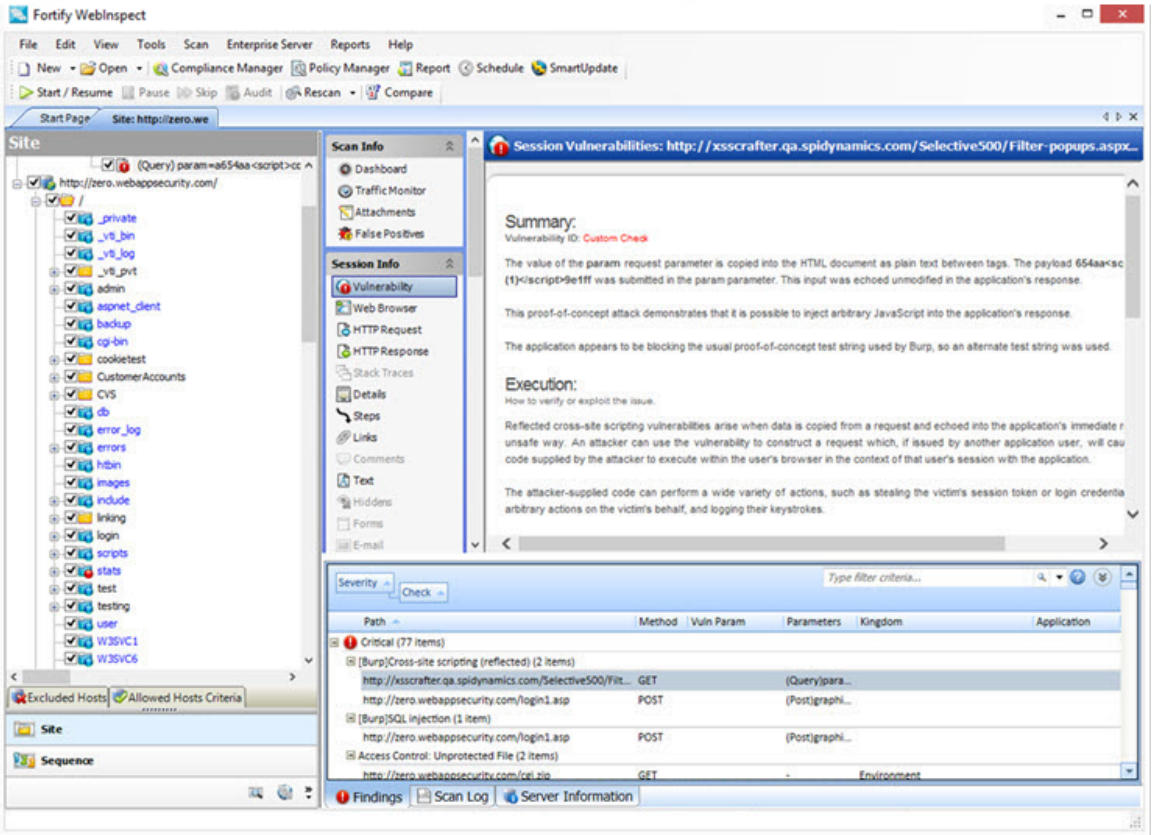
2. **[スキャナ(Scanner)]**タブをクリックしてから、 **[結果(Results)]**タブをクリックします。
3. Web探索対象の要求/応答をOpenText DASTに送信するには、その要求を右クリックして、 **[WebInspectに送信(Send To WebInspect)] > [スキャン名]**を選択します。



OpenText DASTにより、Web探索可能な要求のセッションが作成されます。[WebInspect]タブでスキャンに戻り、 **[スキャンの再開(Resume Scan)]**をクリックして、セッションをWeb探索します。

注記: 開いているスキャンのスキャン設定は、送信されるセッションに適用されます。これは、OpenText DASTがセッションで実行する内容に影響する場合があります。たとえば、開いているスキャンがホストA用で、ホストBからセッションを送信するが、開いているスキャンの [許可ホスト(Allowed Hosts)]リストにホストBが含まれていない場合、このセッションは除外され、Web探索は行われません。

4. OpenText DASTに問題を手動での検出事項として送信するには、問題を右クリックして、 **[WebInspectに送信(Send To WebInspect)] > [スキャン名]]**を選択します。
   この問題には、Burpのレポートデータが取り込まれ、問題名には [Burp]というタグが付いています。これは、外部リソースから問題が追加されたことを示します。



参照情報

"Burp API拡張機能について" ページ384

"OpenText DAST REST API" ページ357

"OpenText DAST Monitor" ページ110

WebInspect SDKについて

WebInspect Software Development Kit(SDK)はVisual Studio拡張機能であり、これを使うとソフトウェア開発者はセッション応答で特定の脆弱性をテストする監査拡張機能を作成で

きます。

注意! {/b}OpenTextは、Visual Studioを使用したコード開発の専門知識を持つ有資格のソフトウェア開発者のみがWebInspect SDKを使用することを推奨します。

監査拡張機能/カスタムエージェント

開発者は、WebInspect SDKをOpenText DASTコードへのエントリポイントとして使用できます。OpenText DASTが要求/応答ペアを作成すると、開発者は応答を調べて、脆弱性にフラグを付ける監査拡張機能を作成できます。作成が済むと、開発者は拡張機能をSecureBase (アダプティブエージェントと脆弱性チェックのOpenText DASTデータベース)のローカルコピーに送信し、そこでカスタムエージェントとして保存します。カスタムエージェントにはGUID (Globally Unique Identifier)が割り当てられ、OpenText DAST製品のPolicy Managerでポリシーに使用できるようになります。

注記: カスタムエージェントは、SecureBaseの更新によって上書きされません。

スキャン結果を検査するときには、カスタムエージェントによって検出された脆弱性に対して、標準チェックによって検出された脆弱性に対するアクションと同じアクション(URLのコピーや脆弱性の確認など)を実行できます。詳細については、「"結果の検査" ページ284」を参照してください。

SDKの機能

SDKは、開発者に次の機能を提供します。

- OpenText DAST Web探索プログラムと監査機能により生成されるセッションを検査する
- パラメータに値を挿入する(パラメータおよびサブパラメータのファジング)
- URLをWeb探索のためにキューに登録する(OpenText DAST Web探索プログラムがWeb探索できるようにするため)
- 脆弱性にフラグを付ける
- OpenText DASTリクエスタから生のHTTP要求を送信する
- ParseLibによる要求と応答の解析
- イベントとエラーをログに記録する

インストールの推奨事項

WebInspect SDKは、OpenText DAST製品と同じマシンにインストールする必要はありません。ほとんどの場合、ソフトウェア開発者の開発マシンにインストールされます。ただし、デバッグが必要な新しい拡張機能を開発している場合、OpenTextは拡張機能を作成する開発マシンにOpenText DASTをインストールすることをお勧めします。これにより、拡張機能をローカルでテストできます。デバッグを必要としない既存の拡張機能の場合は、OpenText DASTをローカルにインストールする必要はありません。

WebInspect SDKのインストールと使用に関する最小要件については、『*OpenText™ Application Securityソフトウェアのシステム要件*』ドキュメントを参照してください。

WebInspect SDKのインストール

WebInspect SDKを使用するには、開発者がWebInspectSDK.vsixという名前のVisual Studio拡張機能ファイルをインストールする必要があります。

OpenText DASTのインストール中に、WebInspectSDK.vsixファイルのコピーがOpenText DASTのインストール場所のExtensionsディレクトリにインストールされます。デフォルトの場所は次のいずれかです。

- C:\Program Files\Fortify\Fortify WebInspect\Extensions
- C:\Program Files (x86)\Fortify\Fortify WebInspect\Extensions

開発者のマシンでOpenText DASTがインストールされている場所にローカルコピーをインストールするには:

1. **Extensions**フォルダに移動し、**WebInspectSDK.vsix**ファイルをダブルクリックします。
   VSIXインストーラが起動します。
2. プロンプトが表示されたら、拡張機能をインストールするVisual Studio製品を選択し、**[インストール(Install)]**をクリックします。
   WebInspect Audit Extensionプロジェクトテンプレートが Visual Studioで作成されます。"インストールの検証" 下の手順に従います。

開発者のマシンでOpenText DASTがインストールされていない場所にローカルコピーをインストールするには:

1. **Extensions**フォルダに移動し、**WebInspectSDK.vsix**ファイルをUSBドライブなどのポータブルメディアにコピーします。
2. Visual Studio 2013や、関連する必須ソフトウェアおよびハードウェアがインストールされている開発マシンにドライブを挿入します。
3. USBドライブに移動し、**WebInspectSDK.vsix**ファイルをダブルクリックします。
   VSIXインストーラが起動します。
4. プロンプトが表示されたら、拡張機能をインストールするVisual Studio製品を選択し、**[インストール(Install)]**をクリックします。
   WebInspect Audit Extensionプロジェクトテンプレートが Visual Studioで作成されます。"インストールの検証" 下の手順に従います。

インストールの検証

拡張機能が正常にインストールされていることを検証するには:

1. Visual Studioで **[ツール] > [拡張機能と更新プログラム]**を選択します。
2. 拡張機能のリストを下に向かってスクロールします。

リストに [WebInspect SDK] が表示されていれば、拡張機能は正常にインストールされています。

インストール後

WebInspect SDKをインストールして設定した後、開発者はVisual Studioで新しいWebInspect Audit Extensionプロジェクトを作成できます。このプロジェクトでは、開発者は監査拡張機能を作成し、その拡張機能をデバッグおよびテストし、カスタムエージェントとしてSecureBaseに発行します。WebInspect Audit Extensionプロジェクトテンプレートの使用法については、Visual StudioのWebInspect SDKのドキュメントを参照してください。

開発者がカスタムエージェントをSecureBaseに送信した後、このエージェントをPolicy Managerのポリシーで選択できるようになります。詳細については、Policy Managerのドキュメントを参照してください。

ページまたはディレクトリを追加する

OpenText DASTでは検出されなかったリソースを検出するために手動検査またはその他のセキュリティ分析ツールを使用する場合、これらの場所を手動で追加して脆弱性を割り当てることができます。データをOpenText DASTスキャンに組み込むことで、OpenText DAST機能を使用して脆弱性を報告および追跡することができます。

注記: データ階層に何かを追加する場合は、論理的な順序に従って手動でリソースを追加する必要があります。たとえば、サブディレクトリとページを作成するには、サブディレクトリを作成してからページを作成する必要があります。

1. ページまたはディレクトリのデフォルト名を、追加するリソースの名前に置き換えます。
2. 必要に応じて、HTTP要求と応答を編集します。要求パスは変更しないでください。
3. リソースに要求を送信し、応答をセッションデータに記録できます。これにより、OpenText DASTによって検出されなかったリソースの存在も検証されます。
   a. [HTTP Editor] をクリックして、HTTP Editorを開きます。
   b. 必要に応じて、要求を変更します。
   c. 

をクリックします。
   d. HTTP Editorを閉じます。
   e. 変更した要求と応答の使用を求めるプロンプトが表示されたら、 [はい(Yes)] を選択します。
4. (オプション)すべての要求と応答の変更を削除するには、 [リセット(Reset)] をクリックします。
5. 終了したら、 [OK] をクリックします。

バリエーションを追加する

OpenText DASTでは検出されなかったリソースを検出するために手動検査またはその他のセキュリティ分析ツールを使用する場合、これらの場所を手動で追加して脆弱性を割り当てることができます。データをOpenText DASTスキャンに組み込むことで、OpenText DAST機能を使用して脆弱性を報告および追跡することができます。

バリエーションとはある場所のサブノードであり、その場所の特定の属性を一覧にしたものです。たとえば、場所login.aspには次のバリエーションがあるかもしれません。

(Post) uid=12345&Password=foo&Submit=Login

他の場所と同様に、バリエーションには脆弱性とサブノードが付加されている場合もあります。

1. [**名前(Name)**]ボックスで、デフォルトの「attribute=value」を、送信する実際のパラメータに置き換えます(uid=9999&Password=kungfoo&Submit=Loginなど)。
2. [**ポスト(Post)**]または[**クエリ(Query)**]を選択します。
3. 必要に応じて、HTTP要求と応答を編集します。要求パスは変更しないでください。
4. リソースに要求を送信し、応答をセッションデータに記録できます。これにより、OpenText DASTによって検出されなかったリソースの存在も検証されます。
   a. [**HTTP Editor**]をクリックして、HTTP Editorを開きます。
   b. 必要に応じて、要求を変更します。
   c. 

をクリックします。
   d. HTTP Editorを閉じます。
   e. 変更した要求と応答の使用を求めるプロンプトが表示されたら、[**はい(Yes)**]を選択します。
5. (オプション)すべての要求と応答の変更を削除するには、[**リセット(Reset)**]をクリックします。
6. 終了したら、[**OK**]をクリックします。

OpenText DAST Monitor: Enterprise Serverセンサの設定

この設定情報は、OpenText DASTをセンサとしてFortify WebInspect Enterpriseに統合するために使用されます。情報を入力してセンササービスを開始したら、OpenText DASTグラフィカルユーザインタフェースではなく、Fortify WebInspect Enterprise Webコンソールを使用してスキャンを実行する必要があります。

センサ設定項目の説明を次の表に示します。

項目	説明
マネージャURL (Manager URL)	Enterprise Server ManagerのURLまたはIPアドレスを入力します。
センサ認証 (Sensor Authentication)	ユーザ名(ドメイン\ユーザ名の形式)とパスワードを入力してから、 **テスト(Test)**]をクリックしてエントリを検証します。
プロキシの有効化 (Enable Proxy)	OpenText DASTがプロキシサーバを経由して、Enterprise Server Managerにアクセスする必要がある場合は、 **プロキシの有効化 (Enable Proxy)**]を選択してから、サーバのIPアドレスとポート番号を入力します。認証が必要な場合は、有効なユーザ名とパスワードを入力します。
データベース設定の上書き (Override Database Settings)	通常、OpenText DASTは、スキャンデータを"アプリケーション設定:データベース" ページ484で指定するデバイスに保存します。ただし、OpenText DASTがセンサとしてFortify WebInspect Enterpriseに接続されている場合は、このオプションを選択してから、 **設定 (Configure)**]をクリックして代替デバイスを指定できます。
サービスアカウント (Service Account)	センササービスには、LocalSystemアカウントまたは指定したアカウントを使用してログオンできます。
センサステータス (Sensor Status)	このエリアにはセンササービスの現在のステータスが表示され、サービスを開始または停止するためのボタンが表示されます。

センサとして設定後

OpenText DASTをセンサとして設定したら、 **開始(Start)**]をクリックします。

ブラックアウト期間

OpenText DASTがFortify WebInspect Enterpriseに接続されている場合は、ユーザがブラックアウト期間中にスキャンを試みる可能性があります。これは、スキャンが企業管理者によって許可されない一定の時間です。この問題が発生した場合は、次のエラーメッセージが表示されます。

「開始URLが次のブラックアウト期間に入っているためスキャンを開始できません...(Cannot start Scanner because the start URL is under the following blackout period(s)...)」

スキャンを実行するには、ブラックアウト期間が終了するまで待つ必要があります。

同様に、ブラックアウト期間が始まったときにスキャンが実行されていた場合、企業管理者はスキャンを一時停止して、保留中のジョブキューに登録し、ブラックアウト期間が終了したらスキャンを完了します。複数のIPアドレスに対してブラックアウトが定義されている場合、企業管理者は、指定されたIPアドレスの1つからスキャンが開始された場合にのみスキャンを一時停止します。除外されていないIPアドレスでスキャンが開始されるものの、その後、IPアドレスがブラックアウト設定で指定されたホストへのリンクをたどる場合、スキャンは一時停止されません。

除外の作成

除外/拒否基準を追加するには:

1. **[追加(Add)]**(**[その他の除外/拒否基準(Other Exclusion/Rejection Criteria)]**リストの右側にある)をクリックします。

   [除外の作成(Create Exclusion)]ウィンドウが開きます。
2. **[ターゲット(Target)]**リストから項目を選択します。
3. ターゲットとして[クエリパラメータ(Query Parameter)]、[ポストパラメータ(Post Parameter)]、または[応答ヘッダ(Response Header)]を選択した場合は、**[ターゲット名(Target Name)]**を入力します。
4. **[一致タイプ(Match Type)]**リストから、ターゲット内のテキストの一致に使用される方法を選択します。
   - [正規表現に一致(Matches Regex)] - **[一致文字列(Match String)]**ボックスで指定した正規表現に一致します。
   - [正規表現の拡張に一致(Matches Regex Extension)] - **[一致文字列(Match String)]**ボックスで指定したOpenText正規表現の拡張から入手可能な構文に一致します。詳細については、「"正規表現の拡張" ページ356」を参照してください。
   - [一致(Matches)] - **[一致文字列(Match String)]**ボックスで指定したテキスト文字列に一致します。
   - [含む(Contains)] - **[一致文字列(Match String)]**ボックスで指定したテキスト文字列を含みます。
5. **[一致文字列(Match String)]**ボックスに、ターゲットで検索する文字列または正規表現を入力します。または、**[一致タイプ(Match Type)]**で正規表現オプションを選択した場合は、ドロップダウン矢印をクリックして、**[正規表現の作成(Create Regex)]**を選択し、Regular Expression Editorを起動します。
6.  をクリックします。
7. (オプション)ステップ2-6を繰り返して、条件を追加します。複数の一致は、AND条件として扱われます。
8. [現在の設定(Current Settings)]で作業している場合は、**[テスト(Test)]**をクリックして現在のスキャンの除外を処理できます。基準によって絞り込まれたそのスキャンからのセッションがテスト画面に表示され、必要に応じて設定を変更できます。
9. [OK]をクリックします。

10. **[その他の除外/拒否基準(Other Exclusion/Rejection Criteria)]**リストに除外が表示されている場合は、**[拒否(Reject)]**と**[除外(Exclude)]**のいずれかまたは両方を選択します。

注記: スキャン中は、応答タイプ、応答ヘッダタイプ、およびステータスコードターゲットタイプを拒否することができません。これらのターゲットタイプは除外することしかできません。

例1

Microsoft.comのリソースに対する要求を無視して送信しないようにするには、次の除外を入力して、**[拒否(Reject)]**を選択します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	contains	Microsoft.com

例2

一致文字列として「logout」と入力します。この文字列がURLの任意の部分で見つかった場合は、そのURLが除外または拒否されます(選択されたオプションによって異なる)。「logout」の例を使用すると、OpenText DASTは、loutout.aspやapplogout.jspなどのURLを除外または拒否します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	contains	logout

例3

次の例では、クエリパラメータ「username」が「John」と等しいクエリを含むセッションを拒否または除外します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
クエリパラメータ(Query parameter)	username	一致(matches)	John

例4

次の例では、次のディレクトリを除外または拒否します。

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	正規表現に一致(matches regex)	/W3SVC[0-9]*/

Internet Protocolバージョン6

OpenText DASTでは、Webサイトスキャンおよびウェブサービススキャンでは IPv6 (Internet Protocolバージョン6)アドレスがサポートされています。開始URLを指定する場合は、IPv6アドレスを括弧で囲む必要があります。例:

- http://[::1]
  OpenText DASTは「localhost」をスキャンします。
- http://[fe80::20c:29ff:fe32:bae1]??/subfolder/??
  OpenText DASTは、指定されたアドレスのホストのスキャンを「subfolder」ディレクトリから開始します。
- http://[fe80::20c:29ff:fe32:bae1]??:8080/subfolder/??
  OpenText DASTは、ポート8080で実行されているサーバのスキャンを「subfolder」から開始します。

第6章:デフォルトのスキャン設定

この章では、デフォルトのスキャン設定について説明します。デフォルト設定を使用して、スキャンアクションのスキャンパラメータを設定します。OpenText DASTは、スキャンの開始中に代わりのオプションを指定(スキャンウィザードから、または [現在の設定(Current Settings)]にアクセスして使用可能なオプションを使用する)しない限り、これらを使用します。

参照情報

"Web探索設定" ページ456

"監査設定" ページ469

スキャン設定:方法

この機能にアクセスするには、 **[編集(Edit)]**メニューをクリックし、 **[デフォルトのスキャン設定(Default Scan Settings)]**または **[現在のスキャン設定(Current Scan Settings)]**を選択します。その後で、 **[スキャン設定(Scan Settings)]**カテゴリで、 **[方法(Method)]**を選択します。

スキャンモード(Scan mode)

[スキャンモード(Scan Mode)]オプションについて、次の表で説明します。

オプション	説明
Web探索のみ(Crawl Only)	このオプションは、サイトのツリー構造を完全にマッピングします。Web探索が完了したら、 **[監査(Audit)]**をクリックしてアプリケーションの脆弱性を評価できます。
Web探索および監査(Crawl and Audit)	OpenText DASTは、サイトの階層データ構造をマッピングし、各リソース(ページ)が検出されるたびにそれを監査します(サイト全体をWeb探索してから監査を実行するのではなく)。このオプションは、Web探索が完了する前にコンテンツが変更される可能性がある非常に大規模なサイトで最も有用です。これについては、 [デフォルト設定(Default Settings)]の [Web探索および監査モード(Crawl and Audit Mode)]の [同時(Simultaneously)]というオプションで説明しています。詳細については、「"Web探索および監査モード(Crawl and audit mode)" 次のページ」を参照してください。
監査のみ(Audit Only)	OpenText DASTは、選択されたポリシーの手法を適用して脆弱性リスクを判断しますが、WebサイトのWeb探索は行いません。サイト

オプション	説明
	上のリンクをたどることも評価することもありません。
手動 (ガイド付きスキャンでは使用できません)	手動モードでは、アクセス先として選んだのがアプリケーションのどのセクションであれ、そこに手動で移動できます。サイト全体のWeb探索は実行されず、サイト内を手動で移動中に検出したリソースに関する情報のみを記録します。この機能は、Webフォームのログオンページからサイトに入る場合、または調査するアプリケーションの個別のサブセットまたは部分を定義する場合に最もよく使用されます。サイト内を移動し終わったら、結果を監査して、記録したサイトのその部分に関連するセキュリティ脆弱性を評価できます。

Web探索および監査モード(Crawl and audit mode)

[Web探索および監査モード(Crawl and Audit Mode)]オプションについて、次の表で説明します。

オプション	説明
同時(Simultaneously)	OpenText DASTは、サイトの階層データ構造をマッピングし、各リソース(ページ)が検出されるたびにそれを監査します(サイト全体をWeb探索してから監査を実行するのではなく)。このオプションは、Web探索が完了する前にコンテンツが変更される可能性がある非常に大規模なサイトで最も有用です。
順次(Sequentially)	このモードでは、OpenText DASTはサイト全体をWeb探索し、サイトの階層データ構造をマッピングして、サイトのルートから順次監査を実行します。

Web探索および監査の詳細(Crawl and audit details)

[Web探索および監査の詳細(Crawl and Audit Details)]オプションについて、次の表で説明します。

オプション	説明
検索プローブを含める(検索攻撃を送信する)(Include search probes (send search attacks))	このオプションを選択すると、OpenText DASTは、サーバ上に存在する場合も存在しない場合もあるファイルやディレクトリに対する要求を、それらのファイルがサイトのWeb探索で検出されない場合でも送信します。 このオプションは、スキャンモードが [Web探索および監査(Crawl &

オプション	説明
	Audit)]に設定されている場合にのみデフォルトで選択されます。スキャンモードが「Web探索のみ(Crawl Only)]または「監査のみ(Audit Only)]に設定されている場合、このオプションはデフォルトでクリア(オフ)されます。
「ファイルが見つからない」応答でのリンクのWeb探索(Crawl links on File Not Found responses)	このオプションを選択すると、OpenText DASTは「ファイルが見つからない」とマークされた応答のリンクを検索し、Web探索を行います。 このオプションは、スキャンモードが「Web探索のみ(Crawl Only)]または「Web探索および監査(Crawl & Audit)]に設定されている場合はデフォルトで選択されます。このオプションは、スキャンモードが「監査のみ(Audit Only)]に設定されている場合は利用できません。

ナビゲーション

「ナビゲーション(Navigation)]オプションについて、次の表で説明します。

オプション	説明
Web探索時のWebフォームの自動入力(Auto-fill Web forms during crawl)	このオプションを選択すると、OpenText DASTは、すべてのフォームで検出された入力コントロールの値を送信します。値は、Web Form Editorを使用して作成したファイルから抽出されます。参照ボタンを使用して、使用する値を含むファイルを指定します。または、「**編集(Edit)**]ボタン(現在選択されているファイルを変更する場合)または「**作成(Create)**]ボタン(Webフォームファイルを作成する場合)を選択することもできます。 注意! {/b}この機能を認証に使用しないでください。Web探索プログラムと監査プログラムが状態を共有するように設定されている場合、およびOpenText DASTがサイトから誤ってログアウトすることがない場合は、Web Form Editorによって抽出された値をログインフォームに使用できるはずです。ただし、最初のログインの後に監査またはWeb探索によってログアウトがトリガされた場合は、OpenText DASTは再ログインできず、監査は認証されなくなります。OpenText DASTが誤ってアプリケーションからログアウトした場合に途中で終了するのを防ぐには、「スキャン設定(Scan Settings)]-「認証(Authentication)]に移動し、「**フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)**]を選択します。

オプション	説明
Webフォーム値の入力を要求する(Prompt for Web form values)	このオプションを選択すると、OpenText DASTは、HTTPフォームまたはJavaScriptフォームを検出した際にスキャンを一時停止し、フォーム内の入力コントロールの値を入力できるウィンドウを表示します。しかし、 **[タグ付けされた入力に対してのみプロンプトを表示する(Only prompt for tagged inputs)]**も選択した場合、OpenText DASTはユーザ入力用に一時停止しません。ただし、(Web Form Editorを使用して)特定の入力コントロールが **[対話型入力としてマーク(Mark as Interactive Input)]**と指定されている場合は例外です。入力するためのこの一時停止は「対話型モード」と呼ばれ、スキャン中にいつでもキャンセルできます。 対話型スキャンの設定の詳細については、"対話型スキャン" ページ224を参照してください。
Webサービス設計を使用する(Use Web Service Design)	このオプションは、Webサービススキャンにのみ適用されます。 Webサービススキャンを実行するときに、OpenText DASTはWSDLサイトをWeb探索し、操作ごとに各パラメータの値を送信します。これらの値は、Web Service Test Designerツールを使用して作成したファイルに含まれています。次に、OpenText DASTは、SQLインジェクションなどの脆弱性を検出するために各パラメータを攻撃して、サイトを監査します。 参照ボタンを使用して、使用する値を含むファイルを指定します。または、 **[編集]**ボタン  (現在選択されているファイルを変更する場合)または **[作成(Create)]**ボタン  (SOAP値ファイルを作成する場合)を選択することもできます。

SSL/TLSプロトコル(SSL/TLS protocols)

SSL (Secure Sockets Layer)およびTLS (Transport Layer Security)プロトコルは、WebブラウザとWebサーバ間のインターネットトランザクションに対してセキュアなHTTP (HTTPS)接続を提供します。SSL/TLSプロトコルは、Webアプリケーションのサーバ認証、クライアント認証、データ暗号化、およびデータ整合性を有効にします。

注記: **[アプリケーション設定(Application Settings)]**で **[OpenSSLエンジンを使用する(Use OpenSSL Engine)]**が選択されている場合、 **[SSL/TLSプロトコル(SSL/TLS Protocols)]**オプションは無効化されます。個々のプロトコルを選択することはできません。詳細については、「"アプリケーション設定:全般" ページ480」を参照してください。

Webサーバが使用するSSL/TLSプロトコルを選択します。次のオプションを指定できます。

- SSL 2.0を使用(Use SSL 2.0)
- SSL 3.0を使用(Use SSL 3.0)
- TLS 1.0を使用(Use TLS 1.0)
- TLS 1.1を使用(Use TLS 1.2)
- TLS 1.2を使用(Use TLS 1.2)

Webサーバに対応するSSL/TLSプロトコルを設定していない場合でも、OpenText DASTは引き続きサイトに接続しますが、パフォーマンスへの影響が生じる場合があります。

たとえば、OpenText DASTの設定がSSL 3.0のみを使用するように設定されているのに対し、WebサーバがTLS 1.2接続のみを受け入れるように設定されている場合、OpenText DASTはまずSSL 3.0との接続を試みますが、失敗します。その後、OpenText DASTは、TLS 1.2がサポートされていることを検出するまで、各プロトコルを実装します。接続は成功しますが、この作業にはより多くの時間がかかります。OpenText DASTで正しい設定([TLS 1.2を使用(Use TLS 1.2)])を行っていれば、最初の試みで成功したはずです。

スキャン設定:全般

この機能にアクセスするには、**[編集(Edit)]**メニューをクリックし、**[デフォルトのスキャン設定(Default Scan Settings)]**または**[現在のスキャン設定(Current Scan Settings)]**を選択します。その後で、**[スキャン設定(Scan Settings)]**カテゴリで、**[全般(General)]**を選択します。

スキャンの詳細(Scan details)

[スキャンの詳細(Scan Details)]オプションについて、次の表で説明します。

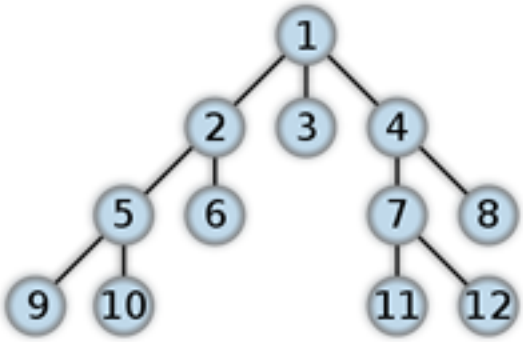
オプション	説明
パス切り捨てを有効にする(Enable Path Truncation)	パスの切り捨て攻撃は、ファイル名がない既知のディレクトリを求める要求です。これにより、ディレクトリー覧が表示される場合があります。OpenText DASTはパスの切り捨てを実行し、その際にディレクトリの一覧が表示されたり、異常なエラーが発生したりしないかを確認します。 **例:** リンクがhttp://www.site.com/folder1/folder2/file.aspで構成されている場合、パスを切り捨てて、http://www.site.com/folder1/folder2/とhttp://www.site.com/folder1/を探すと、サーバでディレクトリの内容が表示されたり、未処理の例外が発生したりする場合があります。

オプション	説明
大文字と小文字を区別する要求と応答の処理(Case-sensitive request and response handling)	ターゲットサイトのサーバでURLの大文字と小文字が区別される場合は、このオプションを選択します。
相関データの再計算(Recalculate correlation data)	このオプションは、スキャンを比較する場合にのみ使用されます。この設定の変更は、カスタマサポート担当者からのアドバイスがある場合にのみ行ってください。
応答データの圧縮(Compress response data)	このオプションを選択すると、OpenText DASTでは、各HTTP応答を圧縮形式でデータベースに保存してディスク容量を節約します。
Traffic Monitorのログを有効にする(Enable Traffic Monitor Logging)	基本スキャンの実行中、OpenText DASTでは、Webサイトの階層構造を示すセッションと脆弱性が検出されたセッションのみをナビゲーションペインに表示します。ただし、[Traffic Monitor]オプションを選択した場合、OpenText DASTは[**Traffic Monitor**]ボタンを[スキャン情報(Scan Info)]パネルに追加し、OpenText DASTによって送信されたすべての単一のHTTP要求と、サーバから受信した関連するHTTP応答を表示および確認できるようにします。
Traffic Monitorファイルの暗号化(Encrypt Traffic Monitor File)	通常、すべてのセッションは、Traffic Monitorファイルに平文として記録されます。パスワードなどの機密情報をコンピュータに保存することに不安を感じる場合は、ファイルの暗号化を選択できます。 暗号化されたファイルは圧縮できません。このオプションを選択すると、ログファイルの入ったエクスポートされたスキャンのサイズが大幅に増加します。 **注記:** Traffic Viewerツールは、トラフィックファイルの暗号化をサポートしていません。[**Traffic Monitorファイルの暗号化(Encrypt Traffic Monitor File)**]オプションは、レガシトラフィックファイルがある特別な状況でのみ使用するために予約されています。
Web探索と監査の最大再帰深度(Maximum crawl-audit recursion depth)	攻撃によって脆弱性が明らかになった場合、OpenText DASTは、そのセッションをWeb探索し、表示されるすべてのリンクをたどります。そのWeb探索と監査によってさらに別のリソースへのリンクが示された場合、深さのレベルがインクリメントされ、検出されたリソースがWeb探索および監査されます。このプロセスは、他のリンクが見つ

オプション	説明
	からなくなるまで繰り返し実行できます。ただし、無限ループに入ることがないように、再帰回数を制限できます。デフォルト値は2です。最大再帰レベルは1,000です。

Web探索の詳細

デフォルトでは、OpenText DASTは、ルートノードから始まり、すべての隣接ノード(1レベル下)を探索する幅優先(breadth-first) Web探索を使用します。その後、それらの最も近いノードごとに、未探索の隣接ノードが探索され、すべてのリソースが特定されるまで順に探索されます。次の図は、リンクされたページが幅優先Web探索を使用してアクセスされる順序を示しています。ノード1には、ノード2、3、および4へのリンクがあります。ノード2には、ノード5および6へのリンクがあります。



ユーザインタフェースでは、このWeb探索方法を変更できません。ただし、設定可能な[Web探索の詳細(Crawl Details)]オプションについて、次の表で説明します。

オプション	説明
キーワード検索監査を有効にする(Enable keyword search audit)	キーワード検索は、その名前が示すように、サーバの応答を調べて、たいていの場合に脆弱性を示す特定のテキスト文字列を検索する攻撃エンジンを使用します。通常、このエンジンは、Web探索のみのスキャンでは使用されませんが、このオプションを選択して有効にできます。
冗長ページ検出の実行(Perform redundant page detection)	非常にダイナミックなサイトでは、事実上同一の無限の数のリソース(ページ)が作成される可能性があります。各リソースの追跡を許可されると、OpenText DASTはスキャンを完了できなくなります。このオプションはページ構造を比較して類似性のレベルを判断し、OpenText DASTが冗長リソースの処理を識別して除外できるようにします。 重要! {/b}冗長ページ検出は、スキャンのWeb探索部分で機

オプション	説明
	能します。監査の対象となるセッションが冗長になる場合、そのセッションがスキャンから除外されることはありません。 冗長ページ検出では、次の設定を行えます。 • **ページ類似性のしきい値(Page Similarity Threshold)** - 2つのページが冗長と見なされるのに必要な類似度を示します。1から100のパーセンテージを入力します。100は完全一致です。デフォルト設定は95%です。 • **含めるタグ属性(Tag attributes to include)** -ページ構造に含めるタグ属性を示します。通常、タグ属性とその値は、構造を決定するときに削除されます。カンマ区切りリストでこのフィールドにタグ属性を指定すると、それらの属性とその値がページ構造に追加されます。デフォルトでは、「`id,class`」タグ属性が含められます。 **ヒント:** いくつかのサイトは、主に1種類のタグで構成されることがあります(例: `<div>`)。これらの属性を含めると、より厳密なページの照合が行われます。これらの属性を除外すると、照合の厳密度は低くなります。
1つのURLの最大ヒット数を以下に制限する(Limit maximum single URL hits to)	サイトの設定により、Web探索が同じURLを無限にループする場合があります。このフィールドを使用して、1つのURLがWeb探索される回数を制限します。デフォルト値は5です。
ヒット数にパラメータを含める(Include parameters in hit count)	**[1つのURLの最大ヒット数を以下に制限する(maximum single URL hits to)]**(上記)を選択すると、同じURLが検出されるたびにカウンタがインクリメントされます。ただし、 **[ヒット数にパラメータを含める(Include parameters in hit count)]**も選択すると、HTTP要求で指定されたURLにパラメータが追加された場合に、Web探索プログラムは、そのリソースを1つのURLの上限までWeb探索します。異なるパラメータのセットは、それぞれ固有のものと見なされ、別のカウントが行われます。 たとえば、このオプションを選択すると、「page.aspx?a=1」と「page.apsx?b=1」の両方が固有のリソースとしてカウントされます(つまり、Web探索プログラムが2つのページを検出したことを意味します)。 このオプションを選択しない場合、「page1.aspx?a=1」と

オプション	説明
	「page.aspx?b=1」は同じリソースとして扱われます(つまり、Web探索プログラムが同じページを2度検出したことを意味します)。 **注記:** この設定は、GETとPOSTの両方のパラメータに適用されます。
ディレクトリの最大ヒット数を以下に制限する(Limit maximum directory hit count to)	この設定では、Web探索中に各ディレクトリ内で一巡するサブディレクトリおよびページの最大数を定義します。この設定は、Web探索の範囲を縮小し、コンテンツ管理システム(CMS)で構成されるサイトなど、一部のサイトのスキャン時間を短縮するのに役立ちます。デフォルト設定は200です。
最小フォルダ深度(Minimum folder depth)	**ディレクトリの最大ヒット数を以下に制限する(Limit maximum directory hit count to)**](上記)を選択した場合、この設定は、ディレクトリの最大ヒット数の適用を開始するフォルダの深さを定義します。デフォルト設定は1です。
リンクトラバーサルシーケンスの最大数を以下に制限する(Limit maximum link traversal sequence to)	このオプションは、OpenText DASTがサイトをWeb探索するときに連続してアクセスできるハイパーリンクの数を制限します。たとえば、5つのリソースが次のようにリンクされている場合、 • ページAにページBへのハイパーリンクが含まれている • ページBにページCへのハイパーリンクが含まれている • ページCにページDへのハイパーリンクが含まれている • ページDにページEへのハイパーリンクが含まれている このオプションを「3」に設定すると、ページEはWeb探索されません。デフォルト値は15です。
Web探索フォルダの最大深度を以下に制限する(Limit maximum Crawl folder depth to)	このオプションは、1つの要求に含めることができるディレクトリの数を制限します。デフォルト値は15です。 たとえば、次のURLの場合、 http://www.mysite.com/Dir1/Dir2/Dir3/Dir4/Dir5/Dir6/Dir7 このオプションを「4」に設定すると、ディレクトリ5、6、および7の内容はWeb探索されません。
Web探索の最大数を以下に制限する(Limit maximum crawl count to)	この機能は、Web探索プログラムによって送信されるHTTP要求の数を制限します。大規模サイトのスキャンの完了に問題が発生した場合にのみ使用する必要があります。

オプション	説明
	注記: ここで設定した制限は、スキャン中に表示される[Web探索済み(Crawled)]進行状況バーには直接相関していません。ここで設定したWeb探索の最大数は、アプリケーションのWeb探索中にWeb探索プログラムによって検出されたリンクに適用されます。[Web探索済み(Crawled)]進行状況バーには、Web探索中にWeb探索プログラムによって検出されたリンクだけではなく、Web探索と監査中にリンクの解析が行われるすべてのセッション(要求と応答)が含まれます。
Webフォームの最大送信数を以下に制限する(Limit maximum Web form submission to)	通常、OpenText DASTは、複数のオプションを持つコントロール(リストボックスなど)が含まれているフォームを検出すると、リストから最初のオプション値を抽出してフォームを送信します。次に、2番目のオプション値を抽出してフォームを再送信し、リスト内のすべてのオプション値が送信されるまでこのプロセスを繰り返します。これにより、可能なすべてのリンクを確実にたどることができます。 ただし、値の完全なリストを送信すると逆効果になる場合があります。たとえば、「State」という名前のリストボックスに、米国の50州それぞれについて1つの値が含まれている場合、フォームのインスタンスを50件送信する必要はおそらくありません。 この設定を使用して、OpenText DASTが実行する送信の総数を制限します。デフォルト値は3です。
反復パスセグメントの抑止(Suppress Repeated Path Segments)	多くのサイトには、相対パスのようでありながら、OpenText DASTによる解析と、Web探索対象のURLへの追加が済むと、使用不能なURLになるテキストがあります。こうしたものの出現は、パスが連続して追加される場合(`/foo/bar/foo/bar/`など)に、暴走スキャンになるおそれがあります。こうしたものの出現を減らす上でこの設定は役に立ち、デフォルトで有効になっています。 この設定が**有効**な場合、次のオプションがあります。 **1** - URL内のどこかで繰り返されている単一のサブフォルダを検出し、一致がある場合はそのURLを拒否します。たとえば、`/foo/baz/bar/foo/`では「`/foo/`」が繰り返されているので一致します。この繰り返しは隣接している必要はありません。 **2** -隣接するサブフォルダの2つ以上のペアを検出し、一致がある場合はURLを拒否します。たとえば、`/foo/bar/baz/foo/bar/`では「`/foo/bar/`」が繰り返されているので一致します。 **3** -隣接する3つのサブフォルダの2つ以上のセットを検出し、一致が

オプション	説明
	ある場合はURLを拒否します。 **4** -隣接する4つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。 **5** -隣接する5つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。 この設定が**無効**な場合、サブフォルダの繰り返しは検出されず、一致が原因でURLが拒否されることはありません。

スキャン設定: JavaScript

この機能にアクセスするには、 **編集(Edit)**]メニューをクリックし、 **デフォルトのスキャン設定(Default Scan Settings)**]または **現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、 **スキャン設定(Scan Settings)**]カテゴリで、 **JavaScript**]を選択します。

JavaScriptの設定

JavaScriptアナライザを使用すると、OpenText DASTは、JavaScriptによって定義されたリンクをWeb探索し、JavaScriptによってレンダリングされたドキュメントを作成して監査することができます。

ヒント: スクリプトの分析中にOpenText DASTがWeb探索を実行する速度を上げるには、イメージ/写真が表示されないようにブラウザオプションを変更します。

次の表の説明に従って設定を行います。

オプション	説明
スクリプト実行で検出されたリンクをWeb探索する(Crawl links found from script execution)	このオプションを選択した場合は、Web探索プログラムがダイナミックリンク(つまり、JavaScriptの実行中に生成されたリンク)をたどります。
詳細スクリプトパーサのデバッグログ記録(Verbose script parser debug	この設定を選択し、かつ ログレベルのアプリケーション設定(Application setting for logging level)]が デバッグ(Debug)]に設定されている場合、OpenText DASTはDOMオブジェクトで呼び出されたすべてのメソッドをログに記録します。これにより、中規模サイ

オプション	説明
logging)	トや大規模サイト用の数ギガバイトのデータを簡単に作成できます。
JavaScriptエラーのログ記録(Log JavaScript errors)	OpenText DASTは、スクリプト解析エンジンからのJavaScript解析エラーをログに記録します。
JS Framework UI除外の有効化(Enable JS Framework UI Exclusions)	このオプションが選択されている場合、OpenText DASTのJavaScriptパーサは、カレンダコントロールやリボンバーなどの一般的なJQueryおよびExt JSユーザインタフェースコンポーネントを無視します。その後、これらの項目はスキャン中にJavaScript実行から除外されます。
サイト全体のイベント削減の有効化(Enable Site-Wide Event Reduction)	このオプションが選択されている場合、Web探索プログラムとJavaScriptエンジンは、Webサイトのさまざまな部分に表示される共通の機能エリア(共通メニューやページフッタなど)を認識します。これにより、すでにWeb探索済みのHTMLコンテンツ内のダイナミックリンクやフォームを検索する必要がなくなり、その結果、スキャンが高速化します。このオプションはデフォルトで有効であり、通常、無効にすべきではありません。
WebSocketイベントのキャプチャ	WebSocketは非同期プロトコルです。このことは、すべての要求が応答を必要とするわけではないことを意味します。要求が応答を受信しない場合、WebSocketは多くの場合タイムアウトで終了し、スキャン時間と新しい攻撃露呈部分の検出機能の両方に影響を与えます。スキャン品質に悪影響を与えるのを防ぐため、このオプションはデフォルトで無効になっています。
1ページあたりの最大スクリプトイベント数(Max script events per page)	特定のスクリプトは、同じイベントを無限に実行します。単一のページで許容されるイベントの数を、1-9999の値に制限できます。デフォルト値は1000です。
SPAのサポート	SPAサポートは、シングルページアプリケーションに適用されます。有効にすると、DOMスクリプトエンジンは、Web探索中に、JavaScriptインクルード、フレームとiframeのインクルード、CSSファイルインクルード、およびAJAX呼び出しを検索してから、それらのイベントによって生成されたすべてのトラフィックを監査します。 SPAサポートのオプションを以下に示します。 • **自動(Automatic)** - OpenText DASTがSPAフレームワークを検出すると、自動的にSPAサポートモードに切り替わります。

オプション	説明
	• **有効(Enabled)** - SPAフレームワークがターゲットアプリケーションで使用されていることを示します。 注意! {/b}SPAサポートは、シングルページアプリケーションに対してのみ有効にするべきです。SPAサポートを有効にしてSPA以外のWebサイトをスキャンすると、スキャンが遅くなります。 • **無効(Disabled)** - SPAフレームワークがターゲットアプリケーションで使用されていないことを示します。 詳細については、「"シングルページアプリケーションスキャンについて" ページ235」を参照してください。

スキャン設定:リクエスタ

リクエスタは、HTTP要求と応答を処理するソフトウェアモジュールです。

この機能にアクセスするには、 **[編集(Edit)]** メニューをクリックし、 **[デフォルトのスキャン設定(Default Scan Settings)]** または **[現在のスキャン設定(Current Scan Settings)]** を選択します。その後で、 **[スキャン設定(Scan Settings)]** カテゴリで、 **[リクエスタ(Requestor)]** を選択します。

リクエスタパフォーマンス(Requestor performance)

[リクエスタパフォーマンス(Requestor Performance)]オプションについて、次の表で説明します。

オプション	説明
共有リクエスタを使用する(Use a shared requestor)	このオプションを選択すると、Web探索プログラムと監査プログラムは、サイトのスキャン時に共通のリクエスタを使用し、各スレッドは同じ状態を使用します。この状態も両方のモジュールで共有されます。これは以前のバージョンのOpenText DASTで使用されていた手法を再現するものであり、状態の維持が重要な考慮事項ではない場合に適しています。スレッドの最大数(最大75)も指定します。
個別のリクエスタを使用する(Use separate	このオプションを選択した場合、Web探索プログラムと監査プログラムは別々のリクエスタを使用します。また、監査プログラムのリクエスタは、すべてのスレッドで同じ状態を使用するのではなく、各スレッド

オプション	説明
requestors)	に状態を関連付けます。この方法により、スキャンが大幅に高速になります。 Web探索および監査を実行するとき、リクエスタごとに作成できるスレッドの最大数を指定できます。 [**Web探索リクエスタスレッド数(Crawl requestor thread count)**]オプションでは、最大25の同時HTTP要求を送信してから、最初の要求に対するHTTP応答を待機するように設定できます。デフォルト設定は5です。 [**監査リクエスタスレッド数(Audit requestor thread count)**]は、最大50に設定できます。デフォルト設定は10です。スレッド数を増やすと、スキャンの速度を速くすることができますが、スキャンするサーバのリソースだけでなく、システムリソースも消費し尽くされる場合があります。 **注記:** スキャンするアプリケーションの容量によっては、スレッド数を増やすと、サーバの負荷が増大するために要求の失敗が増加し、一部の応答が [**要求タイムアウト(Request timeout)**]設定を超える場合があります。要求の失敗によってスキャンのカバレッジが縮小する可能性があります。これは、失敗した応答によって、追加の攻撃露呈部分が明らかになったり脆弱性が表面化したりした可能性があるためです。要求の失敗の増加に気付いた場合は、それを縮小するために [**要求タイムアウト(Request timeout)**]を大きくしたり、 [**Web探索リクエスタスレッド数(Crawl requestor thread count)**]と [**監査リクエスタスレッド数(Audit requestor thread count)**]を小さくしたりすることができます。 また、スキャンするアプリケーションの性質によっては、Web探索スレッド数の増加により、同じサイトの後続のスキャンどうしの整合性が低下する場合があります。これはWeb探索要求の順序が異なることが原因です。デフォルトの [**Web探索リクエスタスレッド数(Crawl requestor thread count)**]設定を1に減らすと、整合性が向上する可能性があります。

リクエスタ設定(Requestor settings)

[リクエスタ設定(Requestor Settings)]オプションについて、次の表で説明します。

オプション	説明
最大応答サイズを以下に制限する(Limit maximum response size to)	このオプションを選択すると、受け入れるサーバ応答のサイズを制限し、最大サイズ(キロバイト単位)を指定できます。デフォルトは1000キロバイトです。Flashファイル(.swf)およびJavaScriptの「include」ファイルは、この制限を受けないことに注意してください。
要求の再試行回数(Request retry count)	「failed」応答(ソケットエラーまたは要求タイムアウトとして定義されます)を受信した後に、OpenText DASTがHTTP要求を再送信する回数を指定します。値はゼロより大きくする必要があります。
要求タイムアウト(Request timeout)	OpenText DASTがサーバからのHTTP応答を待つ時間を指定します。このしきい値を超えると、OpenText DASTは、再試行回数に達するまで要求を再送信します。OpenText DASTは、応答を受信しない場合、タイムアウトをログに記録し、次の一連の攻撃の最初のHTTP要求を送信します。デフォルト値は20秒です。 **注記:** タイムアウトが初めて発生したときに、OpenText DASTはタイムアウト期間を延長し、サーバが応答していないことを確認します。延長された要求タイムアウト時間内にサーバが応答した場合、その延長期間が現在のスキャンの新しい要求タイムアウトになります。

コネクティビティの喪失が検出された場合にスキャンを停止する(Stop scan if loss of connectivity detected)

スキャン中に、Webサーバで障害が発生したり、過度にビジーになって、タイミングよく応答できなくなったりする場合があります。タイムアウトの回数にしきい値を指定することで、スキャンを終了するようにOpenText DASTに指示できます。

次の表で、オプションについて説明します。

オプション	説明
スキャンを停止するまでの「単一ホスト」の連続した再試行失敗数	1つの特定のサーバで許可される連続タイムアウトの数を入力します。デフォルト値は75です。

オプション	説明
(Consecutive "single host" retry failures to stop scan)	
スキャンを停止するまでの「すべてのホスト」の連続した再試行失敗数 (Consecutive "any host" retry failures to stop scan)	すべてのホストで許可される連続タイムアウトの総数を入力します。デフォルト値は150です。
スキャンを停止するまでの「単一ホスト」の非連続の再試行失敗数 (Nonconsecutive "single host" retry failures to stop scan)	1つのホストで許可される非連続タイムアウトの総数を入力します。デフォルト値は「無制限」です。
スキャンを停止するまでの「すべてのホスト」の非連続の再試行失敗数 (Nonconsecutive "any host" retry failures to stop scan)	すべてのホストで許可される非連続のタイムアウトの総数を入力します。デフォルト値は350です。
最初の要求が失敗した場合にスキャンを停止する(If first request fails, stop scan)	このオプションを選択すると、ターゲットサーバがOpenText DASTの最初の要求に応答しない場合に、OpenText DASTで強制的にスキャンが終了されます。
受信した場合にスキャンを停止する応答コード(Response codes to stop scan if received)	受信した場合に、OpenText DASTで強制的にスキャンが終了されるHTTPステータスコードを入力します。カンマを使用してエントリを区切ります。コードの範囲(両端を含む)を指定するにはハイフンを使用します。

スキャン設定:セッション除外

この機能にアクセスするには、 **[編集(Edit)]** メニューをクリックし、 **[デフォルトのスキャン設定(Default Scan Settings)]** または **[現在のスキャン設定(Current Scan Settings)]** を選択します。その後で、 **[スキャン設定(Scan Settings)]** カテゴリで、 **[セッション除外(Session Exclusions)]** を選択します。

これらの設定は、OpenText DAST脆弱性スキャンのWeb探索と監査の両方のフェーズに適用されます。Web探索のみまたは監査のみの除外を指定するには、 **[Web探索設定:セッション除外(Crawl Settings: Session Exclusions)]** または **[監査設定:セッション除外(Audit Settings: Session Exclusions)]** を使用します。

除外または拒否するファイル拡張子

ファイルのタイプを指定して、そのファイルを除外するか拒否するかを指定できます。

- **拒否(Reject)** - OpenText DASTは、指定したタイプのファイルを要求しません。
- **除外(Exclude)** - OpenText DASTはファイルを要求しますが、(監査中に)それらのファイルを攻撃したり、それらのファイルで他のリソースへのリンクを検査したりしません。

デフォルトでは、ほとんどのイメージ、描画、メディア、オーディオ、ビデオ、および圧縮ファイルのタイプは拒否されます。

拒否または除外するファイル拡張子を追加するには:

1. **[追加(Add)]** をクリックします。
   [除外拡張子(Exclusion Extension)] ウィンドウが開きます。
2. **[ファイル拡張子(File Extension)]** ボックスに、ファイル拡張子を入力します。
3. **[拒否(Reject)]** と **[除外(Exclude)]** のどちらかまたは両方を選択します。
4. **[OK]** をクリックします。

除外MIMEタイプ

OpenText DASTは、指定したMIMEタイプに関連付けられたファイルを処理しません。デフォルトでは、イメージ、オーディオ、およびビデオのタイプは除外されます。

除外するMIMEタイプを追加するには:

1. **[追加(Add)]** をクリックします。
   [除外するMimeタイプの指定(Provide a Mime-type to Exclude)] ウィンドウが開きます。
2. **[Mimeタイプの除外(Exclude Mime-type)]** ボックスに、MIMEタイプを入力します。
3. **[OK]** をクリックします。

その他の除外/拒否基準

HTTPメッセージのさまざまなコンポーネントを特定してから、そのコンポーネントを含むセッションを除外するか拒否するかを指定できます。

- **拒否(Reject)** - OpenText DASTは、指定されたホストまたはURLにHTTP要求を送信しません。たとえば、通常、サイトからのログオフを処理するURLは拒否する必要があります。これは、スキャンが完了する前にアプリケーションからログアウトしたくないためです。
- **除外(Exclude)** - Web探索中に、OpenText DASTは、指定されたURLまたはホストで他のリソースへのリンクを調査しません。スキャンの監査部分の間は、OpenText DASTは指定されたホストまたはURLを攻撃しません。HTTP応答を処理せずにURLまたはホストにアクセスする場合は、 **除外(Exclude)**]オプションを選択しますが、 **拒否(Reject)**]は選択しません。たとえば、処理しないURL上の壊れたリンクをチェックするには、 **除外(Exclude)**]オプションだけを選択します。

基準の編集

デフォルトの基準を編集するには:

1. 基準を選択して、 **編集(Edit)**](**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。

   ホストまたはURLの拒否または除外(Reject or Exclude a Host or URL)]ウィンドウが開きます。
2. **ホスト(Host)**]または **URL**]を選択します。
3. **ホスト/URL(Host/URL)**]ボックスに、URLまたは完全修飾ホスト名、またはターゲットのURLまたはホストに一致するように設計された正規表現を入力します。
4. **拒否(Reject)**]と **除外(Exclude)**]のどちらかまたは両方を選択します。
5. **OK**]をクリックします。

基準の追加

除外/拒否基準を追加するには:

1. **追加(Add)**](**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。

   除外の作成(Create Exclusion)]ウィンドウが開きます。
2. **ターゲット(Target)**]リストから項目を選択します。
3. ターゲットとして **クエリパラメータ(Query Parameter)**]または **ポストパラメータ(Post Parameter)**]を選択した場合は、 **ターゲット名(Target Name)**]を入力します。
4. **一致タイプ(Match Type)**]リストから、ターゲット内のテキストの一致に使用される方法を選択します。
   - **正規表現に一致(Matches Regex)**] - **一致文字列(Match String)**]ボックスで指定した正規表現に一致します。

- [正規表現の拡張に一致(Matches Regex Extension)] - [一致文字列(Match String)]ボックスで指定したFortify正規表現の拡張から入手可能な構文に一致します。
- [一致(Matches)] - [一致文字列(Match String)]ボックスで指定したテキスト文字列に一致します。
- [含む(Contains)] - [一致文字列(Match String)]ボックスで指定したテキスト文字列を含みます。

5. [一致文字列(Match String)]ボックスに、ターゲットで検索する文字列または正規表現を入力します。または、[一致タイプ(Match Type)]で正規表現オプションを選択した場合は、ドロップダウン矢印をクリックして、[正規表現の作成(Create Regex)]を選択し、Regular Expression Editorを起動します。
6.  をクリックします(または<Enter>を押します)。
7. (オプション)ステップ2-6を繰り返して、条件を追加します。複数の一致はAND処理されます。
8. [現在の設定(Current Settings)]で作業している場合は、[テスト(Test)]をクリックして現在のスキャンの除外を処理できます。基準によって絞り込まれたそのスキャンからのセッションがテスト画面に表示され、必要に応じて設定を変更できます。
9. [OK]をクリックします。
10. [その他の除外/拒否基準(Other Exclusion/Rejection Criteria)]リストに除外が表示されている場合は、[拒否(Reject)]と[除外(Exclude)]のいずれかまたは両方を選択します。

注記: スキャン中は、応答タイプ、応答ヘッダタイプ、およびステータスコードターゲットタイプを拒否することができません。これらのターゲットタイプは除外することしかできません。

例1

Microsoft.comのリソースに対する要求を無視して送信しないようにするには、次の除外を入力して、[拒否(Reject)]を選択します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	contains	Microsoft.com

例2

一致文字列として「logout」と入力します。この文字列がURLの任意の部分で見つかった場合は、そのURLが除外または拒否されます(選択されたオプションによって異なる)。「logout」の例を使用すると、OpenText DASTは、loutout.aspやapplogout.jspなどのURLを除外または拒否します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	contains	logout

例3

次の例では、クエリパラメータ「username」が「John」と等しいクエリを含むセッションを拒否または除外します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
クエリパラメータ(Query parameter)	username	一致(matches)	John

例4

次の例では、次のディレクトリを除外または拒否します。

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	正規表現に一致(matches regex)	/W3SVC[0-9]*/

スキャン設定:許可ホスト

この機能にアクセスするには、 **編集(Edit)**]メニューをクリックし、 **デフォルトのスキャン設定(Default Scan Settings)**]または **現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、 **スキャン設定(Scan Settings)**]カテゴリで、 **許可ホスト(Allowed Hosts)**]を選択します。

許可ホスト設定の使用

許可ホスト(Allowed Host)]設定は、Web探索して監査するドメインを追加する場合に使用します。Webプレゼンスで複数のドメインが使用されている場合は、それらのドメインをここ

に追加します。たとえば、「WIexample.com」をスキャンする場合、「WIexample2.com」と「WIexample3.com」がWebプレゼンスの一部であり、かつそれらをWeb探索と監査に含めたいのであれば、それらのドメインをここに追加する必要があります。

この機能を使用して、指定したテキストが名前に含まれているドメインをスキャンすることもできます。たとえば、スキャンターゲットとして「www.myco.com」を指定し、許可ホストとして「myco」と入力したとします。OpenText DASTは、ターゲットサイトをスキャンして「myco」を含むURLへのリンクを検出すると、そのリンクをたどってそのサイトのサーバをスキャンします。この処理は、すべてのリンク先のサイトがスキャンされるまで繰り返されます。この仮説例では、OpenText DASTによって次のドメインがスキャンされます。

- www.myco.com:80
- contact.myco.com:80
- www1.myco.com
- ethics.myco.com:80
- contact.myco.com:443
- wow.myco.com:80
- mycocorp.com:80
- www.interconnection.myco.com:80

許可されたドメインの追加

許可するドメインを追加するには:

1. [**追加(Add)**]をクリックします。
2. [**許可ホストの指定(Specify Allowed Host)**]ウィンドウで、URL(またはURLを表す正規表現)を入力し、[**OK**]をクリックします。

注記: URLを指定する場合は、プロトコル指定子(http://やhttps://など)を含めないでください。

ドメインの編集または削除

許可されたドメインを編集または削除するには:

1. [**許可ホスト(Allowed Hosts)**]リストからドメインを選択します。
2. [**編集(Edit)**]または[**削除(Remove)**]をクリックします。

スキャン設定:HTTP解析

この機能にアクセスするには、[**編集(Edit)**]メニューをクリックし、[**デフォルトのスキャン設定(Default Scan Settings)**]または[**現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、[**スキャン設定(Scan Settings)**]カテゴリで、[**HTTP解析(HTTP Parsing)**]を選択します。

オプション

[HTTP解析(HTTP Parsing)]オプションについて、次の表で説明します。

オプション	説明
状態に使用されるHTTPパラメータ(HTTP Parameters Used for State)	お使いのアプリケーションでWebサイト内の状態を維持するためにURLの書き換えまたはPOSTデータの手法を使用する場合は、使用するパラメータを指定する必要があります。たとえば、PHP4スクリプトでは、セッション内で使用できる、SIDという名前のセッションIDの定数を作成できます。これをURLの末尾に追加すると、そのセッションIDを次のページで使用できるようになります。実際のURLは次のようになります。 .../page7.php?PHPSESSID=4725a759778d1be9bdb668a236f01e01 セッションIDは接続ごとに変更されるため、このURLを含むHTTP要求を再生しようとするとエラーが発生します。ただし、パラメータ(この例ではPHPSESSID)を指定すると、OpenText DASTは、接続が確立されるたびに、割り当てられた値を、サーバから取得された新しいセッションIDに置き換えます。 同様に、一部の状態管理手法では、POSTデータを使用して情報を渡します。たとえば、HTTPメッセージのコンテンツに、userid=slbhkelvbkl73dhjが含まれている場合があります。この場合、「userid」はユーザが指定するパラメータです。 **注記:** パラメータを指定する必要があるのは、アプリケーションが状態の管理にURLの書き換えまたはPOSTされたデータを使用する場合のみです。クッキーを使用する場合は必要ありません。 OpenText DASTは、潜在的なパラメータがPOSTされたデータとして出現する場合、またはURLのクエリ文字列内に存在する場合に、そのパラメータを特定できます。ただし、アプリケーションでセッションデータが拡張パス情報としてURLに埋め込まれている場合は、それを識別する正規表現を指定する必要があります。次の例では、「1234567」がセッション情報です。 http://www.onlinestore.com/bikes/(1234567)/index.html パラメータを識別するための正規表現は、/\([\w\d]+\)/です。
CSRFを有効にする(Enable CSRF)	[CSRFを有効にする(Enable CSRF)]オプションは、スキャンしているサイトにクロスサイトリクエストフォージェリ(CSRF)トークンが含まれている場合にのみオンにする必要があります。これをオンにするとプロセスのオーバーヘッドが追加されるためです。詳細については、「"CSRF" ページ427」を参照してください。

オプション	説明
URLパスから状態を判断する(Determine State from URL Path)	アプリケーションがURLパス内の特定のコンポーネントから状態を判断する場合は、このチェックボックスを選択して、それらのコンポーネントを識別する1つ以上の正規表現を追加します。2つのデフォルトの正規表現は、ASP.NETの2つのクッキーレスセッションIDを識別します。3番目の正規表現はjsessionidクッキーに対応します。
応答状態ルールを有効にする(Enable Response State Rules)	お使いのアプリケーションが、ベアラトークンを使用してクライアントの状態を維持している場合は、このオプションを選択して、応答からベアラートークンを識別し、次の要求に自動的に追加するルールを作成します。 **注記:** **自動応答状態ルール(Auto Response State Rules)**]オプションはデフォルトで有効に設定され、ベアラトークンの自動検出用に事前定義された複数のルールを提供します。次の手順で説明するように、応答状態ルールを有効にして、ルールを追加することにより、ベアラトークンの自動検出を強化できます。 ルールを追加するには: 1. **応答状態ルールを有効にする(Enable Response State Rules)**]チェックボックスを選択した後に、 **追加(Add)**.]をクリックします。 **ルールの検索と置換(Rule Search and Replace)**]ウィンドウが表示されます。 2. **ルール名(Rule Name)**]フィールドに、ルールの固有名を入力します。例: `Bearer`。 3. **応答での検索(Search in Response)**]フィールドの横の **追加(Add)**]をクリックします。 **応答での検索(Search in Response)**]ダイアログボックスが簡易モードで開きます。 **注記:** 以前に正規表現モードを選択していた場合は、ダイアログボックスは正規表現モードで開きます。 4. 次のいずれかを実行します。 • 簡易モードでルールを作成するには、トークンが含まれているテキストを **ルール(Rule)**]ボックスに入力します。入力すると、正規表現が **正規表現表示(Regex View)**]ボックスに自動的に生成されます。 **ヒント:** をクリックすると、事前定義されたトークンのリストが表示されます。

オプション	説明
	• 事前定義された正規表現を使用するには、[**正規表現モード(Regex Mode)**]を選択し、[**正規表現(Regex)**]リストから正規表現ステートメントを選択します。これで、選択されたステートメントを編集できます。 5. [**OK**]をクリックします。 正規表現が検証されます。先に進む前に、見つかったエラーをすべて修正する必要があります。 6. [**要求での置換(Replace in Request)**]フィールドの横の[**追加(Add)**]をクリックします。 [要求での置換(Replace in Request)]ダイアログボックスが簡易モードで開きます。 **注記:** 以前に正規表現モードを選択していた場合は、ダイアログボックスは正規表現モードで開きます。 7. 次のいずれかを実行します。 • 簡易モードでルールを作成するには、トークンが含まれているテキストを[**ルール(Rule)**]ボックスに入力します。入力すると、正規表現が[**正規表現表示(Regex View)**]ボックスに自動的に生成されます。 **ヒント:** をクリックすると、事前定義されたトークンのリストが表示されます。 • 事前定義された正規表現を使用するには、[**正規表現モード(Regex Mode)**]を選択し、[**正規表現(Regex)**]リストから正規表現ステートメントを選択します。これで、選択されたステートメントを編集できます。 8. [**OK**]をクリックします。 正規表現が検証されます。先に進む前に、見つかったエラーをすべて修正する必要があります。 9. [**OK**]をクリックして、[ルールの検索と置換(Rule Search and Replace)]ウィンドウを閉じます。 重要! {/b}システムリソースを消費し、スキャンのパフォーマンスに影響を与える可能性のある正規表現が使用されないようにするために、正規表現の構築時に以下のテキスト文字列は使用しないでください。 • 無限数を表す".*"または".+"を使用する文字 • 肯定先読み"(?=…)"

オプション	説明
	• 否定先読み"(?!...)" • 肯定後読み"(?<=…)" • 否定後読み"(?<!...)"
ナビゲーションに使用されるHTTPパラメータ(HTTP Parameters Used for Navigation)	一部のサイトでは、直接アクセスできるリソースは1つだけであり、要求された情報を提供するためにクエリ文字列を使用します。以下にいくつかの例を示します。 例:1 – http://www.anysite.com?Master.asp?Page=1例:2 – http://www.anysite.com?Master.asp?Page=2;例: 3 – http://www.anysite.com?Master.asp?Page=13;Subpage=4 1 – http://www.anysite.com?Master.asp?Page=1 Ex. 2 – http://www.anysite.com?Master.asp?Page=2; Ex. 3 – http://www.anysite.com?Master.asp?Page=13;Subpage=4 通常、OpenText DASTでは、これらの3つの要求が同じリソースを参照していると想定し、それらの1つに対してのみ脆弱性スキャンを実行します。そのため、ターゲットのWebサイトでこのタイプのアーキテクチャを採用する場合、使用される特定のリソースパラメータを識別する必要があります。 例1と2には、「Page」という1つのリソースパラメータが含まれています。 例3には、「Page」と「Subpage」という2つのパラメータが含まれています。 リソースパラメータを識別するには: 1. [追加(Add)]をクリックします。 2. [HTTPパラメータ(HTTP Parameter)]ウィンドウで、パラメータ名を入力して、[OK.]をクリックします。 入力した文字列が[パラメータ(Parameter)]リストに表示されます。 3. 追加のパラメータについて上記の手順を繰り返します。
高度なHTTP解析(Advanced HTTP Parsing)	ほとんどのWebページには、使用する文字セットをブラウザに知らせる情報が含まれています。この指示は、HTMLドキュメントのHEADセクションのContent-Type応答ヘッダ(またはHTTP-EQUIV属性を持つMETAタグ)を使用して行われます。 文字セットが示されていないページでは、OpenText DASTで使用すべき言語ファミリ(および暗黙の文字セット)を指定できます。
値のみ存在する場合にクエリパラメータ	この設定は、OpenText DASTが値のないクエリパラメータを解釈する方法を定義します。例: http://somehost?param

オプション	説明
値をパラメータ名として扱う(Treat query parameter value as parameter name when only value is present)	このチェックボックスが選択されている場合、OpenText DASTは、空の値を持つ「param」という名前のパラメータとして「param」を解釈します。 このチェックボックスがオフの場合、OpenText DASTは、値「param」を持つ名前のないパラメータとして「param」を解釈します。 この設定は、OpenText DASTがヒットカウントを計算する方法に影響することがあります(「スキャン設定: 全般」の"1つのURLの最大ヒット数を以下に制限する(Limit maximum single URL hits to)" ページ409の設定を参照してください)。この設定は、URLにアンチキャッシュ(anti-caching)パラメータが含まれているシナリオで役に立ちます。多くの場合、これらは数値カウンタまたはタイムスタンプの形式になります。たとえば、以下のパラメータは数値カウンタです。 • http://somehost?1234567 • http://somehost?1234568 この場合、値は要求ごとに変わります。値がパラメータ名として処理され、[ヒット数にパラメータを含める(Include parameters in hit count)]設定がオンになっている場合、Web探索のカウントが人為的に引き上げられて、スキャン時間が長くなる可能性があります。このような場合は、[値のみ存在する場合にクエリパラメータ値をパラメータ名として扱う(Treat query parameter value as parameter name when only value is present)]チェックボックスをオフにすると、これらのカウンタがヒットカウントに影響しないようになり、スキャン時間がより適切なものとなります。

CSRF

[CSRFを有効にする(Enable CSRF)]オプションは、スキャンしているサイトにクロスサイトリクエストフォージェリ(CSRF)トークンが含まれている場合にのみオンにする必要があります。これをオンにするとプロセスのオーバーヘッドが追加されるためです。

CSRFについて

クロスサイトリクエストフォージェリ(CSRF)はWebサイトの悪意のあるエクスプロイトであり、Webサイトが信頼するユーザのブラウザから不正なコマンドが送信されます。CSRFエクスプロイトは、サイトがユーザのブラウザで置いている信頼に便乗します。つまり、ユーザがサイトによってすでに認証され、信頼チェーンがまだ開いているという事実を利用します。

例:

ユーザが銀行にアクセスして認証を受け、ユーザのマシンにクッキーが残されます。ユーザは、銀行取引を完了すると、別のブラウザタブに切り替えて、自分の趣味をテーマにした、愛好家のWebサイトでやり取りを継続します。サイト上で、誰かがHTMLイメージ要素を含むメッセージを投稿していました。このHTMLイメージ要素には、口座からすべての現金を引き出して別の口座に振り込むという、ユーザの銀行に対する要求が含まれています。ユーザのデバイスにはまだ期限切れではないクッキーがあるため、取引が履行され、口座内のすべての資金が引き出されます。

多くの場合、CSRFエクスプロイトにはユーザの識別情報に対する信頼に依存するサイトが関わっています。多くの場合、その信頼は、クッキーの使用を通して維持されます。次いで、ユーザのブラウザはだまされて、ユーザのブラウザとターゲットサイトとの間にまだ信頼が存在していると思って、ターゲットサイトにHTTP要求を送信します。

CRSFトークンの使用

クロスサイトリクエストフォージェリの発生を阻止する一般的な方法は、「CSRFToken」などの一般名を持つランダムに生成されたパラメータを含む要求を生成するようにサーバをセットアップすることです。トークンはセッションごとに1回ずつ生成することも、要求ごとに新しく生成することもできます。コード内でCSRFトークンを使用し、OpenText DASTでCSRFを有効にしている場合は、それを考慮に入れてサイトがWeb探索されます。OpenText DASTは、攻撃を仕掛けるたびに、新しいCSRFトークンを取得するためのフォームを要求します。これにより、OpenText DASTがスキャンを完了するまでにかかる時間が大幅に増えるため、サイト上でCSRFトークンを使用していない場合はCSRFを有効にしないでください。

OpenText DASTでのCSRF認識の有効化

サイトでCSRFトークンを使用している場合は、次のように、OpenText DASTでCSRF認識を有効にすることができます。

1. [**編集(Edit)**]メニューから[**デフォルトのスキャン設定(Default Scan Settings)**]を選択します。
   [**スキャン設定(Scan Settings)**]ウィンドウが表示されます。
2. [**スキャン設定(Scan Settings)**]列で、[**HTTP解析(HTTP Parsing)**]を選択します。
3. [**CSRFの有効化(Enable CSRF)**]ボックスをオンにします。

スキャン設定:カスタムパラメータ

この機能にアクセスするには、[**編集(Edit)**]メニューをクリックし、[**デフォルトのスキャン設定(Default Scan Settings)**]または[**現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、[**スキャン設定(Scan Settings)**]カテゴリで、[**カスタムパラメータ(Custom Parameters)**]を選択します。

カスタムパラメータは、URL書き換え手法およびREST (Representation State Transfer) Webサービステクノロジ(あるいはその一方)を使用するサイトに対応するために使用されます。これらのカスタムパラメータのルールを記述するか、Webアプリケーション記述言語(WADL)で記述された共通の環境設定ファイルからルールをインポートできます。

URLの書き換え

多くのダイナミックサイトではURLの書き換えが使用されます。スタティックURLはユーザが覚えやすく、検索エンジンがサイトにインデックスを付けやすいためです。たとえば、次のようなHTTP要求は、

http://www.pets.com/ShowProduct/7

サーバの書き換えモジュールに送信され、URLが以下に変換されます。

http://www.pets.com/ShowProduct.php?product_id=7

この例では、このURLによってサーバはPHPスクリプト「ShowProduct」を実行し、製品番号7の情報を表示します。

OpenText DASTは、ページをスキャンする際、どの要素が変数か判断して、攻撃エージェントが脆弱性を完全にチェックできるようにする必要があります。これを有効にするには、これらの要素を識別するルールを定義する必要があります。そのためには、独自のOpenText DAST構文を使用します。

例:

HTML: User 1 details
ルール: /someDetails/{username}/

HTML: User 1 details
ルール: /TwoParameters/Details/{username}/{parameter2}

HTML: User 1 details
ルール: /{parameter2}/PreFixParameter/Details/{username}

RESTfulサービス

RESTful Webサービス(RESTful Web APIとも呼ばれる)は、HTTPおよびRESTの原則を使用して実装されるシンプルなWebサービスです。これは、SOAPおよびWSDL(Web Services Description Language)ベースのWebサービスに代わるシンプルなサービスとして、Web全体で広く普及しています。

以下の要求は、HTTPクエリ文字列を使用してファイルに名前を追加します。

```
GET /adduser?name=Robert HTTP/1.1
```

あるWebサービスでは、これと同じ機能を次の方法で達成できます。パラメータ名と値が要求URIから移動され、要求本文にXMLタグとして現れていることに注意してください。

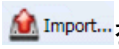
```
POST /users HTTP/1.1 Host: myserver
 Content-Type: application/xml
 <?xml version="1.0"?>
```

```
<user>
<name>Robert</name>
</user>
```

URLの書き換えとRESTful Webサービスのどちらの場合も、適切な要求の作成方法をOpenText DASTに指示するルールを作成する必要があります。

ルールの操作

次の表の説明に従って、カスタムパラメータのルールを操作できます。

目的の作業...	その場合...
ルールを作成する	1. **新規ルール(New Rule)**]をクリックします。 2. **式(Expression)**]列にルールを入力します。ガイドラインと例については、「"パスマトリックスパラメータ" 次のページ」を参照してください。 デフォルトでは、 **有効(Enabled)**]チェックボックスがオンになります。OpenText DASTによってルールが調べられ、有効な場合は、赤い**X**が削除されます。
ルールを削除する	1. **カスタムパラメータルール(Custom Parameters Rules)**]リストからルールを選択します。 2. **削除(Delete)**]をクリックします。
ルールを削除せずに無効にする	1. ルールを選択します。 2. **有効(Enabled)**]列のチェックマークをオフにします。
ルールを含むファイルをインポートする	1.  をクリックします。 2. 標準のファイル選択ダイアログボックスを使用して、適用するカスタムルールを含むファイルのタイプ(.wadlまたは.txt)を選択します。 3. ファイルを見つけて、 **開く(Open)**]をクリックします。

スキャン時に使用されていないルールの自動シードを有効にする(Enable automatic seeding of rules that were not used during scan)

カスタムパラメータの最も信頼できるルールは、WADLファイルから推測されたルール、またはWebサイトの開発者によって作成されたルールです。スキャン中にルールが呼び出されない場合(ルールがどのURLにも一致しないため)、OpenText DASTは、サイトの有効な部分が攻撃されていないとプログラム的に想定できます。したがって、このオプションを選択すると、OpenText DASTは、攻撃露呈部分を拡大するためにこれらの未使用のルールを実行するセッションを作成します。

URLパラメータのダブルエンコード(Double encode URL parameters)

ダブルエンコーディングは、セキュリティ制御をバイパスしたり、アプリケーションから予期しない動作を引き起こしたりするために、ユーザ要求パラメータを16進数形式で2回エンコードする攻撃手法です。たとえば、クロスサイトスクリプティング(XSS)攻撃は通常、次のようになります。

```
<script>alert('FOO')</script>
```

この悪意のあるコードが脆弱なアプリケーションに挿入され、警告ウィンドウに「FOO」というメッセージが表示される可能性があります。ただし、Webアプリケーションでは、<(より小さい)、>(より大きい)、および/(スラッシュ)などの文字を禁止するフィルタを使用できます。これらの文字がWebアプリケーション攻撃の実行に使用されるためです。攻撃者は、「ダブルエンコーディング」手法を使用してクライアントのセッションを悪用することで、この保護手段を回避しようとする可能性があります。このJavaScriptのエンコーディングプロセスは次のとおりです。

文字	16進エンコード	エンコードされた%記号	ダブルエンコードされた結果
<	%3C	%25	%253C
/	%2F	%25	%252F
>	%3E	%25	%253E

最後に、ダブルエンコードされた悪意のあるコードは次のようになります。

```
%253Cscript%253Ealert('XSS')%253C%252Fscript%253E
```

このオプションを選択すると、OpenText DASTは、(単一エンコードパラメータではなく)二重エンコードURLパラメータを作成し、攻撃シーケンスの一部として送信します。これは、Webサーバが、たとえば、Apache mod-rewriteとPHPや、Java URL Rewrite Filter 3.2.0などを使用する場合に推奨されます。

パスマトリックスパラメータ

システムでルールを作成するには3つの方法があります。ルールは次の方法で作成できます。

- 手動で入力する
- ユーザが指定した、またはOpenText DAST Agentを介して受信したWADLファイルから生成する
- ルールのリストを含むフラットファイルからインポートする

ルールを手動で入力する場合は、パラメータとして扱う必要のあるURLのパスセグメントを指定します。

ルールでは、特殊文字を使用して、パラメータを含む実際のURLの一部が指定されます。URLがルールに一致する場合、OpenText DASTによってパラメータが解析されて攻撃が行われます。ルールの重要なコンポーネントは次のものです。

- パス(gp/c/{book_name}/)
- クエリ(「?」の後に続くもの)
- フラグメント(「#」の後に続くもの)

パスセグメントの定義

パスセグメントは「/」文字で始まり、もう1つの「/」文字または行の末尾のいずれかで終了します。たとえば、パス「/a」には1つのセグメントがあるのに対し、パス「/a/」には2つのセグメントがあります(最初のセグメントは文字列「a」を含み、2つ目のセグメントは空です)。パス「/a」とパス「/a/」は等しくありません。URLがルールに一致するかどうかを判断しようとする際には、空のセグメントが考慮されます。

ルールの特別な要素

次の表で説明する特別な要素をルールに含めることができます。

要素	説明
*	アスタリスク。以下で定義する結果に使用できます。パス以外の結果に存在する場合は、URLのこの部分が一致に関与しない(つまり、あらゆるものと一致する)ことを意味します。
{ }	グループ。ルールのパス内で使用できる名前付きパラメータ。内容に特別な意味はなく、攻撃を受けたパラメータの名前としてレポート作成時に使用されます。グループを指定する区切り括弧{ }内で使用できる文字セットは、RFC 3986で*pchar:と定義されています。 `pchar = unreserved / pct-encoded / sub-delims / ":" / "@"` `pct-encoded = "%" HEXDIG HEXDIG` `unreserved = ALPHA DIGIT - . _ ~` `reserved = gen-delims / sub-delims` `gen-delims = : / ? # [ ] @"` `sub-delims = ! $ & ' ( ) * + , ; =` 「左括弧」と「右括弧」文字は、パーセントエンコード要素としてエスケープしない限り、グループの内容に含めることはできません。

パスの外に*を配置する場合のルールは次のとおりです。パスセグメントにいくつでも*と{}グループを入れることができますが、間にプレーンテキストを挟むことが必要です。例:

有効なルール: /gp/c/*={param}
無効なルール: /gp/c/*{}

セグメント内に**、*{}、{}*または{}{}エントリが含まれているルールは無効です。

URLと照合するルールでは、ルールのすべてのコンポーネントが、Web探索されるURLの対応するコンポーネントと一致している必要があります。パスの比較はセグメント単位で実行されます。*と{}グループは任意の数の文字(ゼロ個の文字を含む)に一致し、プレーンテキスト要素はURLのパスセグメントの対応するプレーンテキスト要素に一致します。次に例を示します。

/gp/c/{book_name}は、次のURLに一致します。

- http://www.amazon.com:8080/gp/c/Moby_Dick
- http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&price=0
- https://www.amazon.com/gp/c/Hobbit

一方、次のURLとは一致しません。

- http://www.amazon.com /gp/c/Moby_Dick/ (末尾のスラッシュが原因で一致しない)
- http://www.amazon.com/gp/c/Sex_and_the_City/Horror (セグメント数が異なっているため一致しない)

OpenText DASTでは、ルールURL内の{…}グループに一致するパスセグメントの要素は、クエリ内で検出されたものと同様にパラメータとして扱われます。さらに、ルールに一致するWeb探索対象のURLのクエリパラメータは、URLのパス内にあるパラメータと一緒に攻撃されます。次に挙げる一致するURLの例では、OpenText DASTによって、フォーマットパラメータと価格パラメータ、およびパスの3つ目のセグメント(Singularity_Sky)に対して攻撃が行われます。

http://www.amazon.com/gp/c/Singularity_Sky?format=pdf&:price=0

アスタリスクプレースホルダ

「*」プレースホルダは、次に挙げるURLの結果と副次的な結果で使用できます。

- パス-パス内の*は単一のセグメント、またはそれより小さい部分に一致するため、全体に一致させることはできません。
  - パスセグメント- /gp/*/{param}など。この場合、スキーマHTTP、ホスト名(www.amazon.com)、3つのセグメント(1つ目のセグメントは「gp」そのもの、2つ目は任意のセグメント、3つ目はパラメータとして扱われ、一致に関与しない)を含むパスを持つURLと一致します。
  - パスセグメントの一部- /gp/ref=*など。この場合、2つのセグメント(1つ目は「gp」そのもの、2つ目はプレフィクス「ref=」が付加された任意の文字列を含む)を含むパスを持つURLと一致します。
- クエリ- /gp/c/{param}?*など。この場合、3つのセグメント(1つ目のセグメントは「gp」、2つ目のセグメントは「c」、3つ目のセグメントはパラメータであるため一致に関与しない)から成るパスを持つURLに一致します。このURLには任意の構造のクエリ文字列が含まれている必要もあります。ルール/gp/c/{param}とルール/gp/c/{param}?*の違いに注意してください。1つ目のルールはURL http://www.amazon.com/gp/c/Three_Little_Blind_Miceと一致しますが、2つ目のルールは一致しません。

- クエリのキーと値のペア- `/gp/c/{param}?format=*`など。この場合、クエリ文字列にキーと値のペアが1つだけあり、キー名が「format」の場合に限り、URLと一致します。
- クエリのキーと値のペア- `/gp/c/{param}?*=pdf`など。この場合、クエリ文字列にキーと値のペアが1つだけあり、値が「pdf」の場合に限り、URLと一致します。

- フラグメント- `/gp/c/{param}#*`など。この場合、フラグメント部分が存在するあらゆるURLと一致します。

プレースホルダを使用する利点

プレースホルダを使用する主な利点は、マトリックスパラメータとURLパスベースのパラメータを組み合わせたルールを1つのルール内で作成できることです。関連する以下のURLを例として考慮します。

http://www.amazon.com/gp/color;foreground=green;background=black/something?format=dvi

次のルールを使うと、すべてのパラメータに対する攻撃が許可されます。

```
gp/*/{param}
```

マトリックスパラメータセグメントはパスの2つ目のセグメント内にある*プレースホルダによって無視されますが、OpenText DASTによって認識され、適切に攻撃されます。

複数のルールが1つのURLに一致する場合

複数のルールが特定のURLに一致する場合には、次の2つのオプションがあります:

- 一致が1つ検出されたらルールの反復処理を停止し、最初のルールのみを使用する。
- すべてのルールを反復処理し、一致するすべてのカスタムパラメータを収集する。

たとえば、次のURLの場合、

http://mySite.com/store/books/Areopagitica/32/1

次のルールが両方とも一致します。

- `*/books/{booktitle}/32/{paragraph}`
- `store/*/Areopagitica/{page}/{paragraph}`

OpenText DASTでは、最大の攻撃カバレッジを確保するために両方のルールからパラメータの収集が試みられます。そのため、3つのセグメント(上記の例では「Areopagitica」、「32」、および「1」)がすべて攻撃されます。

スキャン設定:フィルタ

この機能にアクセスするには、 **[編集(Edit)]**メニューをクリックし、 **[デフォルトのスキャン設定(Default Scan Settings)]**または **[現在のスキャン設定(Current Scan Settings)]**を選択します。その後で、 **[スキャン設定(Scan Settings)]**カテゴリで、 **[フィルタ(Filters)]**を選択します。

[フィルタ(Filters)]設定を使用して、HTTP要求と応答の検索および置換ルールを追加します。この機能は、クレジットカード番号、従業員名、または社会保障番号などの機密データが開示されるのを防ぐために最もよく使用されます。これは、OpenText DASTを使用する人や、生データまたは生成されたレポートにアクセスできる人に見られたくない情報を偽装するための方法です。

オプション

[フィルタ(Filter)]オプションについて、次の表で説明します。

オプション	説明
HTTP要求コンテンツのフィルタ(Filter HTTP Request Content)	このエリアを使用して、HTTP要求の検索および置換ルールを指定します。
HTTP応答コンテンツのフィルタ(Filter HTTP Response Content)	このエリアを使用して、HTTP応答の検索および置換ルールを指定します。

キーワードの検索および置換のためのルールの追加

次のステップに従って、要求または応答でキーワードを検索または置換するための正規表現ルールを追加します。

1. **[要求コンテンツ(Request Content)]**または**[応答コンテンツ(Response Content)]**グループのいずれかで、**[追加(Add)]**をクリックします。

   [要求/応答データのフィルタ基準の追加(Add Request/Response Data Filter Criteria)]ウィンドウが開きます。
2. **[テキストの検索(Search for text)]**ボックスに、検索する文字列を入力(または貼り付け)します(または、文字列を表す正規表現を入力します)。

   正規表現表記を挿入したり、Regular Expression Editor (式の作成とテストを容易にします)を起動したりするには、▸をクリックします。
3. **[テキストの検索場所(Search for text In)]**ボックスで、フィルタパターンを検索する要求または応答のセクションを選択します。オプションは次のとおりです。
   - **すべて(All)** -要求全体または応答全体を検索します。
   - **ヘッダ(Headers)** -各ヘッダを個別に検索します。Set-CookieヘッダやHTTP Versionヘッダなど、一部のヘッダは検索されません。

     注記: すべてのヘッダを確実に検索するには、**[プレフィクス(Prefix)]**を選択します。

- **Postデータ(Post Data)** -要求の場合のみ、すべてのHTTPメッセージ本文データを検索します。
- **本文(Body)** -すべてのHTTPメッセージ本文データを検索します。
- **プレフィクス(Prefix)** -要求行またはステータス行内のすべての内容、すべてのヘッダ、および本文の前の空の行を同時に検索します。

4. **検索テキストを次で置換(Replace search text with)**]ボックスに置換文字列を入力(または貼り付け)します。

   をクリックすると、正規表現についてのヘルプが表示されます。
5. 大文字と小文字を区別して検索する場合は、 **大文字と小文字を区別する(Case sensitive match)**]チェックボックスを選択します。
6. **OK**]をクリックします。

スキャン設定:クッキー/ヘッダ

この機能にアクセスするには、 **編集(Edit)**]メニューをクリックし、 **デフォルトのスキャン設定(Default Scan Settings)**]または **現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、 **スキャン設定(Scan Settings)**]カテゴリで、 **クッキー/ヘッダ(Cookies/Headers)**]を選択します。

標準のヘッダパラメータ

このセクションのオプションについて、次の表で説明します。

オプション	説明
HTTP要求ヘッダに「リファラ」を含める(Include 'referer' in HTTP request headers)	リファラヘッダをOpenText DAST HTTP要求に含めるには、このチェックボックスを選択します。クライアントは、Refererのrequest-headerフィールドを使用して、Request-URIの取得元リソースのアドレス(URI)をサーバのために指定できます。
HTTP要求ヘッダに「ホスト」を含める(Include 'host' in HTTP request headers)	ホストヘッダをOpenText DAST HTTP要求に含めるには、このチェックボックスを選択します。Hostのrequest-headerフィールドは、ユーザまたは参照元リソース(通常はHTTP URL)によって指定された元のURIから取得した、要求されているリソースのインターネットホストとポート番号を指定します。

カスタムヘッダの追加

このセクションは、OpenText DASTが実行する各監査に含まれるヘッダを追加、編集、または削除する場合に使用します。たとえば、「Alert: You are attacked by Consultant ABC」な

どのヘッダを追加できます。このヘッダは、OpenText DASTがそのサイトを監査しているときに会社のサーバに送信されるすべての要求に含められます。複数のカスタムヘッダを追加できます。

デフォルトのカスタムヘッダについて、次の表で説明します。

ヘッダ	説明
Accept: */*	任意のエンコーディングまたはファイルタイプをWeb探索プログラムで受け入れ可能です。
Pragma: no-cache	これにより、強制的に新しい応答が返されます。キャッシュまたはプロキシされたデータは受け入れられません。
Accept-Encoding: gzip, deflate	クライアントは、指定されたエンコード方式のいずれかをサーバが使用するよう要求します。

カスタムヘッダの追加

カスタムヘッダを追加するには:

1. [**追加(Add)**]をクリックします。
   [**カスタムヘッダの指定(Specify Custom Header)**]ウィンドウが開きます。
2. [**カスタムヘッダ(Custom Header)**]ボックスに、*<name>*: *<value>*という形式を使用してヘッダを入力します。
3. [**OK**]をクリックします。

カスタムクッキーの追加

このセクションでは、脆弱性スキャンを実行する際に、OpenText DASTによってサーバに送信されるHTTP要求でクッキーヘッダと一緒に送信されるデータを指定します。

スキャントラフィックにフラグを付けるために使用されるデフォルトのカスタムクッキーは次のとおりです。

```
CustomCookie=WebInspect;path=/
```

ヒント: 等号(=)は、名前`CustomCookie`と値`WebInspect`の間の区切り記号です。`path=/`は、このクッキーがすべての要求に適用されることを指定します。`WebInspect`という名前のカスタムクッキーは特別に処理されます。異なる名前を持つ他のカスタムクッキーは、標準クッキーとして扱われます。

カスタムクッキーの追加

カスタムクッキーを追加するには:

1. **[追加(Add)]**をクリックします。
   [カスタムクッキーの指定(Specify Custom Cookie)]ウィンドウが開きます。
2. **[カスタムクッキー(Custom Cookie)]**ボックスに、*<name>=<value>*という形式を使用してクッキーを入力します。

   たとえば、次のように入力すると、

   ```
   CustomCookie=ScanEngine
   ```

   各HTTP-Requestには、次のヘッダが含まれます。

   ```
   Cookie: CustomCookie=ScanEngine
   ```

   ヒント: カスタムクッキーを作成して、`path=/xyz`を指定した場合、そのカスタムクッキーは「`/xyz`」で始まる要求にのみ現れることになります。
3. **[OK]**をクリックします。

スキャン設定:プロキシ

この機能にアクセスするには、**[編集(Edit)]**メニューをクリックし、**[デフォルトのスキャン設定(Default Scan Settings)]**または**[現在のスキャン設定(Current Scan Settings)]**を選択します。その後で、**[スキャン設定(Scan Settings)]**カテゴリで、**[プロキシ(Proxy)]**を選択します。

オプション

[プロキシ(Proxy)]オプションについて、次の表で説明します。

オプション	説明
直接接続(プロキシ無効)(Direct Connection (proxy disabled))	プロキシサーバを使用しない場合は、このオプションを選択します。
プロキシ設定の自動検出(Auto detect proxy settings)	WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、ブラウザのWebプロキシ設定を行います。
システムのプロキシ	ローカルマシンからプロキシサーバ情報をインポートします。

オプション	説明
設定を使用する(Use System proxy settings)	
Firefoxプロキシ設定を使用する(Use Firefox proxy settings)	Firefoxからプロキシサーバ情報をインポートします。 **注記:** Firefoxプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が「プロキシーを使用しない」に設定されている場合、プロキシは使用されません。
PACファイルURLを使用してプロキシを設定する(Configure proxy using a PAC file URL)	[URL]ボックスで指定した場所にあるPAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。
プロキシを明示的に設定する(Explicitly configure proxy)	要求された情報を入力することによって、プロキシを設定します。 1. [サーバ(Server)]ボックスにプロキシサーバのURLまたはIPアドレスを入力し、続いて([ポート(Port)]ボックスに)ポート番号(8080など)を入力します。 2. プロキシサーバ経由でTCPトラフィックを処理するプロトコルの[タイプ(Type)]を、SOCKS4、SOCKS5、または標準から選択します。 3. 認証が必要な場合は、[認証(Authentication)]リストからタイプを選択します。 • **自動** **注記:** 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。 • **ダイジェスト** • **HTTP基本(HTTP Basic)** • **Kerberos** • **ネゴシエート(Negotiate)** • **NT LAN Manager (NTLM)**

オプション	説明
	4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。 5. 特定のIPアドレス(内部テストサイトなど)にアクセスするためにプロキシサーバを使用する必要がない場合は、**[プロキシをバイパスするサイト(Bypass Proxy For)]**ボックスにアドレスまたはURLを入力します。エントリを区切る場合は、カンマを使用します。
HTTPS用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)	HTTPS接続を受け入れるプロキシサーバの場合は、**[HTTPS用の代替プロキシを指定する(Specify Alternative Proxy for HTTPS)]**を選択し、要求された情報を入力します。

スキャン設定:認証

基本スキャン内でこの機能にアクセスするには、**[編集(Edit)]**メニューをクリックし、**[デフォルトのスキャン設定(Default Scan Settings)]**または**[現在のスキャン設定(Current Scan Settings)]**を選択します。その後で、**[スキャン設定(Scan Settings)]**カテゴリで、**[認証(Authentication)]**を選択します。

認証とは、セキュリティ対策として識別情報を検証することです。パスワードとデジタル署名が認証の形態です。OpenText DASTが認証を必要とするサーバまたはフォームに遭遇するたびに、ユーザ名とパスワードが入力されるように自動認証を設定できます。そうしなかった場合は、ログオン情報がないためにWeb探索が途中で停止する可能性があります。

スキャンにはネットワーク認証が必要(Scan Requires Network Authentication)

ユーザがWebサイトまたはアプリケーションにログオンする必要がある場合は、このチェックボックスをオンにします。

認証メソッド

認証が必要な場合は、次のように認証メソッドを選択します。

- **ADFS CBT**
- **自動**
- **基本**
- **ダイジェスト**
- **Kerberos**

- **NT LAN Manager (NTLM)**
- **OAuth 2.0 Bearer**

認証資格情報

OAuth 2.0 Bearerを除くすべての認証方法では、 **[認証資格情報(Authentication Credentials)]** エリアで次の手順を実行します。

1. **[ユーザ名(User name)]** ボックスにユーザIDを入力します。
2. **[パスワード(Password)]** ボックスにユーザのパスワードを入力します。
3. タイプミスから保護するため、 **[パスワードの確認]** ボックスに再度パスワードを入力します。

注意! {/b}OpenText DASTは、このパスワードによるアクセスが許可されたすべてのサーバをWeb探索します(このサイト/サーバが「許可ホスト」設定に含まれている場合)。管理システムに損傷を与える可能性を避けるため、管理権を持っているユーザ名とパスワードは使用しないでください。アクセス権が不明な場合は、システム管理者または社内のセキュリティプロフェッショナルに連絡するか、カスタマサポートにお問い合わせください。

OAuth 2.0 Bearerの方法では、 **[認証資格情報(Authentication Credentials)]** エリアで次の手順を実行します。

1. **[設定(Configure)]** をクリックします。
   [権限付与設定を開く(Open Authorization Configuration)] ダイアログが開きます。
2. "OAuth 2.0のBearer資格情報の設定" ページ447の手順に従います。

クライアント証明書(Client certificates)

クライアント証明書認証を使用すると、ユーザはユーザ名とパスワードを入力するのではなく、クライアント証明書を提示することができます。ローカルマシンから証明書を選択することも、現在のユーザに割り当てられた証明書を選択することもできます。コンピュータに接続された共通アクセスカード(CAC)リーダなどのモバイルデバイスからの証明書を選択することもできます。クライアント証明書を使用するには:

1. **[クライアント証明書(Client Certificates)]** エリアで、 **[有効化(Enable)]** チェックボックスをオンにします。
2. **[選択(Select)]** をクリックします。
   [クライアント証明書(Client Certificates)] ウィンドウが開きます。
3. 次のいずれかを実行します。
   - コンピュータにとってローカルで、コンピュータ上のすべてのユーザにとってグローバルな証明書を使用するには、 **[ローカルマシン(Local Machine)]** を選択します。
   - コンピュータ上のユーザアカウントにとってローカルな証明書を使用するには、 **[現在のユーザ(Current User)]** を選択します。

注記: 共通アクセスカード(CAC)リーダで使用される証明書はユーザ証明書であり、[現在のユーザ(Current User)]に保管されます。

4. 次のいずれかを実行します。
   - 「個人」(「マイ」)証明書ストアから証明書を選択するには、ドロップダウンリストから[マイ(My)]を選択します。
   - 信頼されたルート証明書を選択するには、ドロップダウンリストで[ルート(Root)]を選択します。
5. Webサイトでは、CACリーダまたはパスワードで保護された証明書を使用していますか。
   - 「はい」の場合は、次の手順を実行します。
     i. [証明書(Certificate)]リストから、「(Protected)」というプレフィクスが付いた証明書を選択します。
     選択した証明書に関する情報と[パスワード/PIN (Password/PIN)]フィールドが[証明書情報(Certificate Information)]エリアに表示されます。
     ii. パスワードまたはPINが必要な場合は、[パスワード/PIN (Password/PIN)]フィールドに入力します。

     注記: パスワードまたはPINが必要であるのに、ここで入力していないと、スキャン中にWindowsの[セキュリティ]ウィンドウのプロンプトが表示されるたびに、パスワードまたはPINを入力することが必要になります。

     重要! {/b}デフォルトでは、OpenText DASTはOpenSSLを使用します。OpenSSLではなく特定のSSL/TLSプロトコルを使用している場合、スキャン設定のProfiler部分はパスワードで保護されている証明書で動作しない場合があります。

     iii. [テスト(Test)]をクリックします。
     正しいパスワードまたはPINを入力した場合は、成功メッセージが表示されます。
   - 「いいえ」の場合は、[証明書(Certificate)]リストから証明書を選択します。
     選択した証明書に関する情報が[証明書(Certificate)]リストの下に表示されます。
6. [OK]をクリックします。

複合スキャン設定での証明書の更新

複合スキャン設定には、暗号化された証明書データを格納するBINファイルが含まれています。複合スキャン設定でクライアント証明書を置換または更新する必要がある場合は、更新したPFXファイルまたはP12ファイルを、複合設定のZIPファイル内のcertificatesディレクトリに配置できます。OpenText DASTで設定を開くと、まずPFXファイルとP12ファイルの有無がチェックされます。どちらも存在しない場合、BINファイルが復号化されて使用されます。複合設定の詳細については、"アプリケーション設定: 全般" ページ480を参照してください。

クライアント証明書を置換または更新するには、次の手順を実行します。

1. 複合スキャン設定のZIP内のcertificatesディレクトリで、暗号化されたBINファイルを見つけます。ファイル名はGUIDで、次のようになります。

   `<your-scansettings.zip>\certificates\0b627638-efda-4d01-a83e-80ee3a79b4cf.bin`

   注記: Windowsにおけるデフォルトの設定ファイルの場所は、`C:\ProgramData\HP\HP WebInspect\Settings\`です。

2. 更新したPFXファイルまたはP12ファイルを同じディレクトリに配置します。
3. PFXファイルまたはP12ファイルの名前をBINファイルと同じ名前に変更します。前の例を使用すると、ファイル名は次のようになります。

   `0b627638-efda-4d01-a83e-80ee3a79b4cf.pfx`

   – または –

   `0b627638-efda-4d01-a83e-80ee3a79b4cf.p12`

   重要! {/b}必ず元のファイル拡張子を保持してください。

4. 必要に応じて、暗号化された証明書を設定に保持する場合は、設定を再度保存します。BINファイルには、更新されたPFX証明書またはP12証明書が反映されます。PFX証明書またはP12証明書がZIPから削除されます。

ヒント: PFX証明書およびP12証明書では、多くの場合、パスワードが必要です。次のいずれかのオプションを使用して、設定のパスワードを指定します。

- PFX証明書またはP12証明書を作成するときに空のパスワードを設定し、それを設定のZIPファイルに配置します。
- PFX証明書またはP12証明書のパスワードを保持し、`settings.json`ファイルを編集して、次のようにCertificatePinの値としてパスワードを設定します。

  `"CertificatePin": "<password>"`

OpenText DASTツール用のプロキシ設定ファイルの編集

プロキシが組み込まれたツール(具体的には、Web Macro Recorder、Web Proxy、およびWeb Form Editor)を使用している場合は、証明書が必要な場合でもクライアント証明書を要求しないサーバに遭遇することがあります。この状況に対応するには、次のタスクを実行して`SPI.Net.Proxy.Config`ファイルを編集する必要があります。

タスク1: 証明書のシリアル番号を探す

1. Microsoft Edgeブラウザを開きます。
2. 「Internet Explorerとの互換性」に関する設定を探し、必要に応じて設定を有効にします。
3. [**インターネットオプション(Internet Options)**]を選択します。
4. [インターネットオプション]ウィンドウで、[**コンテンツ**]タブを選択し、[**証明書**]をクリックします。
5. [証明書]ウィンドウで、証明書を選択して、[**表示**]をクリックします。

6. [証明書]ウィンドウで、 [詳細]タブをクリックします。
7. [シリアル番号]フィールドをクリックし、下側のペインに表示されるシリアル番号をコピーします(数字を強調表示して、<Ctrl>を押しながら<C>を押します)。
8. すべてのウィンドウを閉じます。

タスク2: SPI.Net.Proxy.Configファイルでエントリを作成する

1. `SPI.Net.Proxy.Config`をファイル編集用に開きます。デフォルトの場所は`C:\Program Files\Fortify\Fortify WebInspect`です。
2. ClientCertificateOverridesセクションで、次のエントリを追加します。

   ```
   <ClientCertificateOverride HostRegex="RegularExpression"
   CertificateSerialNumber="Number" />
   ```

   ここで:

   RegularExpressionは、ホストURLと一致する正規表現です(例: `.*austin\.spidynamics\.com`)。

   Numberは、タスク1で取得したシリアル番号です。
3. 編集したファイルを保存します。

マクロ検証を有効にする(Enable macro validation)

ほとんどのダイナミックなアプリケーションスキャンでは、アプリケーションのあらゆる側面を明らかにするためにユーザ認証が必要です。ログインマクロでアプリケーションにログインできなかった場合は、スキャン品質が低下します。スキャンの前にログインマクロの品質を測定すれば、低品質のスキャンを回避できます。

[**マクロ検証を有効にする(Enable Macro Validation)**]を選択して、OpenText DASTがスキャンの開始時点でのマクロ動作の矛盾をテストできるようにします。実行された特定のテストの詳細については、"ログインマクロのテスト" ページ546を参照してください。

フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)

この種のマクロは、主にWebフォーム認証に使用されます。誤ってアプリケーションからログアウトした場合に、OpenText DASTが途中で終了するのを防ぐロジックが組み込まれています。この種のマクロを記録する場合は、必ずアプリケーションのログアウト署名を指定してください。省略記号ボタン…をクリックしてマクロを探します。 [**記録(Record)**]をクリックしてマクロを記録します。

注記: ガイド付きスキャンの場合は、ログインマクロを記録するための別のステージが含まれているため、 [記録(Record)]ボタンを使用できません。

ログインマクロパラメータ

このセクションは、 **[フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)]**を選択し、選択または作成したマクロにユーザ名とパスワードのパラメータが指定されたフィールドが含まれている場合にのみ表示されます。

ユーザ名とパスワードのパラメータを含むマクロを使用してスキャンを開始した場合は、これらのエントリに関連付けられた入力要素を含むページをスキャンすると、OpenText DASTがここで指定されたユーザ名とパスワードに置き換えます。この機能により、独自のユーザ名とパスワードを使用してマクロを作成することができますが、このマクロを使用して他のユーザがスキャンを実行すると、その人のユーザ名とパスワードが置き換えられる可能性があります。このことは、2要素認証スキャンで使用される電話番号、電子メール、および電子メールパスワードのパラメータにも適用されます。

Web Macro Recorderで値がマスクされたパラメータがマクロで使用されている場合、OpenText DASTで基本スキャンまたはガイド付きスキャンを設定するときにも、それらの値はマスクされます。

Webマクロレコーダを使用してパラメータを作成する方法の詳細については、『OpenText™ Dynamic Application Security Testingツールガイド』のWebマクロレコーダに関する章を参照してください。

起動マクロを使用する(Use a startup macro)

この種のマクロは、アプリケーションの特定のサブセクションに焦点を当てるために最もよく使用されます。OpenText DASTがそのエリアへのナビゲートに使用するURLを指定します。また、ログイン情報が含まれている場合がありますが、OpenText DASTがアプリケーションからログアウトできないようにするロジックは含まれていません。OpenText DASTは、マクロ内のすべてのURLにアクセスして、ハイパーリンクを収集し、データ階層をマッピングします。その後で、開始URLを呼び出し、通常のWeb探索(およびオプションで監査)を開始します。省略記号ボタン …をクリックしてマクロを探します。 **[記録(Record)]**をクリックしてマクロを記録します。

マルチユーザログイン(Multi-user login)

[マルチユーザログイン(Multi-user Login)]オプションを使用すると、ログインマクロ内のユーザ名とパスワードをパラメータ化してから、スキャンで使用する複数のユーザ名とパスワードのペアを定義できます。2要素認証が必要な場合は、電話番号、電子メール、および電子メールパスワードをパラメータ化することもできます。このアプローチを使用すると、複数のスレッドでスキャンを実行できます。スレッドごとにログインセッションが異なるため、スキャン時間が短縮されます。

重要! {/b}マルチユーザログインを使用するには、まず、 **[フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)]**を選択し、新しいマクロを記録するか、使用する既存のマクロを選択する必要があります。「"フォーム認証にログインマクロを使用する(Use a login macro for forms authentication)" 前のページ」を参照してください。

複数のユーザログインを使用してスキャンを実行するには:

1. [**マルチユーザログイン(Multi-user Login)**]チェックボックスをオンにします。

   注記: スキャンを実行する前に[マルチユーザログイン(Multi-user Login)]チェックボックスをオフにすると、スキャン中に追加の資格情報が使用されません。OpenText DASTは、ログインマクロに記録されたオリジナルの資格情報のみを使用します。

2. 次の表の説明に従って操作を進めます。

目的...	その場合...
ユーザの資格情報を追加する	a. [マルチユーザログイン(Multi-user Login)]で、[**追加(Add)**]をクリックします。 [マルチユーザ資格情報入力(Multi-user Credential Input)]ダイアログボックスが表示されます。 b. [**ユーザ名(Username)**]フィールドに、ユーザ名を入力します。 c. [**パスワード(Password)**]フィールドに、対応するパスワードを入力します。 d. オプションで、2要素認証が必要な場合は、次の基準を追加します。 ◦ **電話番号(Phone Number)** -ユーザ名に対応する電話番号(SMS応答を受信するため) ◦ **電子メール(Email)** -ユーザ名に対応する電子メールアドレス(電子メール応答を受信するため) ◦ **電子メールパスワード(Email Password)** -電子メールアドレスのパスワード(電子メール応答を受信するため) e. [**OK**]をクリックします。 f. 追加するユーザログインごとにステップa-eを繰り返します。 重要! {/b}共有リクエスタスレッドの数が、設定されたユーザの数を超えないようにする必要があります。有効なユーザを持たないリクエスタスレッドでは、スキャンの実行時間が長くなります。複数のユーザを設定する場合は、最初のユーザとして、パラメータ化されたマクロ内のオリジナルのユーザ名とパスワードをカウントすることを忘れないでください。詳細については、「"スキャン設定:リクエスタ" ページ414」を参照してください。
ユーザの資格情報を編集する	a. [マルチユーザログイン(Multi-user Login)]で、テーブル内のエントリを選択し、[**編集(Edit)**]をクリックします。

目的...	その場合...
	[マルチユーザ資格情報入力(Multi-user Credential Input)]ダイアログボックスが表示されます。 b. 必要に応じて資格情報を編集します。 c. [OK]をクリックします。
ユーザの資格情報を削除する	a. [マルチユーザログイン(Multi-user Login)]で、削除するテーブル内のエントリを選択します。 b. [削除(Delete)]をクリックします。

詳細については、「"マルチユーザログインスキャン" ページ218」を参照してください。

OAuth 2.0のBearer資格情報の設定

Open Authorization (OAuth) 2.0は、サービスまたはアプリケーション間で認証トークンを共有し、ユーザの身元を証明するオープン標準の認証プロトコルです。 [オープン認証の設定(Open Authorization Configuration)]ダイアログでは、以下のタイプのOAuth 2.0認証フローを設定できます。

- **クライアント資格情報の付与(Client Credentials Grant)** - クライアントは、保護されたリソースへのアクセスを要求する際に、クライアントIDやクライアントシークレットなどのクライアント資格情報を使用します。
- **パスワード資格情報の付与(Password Credentials Grant)** - クライアントは、通常、対話形式を使用して、ユーザ名やパスワードなどのリソース所有者の資格情報を取得します。

OAuth 2.0認証を設定すると、OpenText DASTは取得したトークンをスキャン全体にわたって使用します。トークンの有効期限が切れた場合は更新されます。

[オープン認証の設定(Open Authorization Configuration)]ダイアログでOAuth 2.0認証を設定するには、以下の手順を実行します。

1. [**OAuthフロー(OAuth flows)**]リストで、フローを選択します。オプションは、**[クライアント資格情報の付与(Client Credentials Grant)]**および**[パスワード資格情報の付与(Password Credentials Grant)]**です。
2. **[アクセストークンURL(Access Token URL)]**ボックスに、トークンの生成に使用するURL (`https://<yourDomain>/oauth2/token`など)を入力します。
3. 必要に応じて、サービスがOAuthフローに対して異なる複数のスコープ(または許可)をサポートしている場合は、**scope**パラメータの値ボックスをダブルクリックし、使用するスコープを指定します。

   ヒント: パラメータが不要な場合は、値を空のままにするか、パラメータ行を選択して**削除**キーを押します。

4. 次の表に従って、認証要求ヘッダに含める情報を入力します。

設定する対象...	その場合...
[クライアント資格情報の付与(Client Credentials Grant)]フロー	a. **client_id**パラメータの値ボックスをダブルクリックし、アプリケーション(クライアント)IDを入力します。 b. **client_secret**パラメータの値ボックスをダブルクリックし、OAuthプロバイダの登録ポータルでアプリケーション用に生成したクライアントシークレットを入力します。
[パスワード資格情報の付与(Password Credentials Grant)]フロー	a. **username**パラメータの値ボックスをダブルクリックし、ユーザ名を入力します。 b. **password**パラメータの値ボックスをダブルクリックし、パスワードを入力します。

ヒント: 必要に応じて、空の行をダブルクリックして、カスタムパラメータ名と値を追加することもできます。ただし、次の制限に注意してください。

- パラメータ名`grant_type`と`scope`は予約済みであり、カスタムパラメータでは使用できません。
- [OAuthフロータイプ(OAuth Flow Type)]が[クライアント資格情報の付与(Client Credentials Grant)]の場合、カスタムパラメータで`client_credentials`、`client_id`、および`client_secret`は使用できません。
- [OAuthフロータイプ(OAuth Flow Type)]が[パスワード資格情報の付与(Password Credentials Grant)]の場合、カスタムパラメータで`username`および`password`は使用できません。

5. デフォルトでは、OpenText DASTはログアウト署名にステータスコード403を使用します。必要に応じて、カスタムステータスコードを使用する場合は、ログアウト署名を示すために、**[ログアウト署名(Logout Signature)]**ボックスにステータスコードまたは正規表現を入力します。次の構文を使用します。

   `[STATUSCODE]<Number>`

6. 必要に応じて、**[テスト(Test)]**をクリックして、サーバへのアクセスと、bearerトークンの受信をテストします。

   注記: bearerトークンを表示したり、エラーを表示したりするには、[テスト結果(Test Results)]ダイアログで**[詳細の表示(Show Details)]**をクリックします。詳細に表示される**[有効期限(Expires In)]**の値は、トークンの有効期間を示しています。有効期限が切れると、トークンは更新されます。

7. **[OK]**をクリックします。

スキャン設定:ファイルが見つからない

この機能にアクセスするには、**[編集(Edit)]**メニューをクリックし、**[デフォルトのスキャン設定(Default Scan Settings)]**または**[現在のスキャン設定(Current Scan Settings)]**を選択します。その後で、**[スキャン設定(Scan Settings)]**カテゴリで、**[ファイルが見つからない(File Not Found)]**を選択します。

オプション

[ファイルが見つからない(File Not Found)]オプションについて、次の表で説明します。

オプション	説明
HTTP応答コードを使用してFNF(ファイルが見つからない)を判別する(Determine File Not Found (FNF) using HTTP response codes)	サーバからのfile-not-found応答を検出するためにHTTP応答コードを使用する場合は、このオプションを選択します。その後、次のカテゴリに適合するコードを特定できます。 • **強制有効応答コード(FNFは不可) (Forced Valid Response Codes (Never an FNF))**: file-not-found応答として扱うべきでないHTTP応答コードを指定できます。 • **強制FNF応答コード(常にFNF)**: 常にfile-not-found応答として扱われるHTTP応答コードを指定します。OpenText DASTは応答の内容を処理しません。 1つの応答コードまたは応答コードの範囲を入力します。範囲には、ダッシュまたはハイフンを使用して、リスト内の最初と最後のコードを区切ります(たとえば、400-404)。複数のコードまたは範囲を指定するには、各エントリをカンマで区切ります。
カスタム提供の署名からFNFを判別する(Determine FNF from custom supplied signature)	このエリアを使用して、会社が使用するカスタムの404ページ通知に関する情報を追加します。404エラーが発生した場合に別のページを表示するように会社が設定している場合は、その情報をここに追加します。サイト固有の404ページからの誤検出がOpenText DASTで発生する可能性があります。
FNFページの自動検出(Auto detect FNF page)	存在しないリソースをクライアントが要求すると、一部のWebサイトではステータス「404 Not Found」を返しません。代わりに、「200 OK」というステータスが返されることがありますが、ファイルが見つからないというメッセージが応答に含まれているか、ホームページやログインページにリダイレクトされる場合があります。OpenText DASTでこれらの「カスタム」のfile-not-foundページを検出するには、このチェックボックスを選択します。

オプション	説明
	OpenText DASTは、サーバ上に存在できない可能性があるリソースに対する要求を送信することによって、カスタムのfile-not-foundページの検出を試みます。続いて、各応答を比較し、応答間で異なるテキストの量を測定します。たとえば、このタイプのほとんどのメッセージは、要求されたリソースの名前が異なる可能性があることを除けば、同じ内容です(「お探しのページは見つかりませんでした(Sorry, the page you requested was not found)」など)。 [**FNFページの自動検出(Auto detect FNF page)**]チェックボックスを選択した場合、同じでなければならない応答コンテンツの割合を [**一致するFNFページ(Match FNF page with)**]フィールドに指定できます。デフォルトは90%です。

スキャン設定:ポリシー

この機能にアクセスするには、 [**編集(Edit)**]メニューをクリックし、 [**デフォルトのスキャン設定(Default Scan Settings)**]または [**現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、 [**スキャン設定(Scan Settings)**]カテゴリで、 [**ポリシー(Policy)**]を選択します。

スキャンウィザードを使用してスキャンを開始するときに別のポリシーに変更できますが、代わりのものを選択しない場合は、ここで選択したポリシーが使用されます。また、スキャン中にセンサによって集約される複数のポリシーを選択することも可能です。ポリシーの詳細については、「"OpenText DAST ポリシー" ページ509」を参照してください。

カスタムポリシーを作成、インポート、または削除することもできます。

1つ以上のポリシーの選択

別のポリシーを選択するには:

1. [**監査ポリシー(Audit Policies)**]リストで、選択済みのポリシーのトグルを無効の位置にスライドします。
2. 目的のポリシーのトグルを有効の位置にスライドします。
3. [**OK**]をクリックします。

追加のポリシーを選択するには、次の方法を実行します。

1. [**監査ポリシー(Audit Policies)**]リストで、目的のポリシーのトグルを有効の位置にスライドします。
2. [**OK**]をクリックします。

ポリシーの作成

ポリシーを作成するには:

1. [**作成(Create)**]をクリックします。
   Policy Managerツールが開きます。
2. [**ファイル(File)**]メニューから[**新規(New)**]を選択します(または[新しいポリシー(New Policy)]アイコンをクリックします)。
3. 新しいポリシーのモデルにするポリシーを選択します。
4. 追加の手順については、Policy Managerのドキュメントを参照してください。

ポリシーの編集

ポリシーを編集するには:

1. カスタムポリシーを選択します。

   注記: カスタムポリシーのみを編集できます。

2. [**スキャンポリシーの編集(Edit Scan Policy)**]をクリックします。
   Policy Managerツールが開きます。
3. 追加の手順については、Policy Managerのドキュメントを参照してください。

ポリシーのインポート

ポリシーをインポートするには:

1. [**インポート(Import)**]をクリックします。
2. [カスタムポリシーのインポート(Import Custom Policy)]ウィンドウで、省略記号ボタン  をクリックします。
3. 標準のファイル選択ウィンドウの[**ファイルの種類**]リストを使用して、以下のポリシータイプから選択します。
   - ポリシーファイル(*.policy): OpenText DAST用に設計および作成されたポリシーファイル。
   - すべてのファイル(*.*): ポリシー以外のファイルを含む、任意のタイプのファイル。
4. [**OK**]をクリックします。

ポリシーのコピーがPoliciesフォルダに作成されます(デフォルトの場所は、`C:\ProgramData\HP\HP WebInspect\Policies\`)。そのポリシーとその有効化されたチェックはすべて、指定したポリシー名を使用してSecureBaseにインポートされます。カスタムエージェントはインポートされません。

ポリシーの削除

ポリシーを削除するには:

1. カスタムポリシーを選択します。

   注記: カスタムポリシーのみを削除できます。

2. [**スキャンポリシーの削除(Delete Scan Policy)**]をクリックします。
   確認メッセージが表示されます。
3. [**Yes**]をクリックします。
   ポリシーがPoliciesディレクトリから削除されます。

スキャン設定:ユーザエージェント

この機能にアクセスするには、[**編集(Edit)**]メニューをクリックし、[**デフォルトのスキャン設定(Default Scan Settings)**]または[**現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、[**スキャン設定(Scan Settings)**]カテゴリで、[**ユーザエージェント(User Agent)**]を選択します。

OpenText DASTとイベントベースのWebマクロレコーダの両方で同期するユーザエージェント設定を行えます。

プロファイルおよびユーザエージェント文字列

ブラウザのユーザエージェント文字列を指定する定義済みのプロファイルを選択できます。次の表に、使用可能なプロファイルを示します。

プロファイル(Profile)	ユーザエージェント文字列
デフォルト(Default)	`Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:110.0) Gecko/20100101 Firefox/110.0`
Google Chrome (Windows)	`Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36`
Microsoft Edge (Windows)	`Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 Edg/133.0.0.0`

プロファイル (Profile)	ユーザエージェント文字列
Safari (macOS)	`Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.3 Safari/605.1.15`
Googlebot 2.1	`Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)`
Bingbot	`Mozilla/5.0 (compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)`
Yahoo!Slurp	`Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)`
Safari (iOS)	`Mozilla/5.0 (iPhone; CPU iPhone OS 18_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.3 Mobile/15E148 Safari/604.1`
Safari (iPadOS)	`Mozilla/5.0 (iPad; CPU OS 18_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.3 Mobile/15E148 Safari/604.1`
Google Chrome (Android)	`Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Mobile Safari/537.36`
カスタム (Custom)	ユーザ指定。 **注記:** Internet Explorer 6、Internet Explorer 7、Internet Explorer 8、iPhone、iOS 14.3など、削除された以前のバージョンのOpenText DASTのユーザエージェントは、既存のスキャンではカスタムプロファイルと見なされます。 重要! {/b}OpenTextでは、上級ユーザのみがカスタムプロファイルを指定することを推奨しています。

ナビゲータインターフェイス設定

ナビゲータインタフェース設定は、レガシWebアプリケーションがブラウザ検出を容易にするために使用する情報を提供します。ブラウザ固有の動作が必要な場合は、これらの設定をカスタマイズできます。次の表で、各ユーザエージェントプロファイルのこれらの設定について説明します。

プロファイル (Profile)	appName	appVersion	プラットホーム[1]
デフォルト (Default)	Netscape	5.0 (Windows)	Win64
Google Chrome (Windows)	Netscape	5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36	Win32
Microsoft Edge (Windows)	Netscape	5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 Edg/133.0.0.0	Win32
Safari (macOS)	Netscape	5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.3 Safari/605.1.15	MacIntel
Googlebot 2.1	N/A	N/A	N/A
Bingbot	N/A	N/A	N/A
Yahoo! SlurpSlurp	N/A	N/A	N/A
Safari (iOS)	Netscape	5.0 (iPhone; CPU iPhone OS 18_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.3 Mobile/15E148 Safari/604.1	iPhone
Safari (iPadOS)	Netscape	5.0 (iPad; CPU OS 18_3 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.3 Mobile/15E148 Safari/604.1	iPad

1ブラウザは空の文字列またはブラウザが実行されているプラットフォームを表す文字列を返します。

プロファイル (Profile)	appName	appVersion	プラットホーム[1]
Google Chrome (Android)	Netscape	5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Mobile Safari/537.36	Linux armv81

1ブラウザは空の文字列またはブラウザが実行されているプラットフォームを表す文字列を返します。

第7章:Web探索設定

この章では、OpenText DAST Web探索プログラムで使用されるWeb探索設定について説明します。OpenText DAST Web探索プログラムは、Webサイト全体のハイパーリンクをたどり、ページを取得してインデックスを付け、サイトの階層構造を文書化するように設計されたソフトウェアプログラムです。OpenText DASTがサイトをWeb探索する方法を制御するパラメータは、[Web探索設定(Crawl Settings)]リストから選択できます。

Web探索設定:リンク解析

この機能にアクセスするには、[**編集(Edit)**]メニューをクリックし、[**デフォルトのスキャン設定(Default Scan Settings)**]または[**現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、[**Web探索設定(Crawl Settings)**]カテゴリで、[**リンク解析(Link Parsing)**]を選択します。

OpenText DASTは、HTMLによって定義されたハイパーリンク(`<a href>`タグを使用)とスクリプト(JavaScriptとVBScript)によって定義されたすべてのハイパーリンクをたどります。ただし、リンクの指定に別の構文を使用する他の通信プロトコルに遭遇する場合があります。このような場合に対応するために、カスタムリンク機能と正規表現を使用して、OpenText DASTにたどらせるリンクを識別できます。これらは特殊リンク識別子と呼ばれています。

特殊リンク識別子の追加

特殊リンク識別子を追加するには:

1. [**追加(Add)**]をクリックします。
   [特殊リンク入力(Specialized Link Entry)]ウィンドウが開きます。
2. [**特殊リンクパターン(Specialized Link Pattern)**]ボックスに、リンクを識別するために設計された正規表現を入力します。
3. (オプション)[**コメント(Comment)**]ボックスにリンクの説明を入力します。
4. [**OK**]をクリックします。

Web探索設定:リンクソース

この機能にアクセスするには、[**編集(Edit)**]メニューをクリックし、[**デフォルトのスキャン設定(Default Scan Settings)**]または[**現在のスキャン設定(Current Scan Settings)**]を選択します。その後で、[**Web探索設定(Crawl Settings)**]カテゴリで、[**リンクソース(Link Sources)**]を選択します。

リンク解析とは

OpenText DAST Web探索プログラムは、開始URLに要求を送信し、応答の内容からリンク(URL)を再帰的に解析します。これらのリンクは作業キューに登録され、キューが空になるまでWeb探索プログラムが繰り返し実行されます。HTTP応答からリンク情報を抽出するために使用される技術は、総称して「リンク解析」と呼ばれています。Web探索プログラムでリンク解析を実行する方法には、パターンベースとDOMベースの2つの選択肢があります。

パターンベースの解析

パターンベースのリンク解析では、テキスト検索とパターンマッチングを組み合わせてURLが検索されます。これらのURLには、<A>要素など、ブラウザによってレンダリングされる通常のコンテンツだけでなく、追加のサイト構造を明らかにする可能性がある不可視テキストも含まれます。

このオプションは、OpenText DASTバージョン10.40以前のデフォルトの動作と一致します。これは、WebサイトをWeb探索するためのより積極的なアプローチであり、スキャンの実行により多くの時間がかかる可能性があります。この積極的な動作のせいで、実際のサイトコンテンツを表すものではない余分なリンクがWeb探索プログラムで多数作成されることがあります。このような状況では、DOMベースの解析によって誤検出を減らしてサイトのURLコンテンツを明らかにできるはずです。

注記: [パターンベースの解析(Pattern-based Parsing)]を選択すると、リンクを検索するためのDOMベースの解析技術がすべて使用されます。ただし、パターンベースの解析では、リンクソースのメタデータを計算することができません。DOMベースの解析では、この情報を計算することができるため、よりインテリジェントな解析が可能になります。また、DOMベースの解析では、使用する解析技術をより細かく制御できます。

DOMベースの解析

ドキュメントオブジェクトモデル(DOM)は、HTMLドキュメントとXMLドキュメントの定義と構築、その構造のナビゲート、およびその要素とコンテンツの編集を行う論理構造を提供するプログラミング概念です。

HTMLページのグラフィカルな表現をDOMで示すと、上下逆さまのツリーのようになります。HTMLノードに端を発するツリー構造の分岐にタグ、サブタグ、およびコンテンツが組み込まれます。この構造をDOMツリーと呼びます。

OpenText DASTではDOMベースの解析を使用してHTMLページをDOMツリーとして解析します。解析された詳細な構造を使用することで、ハイパーリンクのソースを特定する際の忠実性と信頼性を向上させます。DOMベースの解析で誤検出を減らすことができ、「積極的なリンク検出」の度合いも減る可能性があります。

一部のサイトではWeb探索プログラムが不良リンクを繰り返し要求し、応答の内容にこれらのリンクがエコーバックされます。場合によっては、問題を悪化させる余分のテキストが追加されます。このような「不良リンクインと不良リンクアウト」の反復サイクルが原因で、スキャンが長時間実行されたり、まれに、永久に実行されたりする可能性があります。DOMベースの解析

とリンクソースの慎重な選択によって、この暴走スキャン動作を制限するメカニズムが提供されます。Webアプリケーションはそれぞれ構造や内容が異なるため、リンクソース設定を最適なものとするには実験が必要です。

DOMベースの解析を改善するには、リンクの検索に使用する技術を選択します。サイトに関係ない技術を取り除くことでスキャンの完了に要する時間が短くなる可能性があります。ただし、より徹底的なスキャンを行う場合は、すべての技術を選択するか、パターンベースの解析を使用します。DOMベースの解析技術の説明を次の表に示します。詳細については、「"リンクソース設定の制限" ページ464」を参照してください。

技術	説明
コメントリンクを含める(積極的)(Include Comment Links (Aggressive))	プログラマは、自分のために、リンクを含むメモをHTMLコメント内部に残す場合があります。このリンクはサイト上に表示されませんが、攻撃者によって発見される可能性があります。このオプションは、HTMLコメント内部のリンクを検索する場合に使用します。OpenText DASTが見つけるリンクは増えますが、これらのリンクは必ずしも有効なURLとは限らず、Web探索プログラムは存在しないコンテンツへのアクセスを試みる場合があります。同じリンクが各ページに置かれていることや、それらが相対リンクであることもあり、結果としてURLカウントが指数関数的に増加して、スキャン時間が長くなる可能性があります。
条件付きコメントリンクを含める(Include Conditional Comment Links)	条件付きコメントリンクは、要求を行うユーザエージェント(ブラウザのタイプとバージョン)に応じて、ページ上のHTMLが条件付きで包含または除外される場合に発生します。 **通常のコメントの例:** `<!—hidden.txt -->` **条件付きコメントの例:** `<!--[if lt IE9]>` `<script src="//www.somesite.com/static/v/all/js/html5sh.js"></script>` `<link rel="stylesheet" type"text/css" href='//www.somesite.com/static/v/fn-hp/css/IE8.css'>` `<![endif]-->` OpenText DASTは、HTMLコードを評価する際にブラウザの動作をエミュレートし、ユーザエージェントに応じてDOMの処理方法を変えます。あるユーザエージェントにとってコメント内のリンクであるものが、他のユーザエージェントにとっては通常のHTMLリンクになります。 このオプションは、ブラウザのバージョンに基づいてコメントアウトされるリンクなど、HTMLコマンド内部に存在する条件付きリンクを検索する場合に使用します。これらの条件付きステートメントには、スクリプト解析が有効になっている場合に実行する必要があるスクリプトインクルードも含めることができます。これらのリンクのWeb探索はより徹底的なものになりますが、ス

技術	説明
	キャン時間が増える可能性があります。加えて、このようなコメントは最新でなく、Web探索する意味がない場合があります。
プレーンテキストリンクを含める(Include Plain Text Links)	.txtファイル内のプレーンテキストやHTMLコード内部の段落を、`http://www.something.com/mypage.html`のようにURLとして書式設定できます。ただし、これは単なるテキストであって真のリンクではないため、ブラウザはこれをリンクとしてレンダリングせず、そのテキストは機能的にページの一部になりません。たとえば、コンテンツは、ユーザによってクリックされることを想定していない偽の構文を使用してHTMLでコーディングする方法を記述したページの一部である可能性があります。このオプションは、OpenText DASTがこれらのテキストリンクを解析して、Web探索用のキューに登録する場合に使用します。 また、スマートパターンの一致を使用して、OpenText DASTは、.css、.js、.bmp、.png、.jpg、.htmlなどの一般的なファイル拡張子を識別し、これらのファイルをWeb探索キューに登録できます。プレーンテキストで参照されたこれらのファイルを監査すると、誤検出が発生する可能性があります。
スタティックスクリプトブロック内のリンクを含める(Include Links in Static Script blocks)	このオプションは、OpenText DASTが開始スクリプトタグと終了スクリプトタグの内側でリンクに見えるテキストを調査する場合に使用します。有効なリンクがこれらのスクリプトブロック内で見つかる場合もありますが、開発者が開始スクリプトタグと終了スクリプトタグの内側にリンクに似たテキストを含むコメントを残すこともあります。例: `<script type="text/javascript">` `// go to http://www.foo.com/blah.html for help` `var url = "http:www.foo.com/xyz/" + path + "?help"` `</script>` 加えて、これらのタグの内側のJavaScriptコードがスキャン中にJavaScript実行エンジンによって処理される可能性があります。ただし、上記の例の「var url」のように変数を設定するコード行内のスタティックリンクを検索すると、それらの部分パスがWeb探索用のキューに登録されたときに問題が発生する可能性があります。変数に「foo.html」などの一般的な拡張子を持つ相対リンクが含まれている場合は、Web探索プログラムによって、そのコード行を含むすべてのページの末尾に拡張子が付加されます。これにより、使用できないURLが生成され、誤検出が発生する可能性があります。
URLに埋め込まれたURLを解析する(Parse	このオプションは、OpenText DASTがhref属性内部に存在するすべてのテキストを解析して、Web探索キューに登録する場合に使用します。URLに埋め込まれたURLの例を次に示します。 `<a`

技術	説明
URLs Embedded in URLs)	`href="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />` ただし、一部のサイトでは、「ファイルが見つからない」ページでフォームアクションタグに入れてURLが返され、次のようにそのURLがオリジナルのURLに付加されます。 `<form action="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />` その後、OpenText DASTは、フォームアクションを要求し、もう一度「ファイルが見つからない」応答を受け取ります。ここでも、次に示すように、URLがフォームアクションに追加されます。 `<form action="http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah? http://www.foo.com/xyz/bar.html?url=http%3A%2F%2Fwww.zzzz.com%2Fblah" />` このようなサイトでは、これらのURLによって引き続き「ファイルが見つからない」応答が生成され、さらに多くのURLがWeb探索キューに登録されます。その結果、無限のWeb探索ループが発生します。この種のURLをWeb探索キューに登録しないようにするには、このオプションを使用しないでください。
ルート化されていないURLを許可する(Allow Un-rooted URLs) (上記の項目に対して)	このオプションは、前述の5つのオプションの動作を変更します。URLによっては、httpなどの特定のスキームが含まれておらず、完全修飾ドメイン名でないものがあります。`xyz.html`のようなこれらのURLは、アンカーなしまたは「ルート化なし」と見なされます。これは、ルートされていないURLが要求に対して相対的であることが前提です。 たとえば、完全修飾されていないURL `<a href='foo.html' />`にはスキームが含まれていません。このURLでは、コンテキストURLのスキームが使用されます。HTTPSページがコンテンツの取得を要求すると、HTTPSがURLの前に付加されます。 このオプションは、ルート化されていないURLをリンクとして解析時に扱う場合に使用します。このオプションを選択すると、スキャンがより徹底的で積

技術	説明
	極的になりますが、完了にはかなり長い時間がかかる可能性があります。 **URLのサンプルと解析結果** 次のサンプルでは、さまざまなURLと、それらがWeb探索中に解析される方法について説明します。 **通常のURL** 次の要求内のURLには、前方(またはアンカー)スラッシュが含まれています。 リクエスト元: `http://www.foo.com/x/y/z/` 対象: `<a href='/bar.html' />` 結果のリンク先: `http://www.foo.com/bar.html`。 **ルート化されていないシンプルなURL** 次の要求内のURLは、前方スラッシュが含まれていないため、ルート化されません。 リクエスト元: `http://www.foo.com/` 対象: `<a href='bar.html' />` 結果のリンク先: `http://www.foo.com/bar.html`。 **ルート化されていない長いURL** 次の要求は、ルート化されていない長いURLを示しています。 リクエスト元: `http://www.foo.com/x/y/z/` 対象: `<a href='bar.html' />` 結果のリンク先: `http://www.foo.com/x/y/z/bar.html`。 **コード内のコメント** `<!-- baz_ads.js -->`などのコメントが、コード内のスクリプトインクルードの前に含まれている場合があります。次の要求は、積極的なWeb探索中にこのコメントがどのように解釈されるかを示しています。 リクエスト元: `http://www.foo.com/x/y/z/` 対象: `<!-- baz_ads.js -->` 結果のリンク先 `http://www.foo.com/x/y/z/baz_ads.js` マスタページにこのコメントを含めた場合は、積極的なスキャン中に、サイト内のページ応答の多く(すべてではない)でコメントが検出されます。この設定では、暴走スキャンが発生する可能性があります。 マスタページ上のコメント`<!-- baz_ads.js -->`によって、次のような複数の

技術	説明
	リンクが作成されます。 `http://www.foo.com/baz_ads.js` `http://www.foo.com/x/baz_ads.js` `http://www.foo.com/x/y/baz_ads.js` `http://www.foo.com/x/y/z/baz_ads.js` (サイト内のすべてのページで同様です)。

フォームアクション、スクリプトインクルード、およびスタイルシート

フォームアクション、スクリプトインクルード、スタイルシートなどの一部のリンクタイプは、特殊で、他のリンクとは異なる方法で扱われます。サイトによっては、これらのリンクをWeb探索して解析する必要がない場合があります。ただし、あらゆるもののWeb探索と解析を試みる積極的なスキャンが必要な場合は、この目的を達成するために次のオプションが役に立ちます。詳細については、「"リンクソース設定の制限" ページ464」を参照してください。

注記: また、これらのオプションのそれぞれでルート化されていないURLを許可することもできます。このトピックの「ルート化されていないURLを許可する」を参照してください。

オプション	説明
フォームアクションリンクをWeb探索する(Crawl Form Action Links)	OpenText DASTは、Web探索中にHTMLフォームに遭遇すると、ユーザが行い得る入力のバリエーションを作成し、より多くのサイトコンテンツを収集するための要求としてフォームを送信します。たとえば、POSTメソッドを使用したフォームの場合は、OpenText DASTが代わりにGETを使用して情報を公開することもできます。この種のWeb探索に加えて、このオプションは、OpenText DASTがフォームターゲットを通常のリンクとして扱う場合に使用します。
スクリプトインクルードリンクをWeb探索する(Crawl Script Include Links)	スクリプトインクルードは、.jsファイルからJavaScriptをインポートして、現在のページで処理されます。このオプションは、OpenText DASTが.jsファイルをリンクとしてWeb探索する場合に使用します。
スタイルシートリンクをWeb探索する(Crawl Stylesheet Links)	スタイルシートリンクは、.cssファイルからスタイル定義をインポートして、現在のページにレンダリングします。このオプションは、OpenText DASTが.cssファイルをリンクとしてWeb探索する場合に使用します。

その他のオプション

次の追加オプションは、サイトのリンク解析を改善するのに役立つ場合があります。詳細については、「"リンクソース設定の制限" 次のページ」を参照してください。

オプション	説明
FNFページ上のリンクをWeb探索する(Crawl Links on FNF Pages)	このオプションを選択すると、OpenText DASTは「ファイルが見つからない」とマークされた応答のリンクを検索し、Web探索を行います。 このオプションは、スキャンモードが「Web探索のみ(Crawl Only)]または「Web探索および監査(Crawl & Audit)]に設定されている場合はデフォルトで選択されます。このオプションは、スキャンモードが「監査のみ(Audit Only)]に設定されている場合は利用できません。
反復パスセグメントを使用してURLを抑止する(Suppress URLs with Repeated Path Segments)	多くのサイトには、相対パスのようでありながら、OpenText DASTによる解析と、Web探索対象のURLへの追加が済むと、使用不能なURLになるテキストがあります。こうしたものの出現は、パスが連続して追加される場合(`/foo/bar/foo/bar/`など)に、暴走スキャンになるおそれがあります。こうしたものの出現を減らす上でこの設定は役に立ち、デフォルトで有効になっています。 この設定が**有効**な場合、次のオプションがあります。 **1** - URL内のどこかで繰り返されている単一のサブフォルダを検出し、一致がある場合はそのURLを拒否します。たとえば、`/foo/baz/bar/foo/`では「`/foo/`」が繰り返されているので一致します。この繰り返しは隣接している必要はありません。 **2** -隣接するサブフォルダの2つ以上のペアを検出し、一致がある場合はURLを拒否します。たとえば、`/foo/bar/baz/foo/bar/`では「`/foo/bar/`」が繰り返されているので一致します。 **3** -隣接する3つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。 **4** -隣接する4つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。 **5** -隣接する5つのサブフォルダの2つ以上のセットを検出し、一致がある場合はURLを拒否します。 この設定が**無効**な場合、サブフォルダの繰り返しは検出されず、一致が原因でURLが拒否されることはありません。

リンクソース設定の制限

リンクソースのチェックボックスをオフにすると、スタティック解析を使用してその特定の種類のリンクが見つかったとき、Web探索プログラムで処理されません。ただし、これらのリンクは他の多くの方法で見つかる可能性があります。たとえば、 **[スタイルシートリンクをWeb探索する(Crawl Stylesheet Links)]**オプションをオフにしても、パスの切り捨ては制御されず、スクリプトエンジンから発行される.cssファイル要求は抑止されません。この設定をオフにすると、サーバからの.css応答のスタティックリンク解析が阻止されるに過ぎません。同様に、 **[スクリプトインクルードリンクをWeb探索する(Crawl Script Include Links)]**オプションをオフにしても、スクリプトエンジンから発行される.js、AJAX、frameIncludes、またはその他のファイル要求は抑止されません。したがって、リンクソースのチェックボックスをオフにしても、その種のリンクソースに対する普遍的なフィルタにはなりません。

チェックボックスをオフにする目的は、Web探索が大量の不良リンクでいっぱいになってスキャン時間が極端に長くなるのを防ぐことです。

Web探索設定: セッション除外

[スキャン設定-セッション除外(Scan Settings - Session Exclusions)]で指定した項目はすべて、 **[Web探索設定(Crawl Settings)]**と **[監査設定(Audit Settings)]**の両方の **[セッション除外(Session Exclusions)]**に自動的に複製されます。これらの項目は、灰色(黒色ではない)テキストで表示されます。これらのオブジェクトをWeb探索から除外しない場合は、 **[スキャン設定-セッション除外(Scan Settings - Session Exclusions)]**パネルからそれらを削除する必要があります。

このパネル(**[Web探索設定-セッション除外(Crawl Settings - Session Exclusions)]**)では、Web探索から除外する追加のオブジェクトを指定することができます。

除外または拒否するファイル拡張子

[拒否(Reject)]を選択した場合は、指定された拡張子を持つファイルが要求されません。

[除外(Exclude)]を選択した場合は、指定された拡張子を持つファイルが要求されますが、監査されません。

除外/拒否するファイル拡張子の追加

ファイル拡張子を追加するには:

1. **[追加(Add)]**をクリックします。
   [除外拡張子(Exclusion Extension)]ウィンドウが開きます。
2. **[ファイル拡張子(File Extension)]**ボックスに、ファイル拡張子を入力します。
3. **[拒否(Reject)]**と **[除外(Exclude)]**のどちらかまたは両方を選択します。
4. **[OK]**をクリックします。

除外MIMEタイプ

指定されたMIMEタイプに関連付けられたファイルが監査されません。

除外するMIMEタイプの追加

MIMEタイプを追加するには:

1. [**追加(Add)**]をクリックします。
   [除外するMimeタイプの指定(Provide a Mime-type to Exclude)]ウィンドウが開きます。
2. [**Mimeタイプの除外(Exclude Mime-type)**]ボックスに、MIMEタイプを入力します。
3. [**OK**]をクリックします。

その他の除外/拒否基準

HTTPメッセージのさまざまなコンポーネントを特定してから、そのコンポーネントを含むセッションを除外するか拒否するかを指定できます。

- **拒否(Reject)** - OpenText DASTは、指定されたホストまたはURLにHTTP要求を送信しません。たとえば、通常、サイトからのログオフを処理するURLは拒否する必要があります。これは、スキャンが完了する前にアプリケーションからログアウトしたくないためです。
- **除外(Exclude)** - Web探索中に、OpenText DASTは、指定されたURLまたはホストで他のリソースへのリンクを調査しません。スキャンの監査部分の間は、OpenText DASTは指定されたホストまたはURLを攻撃しません。HTTP応答を処理せずにURLまたはホストにアクセスする場合は、 [**除外(Exclude)**]オプションを選択しますが、 [**拒否(Reject)**]は選択しません。たとえば、処理しないURL上の壊れたリンクをチェックするには、 [**除外(Exclude)**]オプションだけを選択します。

デフォルトの基準の編集

デフォルトの基準を編集するには:

1. 基準を選択して、 [**編集(Edit)**]([**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。
   [ホストまたはURLの拒否または除外(Reject or Exclude a Host or URL)]ウィンドウが開きます。
2. [**ホスト(Host)**]または [**URL**]を選択します。
3. [**ホスト/URL(Host/URL)**]ボックスに、URLまたは完全修飾ホスト名、またはターゲットのURLまたはホストに一致するように設計された正規表現を入力します。
4. [**拒否(Reject)**]と [**除外(Exclude)**]のどちらかまたは両方を選択します。
5. [**OK**]をクリックします。

除外/拒否基準の追加

除外/拒否基準を追加するには:

1. [追加(Add)]([その他の除外/拒否基準(Other Exclusion/Rejection Criteria)]リストの右側にある)をクリックします。
   [除外の作成(Create Exclusion)]ウィンドウが開きます。
2. [ターゲット(Target)]リストから項目を選択します。
3. ターゲットとして[クエリパラメータ(Query Parameter)]または[ポストパラメータ(Post Parameter)]を選択した場合は、[ターゲット名(Target Name)]を入力します。
4. [一致タイプ(Match Type)]リストから、ターゲット内のテキストの一致に使用される方法を選択します。
   - [正規表現に一致(Matches Regex)] - [一致文字列(Match String)]ボックスで指定した正規表現に一致します。
   - [正規表現の拡張に一致(Matches Regex Extension)] - [一致文字列(Match String)]ボックスで指定したFortify正規表現の拡張から入手可能な構文に一致します。
   - [一致(Matches)] - [一致文字列(Match String)]ボックスで指定したテキスト文字列に一致します。
   - [含む(Contains)] - [一致文字列(Match String)]ボックスで指定したテキスト文字列を含みます。
5. [一致文字列(Match String)]ボックスに、ターゲットで検索する文字列または正規表現を入力します。または、[一致タイプ(Match Type)]で正規表現オプションを選択した場合は、ドロップダウン矢印をクリックして、[正規表現の作成(Create Regex)]を選択し、Regular Expression Editorを起動します。
6.  をクリックします(または<Enter>を押します)。
7. (オプション)ステップ2-6を繰り返して、条件を追加します。複数の一致はAND処理されます。
8. [現在の設定(Current Settings)]で作業している場合は、[テスト(Test)]をクリックして現在のスキャンの除外を処理できます。基準によって絞り込まれたそのスキャンからのセッションがテスト画面に表示され、必要に応じて設定を変更できます。
9. [OK]をクリックします。
10. [その他の除外/拒否基準(Other Exclusion/Rejection Criteria)]リストに除外が表示されている場合は、[拒否(Reject)]と[除外(Exclude)]のいずれかまたは両方を選択します。

注記: スキャン中は、応答タイプ、応答ヘッダタイプ、およびステータスコードターゲットタイプを拒否することができません。これらのターゲットタイプは除外することしかできません。

例1

Microsoft.comのリソースに対する要求を無視して送信しないようにするには、次の除外を入力して、 **拒否(Reject)**]を選択します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	contains	Microsoft.com

例2

一致文字列として「logout」と入力します。この文字列がURLの任意の部分で見つかった場合は、そのURLが除外または拒否されます(選択されたオプションによって異なる)。「logout」の例を使用すると、OpenText DASTは、loutout.aspやapplogout.jspなどのURLを除外または拒否します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	contains	logout

例3

次の例では、クエリパラメータ「username」が「John」と等しいクエリを含むセッションを拒否または除外します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
クエリパラメータ(Query parameter)	username	一致(matches)	John

例4

次の例では、次のディレクトリを除外または拒否します。

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)

URL	N/A	正規表現に一致 (matches regex)	/W3SVC[0-9]*/

第8章:監査設定

この章では、監査スキャン中にOpenText DASTによって使用される監査設定について説明します。監査とは、脆弱性を検出するように設計された、OpenText DASTによって実行されるプローブまたは攻撃のことです。OpenText DASTによるプローブの実行方法を制御するパラメータは、 [監査設定(Audit Settings)]リストから選択できます。

監査設定: セッション除外

この機能にアクセスするには、 **[編集(Edit)]**メニューをクリックし、 **[デフォルトのスキャン設定(Default Scan Settings)]**または **[現在のスキャン設定(Current Scan Settings)]**を選択します。その後で、 **[監査設定(Audit Settings)]**カテゴリで、 **[セッション除外(Session Exclusions)]**を選択します。

[スキャン設定-セッション除外(Scan Settings - Session Exclusions)]で指定した項目はすべて、 **[Web探索設定(Crawl Settings)]**と **[監査設定(Audit Settings)]**の両方の **[セッション除外(Session Exclusions)]**に自動的に複製されます。これらの項目は、灰色(黒色ではない)テキストで表示されます。これらのオブジェクトを監査から除外しない場合は、 **[スキャン設定-セッション除外(Scan Settings - Session Exclusions)]**パネルからそれらを削除する必要があります。

このパネル(**[監査設定-セッション除外(Audit Settings - Session Exclusions)]**)では、監査から除外する追加のオブジェクトを指定することができます。

除外または拒否するファイル拡張子

[拒否(Reject)]を選択した場合、OpenText DASTは指定された拡張子を持つファイルを要求しません。

[除外(Exclude)]を選択した場合、OpenText DASTは指定された拡張子を持つファイルを要求しますが、監査はしません。

除外/拒否するファイル拡張子の追加

ファイル拡張子を追加するには:

1. **[追加(Add)]**をクリックします。
   [除外拡張子(Exclusion Extension)]ウィンドウが開きます。
2. **[ファイル拡張子(File Extension)]**ボックスに、ファイル拡張子を入力します。
3. **[拒否(Reject)]**と **[除外(Exclude)]**のどちらかまたは両方を選択します。
4. **[OK]**をクリックします。

除外MIMEタイプ

OpenText DASTは、指定されたMIMEタイプに関連付けられたファイルを監査しません。

除外するMIMEタイプの追加

MIMEタイプを追加するには:

1. [**追加(Add)**]をクリックします。
   [除外するMimeタイプの指定(Provide a Mime-type to Exclude)]ウィンドウが開きます。
2. [**Mimeタイプの除外(Exclude Mime-type)**]ボックスに、MIMEタイプを入力します。
3. [**OK**]をクリックします。

その他の除外/拒否基準

HTTPメッセージのさまざまなコンポーネントを特定してから、そのコンポーネントを含むセッションを除外するか拒否するかを指定できます。

- **拒否(Reject)** - OpenText DASTは、指定されたホストまたはURLにHTTP要求を送信しません。たとえば、通常、サイトからのログオフを処理するURLは拒否する必要があります。これは、スキャンが完了する前にアプリケーションからログアウトしたくないためです。
- **除外(Exclude)** - Web探索中に、OpenText DASTは、指定されたURLまたはホストで他のリソースへのリンクを調査しません。スキャンの監査部分の間は、OpenText DASTは指定されたホストまたはURLを攻撃しません。HTTP応答を処理せずにURLまたはホストにアクセスする場合は、 [**除外(Exclude)**]オプションを選択しますが、 [**拒否(Reject)**]は選択しません。たとえば、処理しないURL上の壊れたリンクをチェックするには、 [**除外(Exclude)**]オプションだけを選択します。

デフォルトの基準の編集

デフォルトの基準を編集するには:

1. 基準を選択して、 [**編集(Edit)**]([**その他の除外/拒否基準(Other Exclusion/Rejection Criteria)**]リストの右側にある)をクリックします。
   [ホストまたはURLの拒否または除外(Reject or Exclude a Host or URL)]ウィンドウが開きます。
2. [**ホスト(Host)**]または [**URL**]を選択します。
3. [**ホスト/URL(Host/URL)**]ボックスに、URLまたは完全修飾ホスト名、またはターゲットのURLまたはホストに一致するように設計された正規表現を入力します。
4. [**拒否(Reject)**]と [**除外(Exclude)**]のどちらかまたは両方を選択します。
5. [**OK**]をクリックします。

除外/拒否基準の追加

除外/拒否基準を追加するには:

1. [追加(Add)]([その他の除外/拒否基準(Other Exclusion/Rejection Criteria)]リストの右側にある)をクリックします。
   [除外の作成(Create Exclusion)]ウィンドウが開きます。
2. [ターゲット(Target)]リストから項目を選択します。
3. ターゲットとして [クエリパラメータ(Query Parameter)]または [ポストパラメータ(Post Parameter)]を選択した場合は、 [ターゲット名(Target Name)]を入力します。
4. [一致タイプ(Match Type)]リストから、ターゲット内のテキストの一致に使用される方法を選択します。
   - [正規表現に一致(Matches Regex)] - [一致文字列(Match String)]ボックスで指定した正規表現に一致します。
   - [正規表現の拡張に一致(Matches Regex Extension)] - [一致文字列(Match String)]ボックスで指定したFortify正規表現の拡張から入手可能な構文に一致します。
   - [一致(Matches)] - [一致文字列(Match String)]ボックスで指定したテキスト文字列に一致します。
   - [含む(Contains)] - [一致文字列(Match String)]ボックスで指定したテキスト文字列を含みます。
5. [一致文字列(Match String)]ボックスに、ターゲットで検索する文字列または正規表現を入力します。または、 [一致タイプ(Match Type)]で正規表現オプションを選択した場合は、ドロップダウン矢印をクリックして、 [正規表現の作成(Create Regex)]を選択し、Regular Expression Editorを起動します。
6.  をクリックします(または<Enter>を押します)。
7. (オプション)ステップ2-6を繰り返して、条件を追加します。複数の一致はAND処理されます。
8. [現在の設定(Current Settings)]で作業している場合は、 [テスト(Test)]をクリックして現在のスキャンの除外を処理できます。基準によって絞り込まれたそのスキャンからのセッションがテスト画面に表示され、必要に応じて設定を変更できます。
9. [OK]をクリックします。
10. [その他の除外/拒否基準(Other Exclusion/Rejection Criteria)]リストに除外が表示されている場合は、 [拒否(Reject)]と [除外(Exclude)]のいずれかまたは両方を選択します。

注記: スキャン中は、応答タイプ、応答ヘッダタイプ、およびステータスコードターゲットタイプを拒否することができません。これらのターゲットタイプは除外することしかできません。

例1

Microsoft.comのリソースに対する要求を無視して送信しないようにするには、次の除外を入力して、 **拒否(Reject)**]を選択します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	contains	Microsoft.com

例2

一致文字列として「logout」と入力します。この文字列がURLの任意の部分で見つかった場合は、そのURLが除外または拒否されます(選択されたオプションによって異なる)。「logout」の例を使用すると、OpenText DASTは、loutout.aspやapplogout.jspなどのURLを除外または拒否します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
URL	N/A	contains	logout

例3

次の例では、クエリパラメータ「username」が「John」と等しいクエリを含むセッションを拒否または除外します。

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)
クエリパラメータ(Query parameter)	username	一致(matches)	John

例4

次の例では、次のディレクトリを除外または拒否します。

http://www.test.com/W3SVC55/

http://www.test.com/W3SVC5/

http://www.test.com/W3SVC550/

ターゲット(Target)	ターゲット名(Target Name)	一致タイプ(Match Type)	一致文字列(Match String)

URL	N/A	正規表現に一致 (matches regex)	/W3SVC[0-9]*/

監査設定: 攻撃除外

この機能にアクセスするには、 **編集(Edit)**] メニューをクリックし、 **デフォルトのスキャン設定(Default Scan Settings)**] または **現在のスキャン設定(Current Scan Settings)**] を選択します。その後で、 **監査設定(Audit Settings)**] カテゴリで、 **攻撃除外(Attack Exclusions)**] を選択します。

除外パラメータ

この機能を使用して、OpenText DASTがHTTP要求で特定のパラメータを使用してWebサイトを攻撃するのを防ぎます。この機能は、ほとんどの場合、クエリとPOSTDATAパラメータの破損を避けるために使用されます。

除外するパラメータの追加

特定のパラメータが変更されるのを防ぐには:

1. **除外パラメータ(Excluded Parameters)**] グループで、 **追加(Add)**] クリックします。
   [HTTP除外の指定(Specify HTTP Exclusions)] ウィンドウが開きます。
2. **HTTPパラメータ(HTTP Parameter)**] ボックスに、除外するパラメータの名前を入力します。
   をクリックして、正規表現表記を挿入します。
3. パラメータが見つかる可能性のあるエリア(HTTPクエリデータまたはHTTP POSTデータ)を選択します。必要に応じて、両方のエリアを選択できます。
4. **OK**] をクリックします。

除外クッキー(Excluded cookies)

この機能を使用して、OpenText DASTがHTTP要求で特定のクッキーを使用してWebサイトを攻撃するのを防ぎます。この機能は、クッキー値の破損を回避するために使用されます。

この設定では、クッキーの名前を入力する必要があります。

次のHTTP応答の例では、クッキーの名前が「FirstCookie」になっています。

```
Set-Cookie: FirstCookie=Chocolate+Chip; path=/
```

特定のクッキーの除外

特定のクッキーを除外するには:

1. [除外ヘッダ(Excluded Headers)]グループで、[追加(Add)]クリックします。
   Regular Expression Editorが表示されます。

   注記: クッキーは、テキスト文字列または正規表現を使用して指定できます。

2. テキスト文字列を入力するには:
   a. [式(Expression)]ボックスに、クッキー名を入力します。
   b. [OK]をクリックします。
3. 正規表現を入力するには:
   a. [式(Expression)]ボックスに、検索するテキストと一致すると思われる正規表現を入力または貼り付けます。

      をクリックして、正規表現表記を挿入します。
   b. [比較テキスト(Comparison Text)]ボックスに、検索する文字列([式(Expression)]ボックスで指定)が含まれていることが分かっているテキストを入力または貼り付けます。
   c. 式の大文字と小文字と一致する出現箇所のみを検索するには、[大文字/小文字を区別する(Match Case)]チェックボックスをオンにします。
   d. 正規表現によって識別された文字列を置き換える場合は、[置換(Replace)]チェックボックスをオンにしてから、[置換(Replace)]ボックスから文字列を入力または選択します。
   e. [テスト(Test)]をクリックして、正規表現に一致する文字列を比較テキストで検索します。一致は赤色で強調表示されます。
   f. 正規表現で文字列が識別されましたか?
      - 識別された場合は、[OK]をクリックします。
      - 識別されなかった場合は、識別したい文字列が[比較テキスト(Comparison Text)]に含まれているかどうかを確認するか、正規表現を変更します。

除外ヘッダ(Excluded headers)

この機能を使用して、OpenText DASTがHTTP要求で特定のヘッダを使用してWebサイトを攻撃するのを防ぎます。この機能は、ヘッダ値の破損を回避するために使用されます。

特定のヘッダの除外

特定のヘッダが変更されるのを防ぐには、次に説明する手順を使用して正規表現を作成します。

1. [除外ヘッダ(Excluded Headers)]グループで、 [追加(Add)]クリックします。
   Regular Expression Editorが表示されます。

   注記: ヘッダは、テキスト文字列または正規表現を使用して指定できます。

2. テキスト文字列を入力するには:
   a. [式(Expression)]ボックスに、ヘッダ名を入力します。
   b. [OK]をクリックします。
3. 正規表現を入力するには:
   a. [式(Expression)]ボックスに、検索するテキストと一致すると思われる正規表現を入力または貼り付けます。

      をクリックして、正規表現表記を挿入します。
   b. [比較テキスト(Comparison Text)]ボックスに、検索する文字列([式(Expression)]ボックスで指定)が含まれていることが分かっているテキストを入力または貼り付けます。
   c. 式の大文字と小文字と一致する出現箇所のみを検索するには、 [大文字/小文字を区別する(Match Case)]チェックボックスをオンにします。
   d. 正規表現によって識別された文字列を置き換える場合は、 [置換(Replace)]チェックボックスをオンにしてから、 [置換(Replace)]ボックスから文字列を入力または選択します。
   e. [テスト(Test)]をクリックして、正規表現に一致する文字列を比較テキストで検索します。一致は赤色で強調表示されます。
   f. 正規表現で文字列が識別されましたか?
      - 識別された場合は、 [OK]をクリックします。
      - 識別されなかった場合は、識別したい文字列が [比較テキスト(Comparison Text)]に含まれているかどうかを確認するか、正規表現を変更します。

監査入力エディタ

Audit Inputs Editorを使用して、入力を必要とする監査エンジンとチェック用のパラメータを作成または変更します。

- このツールを起動するには、 [Audit Inputs Editor]をクリックします。
- エディタを使用して過去に作成した入力をロードするには、 [監査入力のインポート(Import Audit Inputs)]をクリックします。

監査設定:攻撃式

この機能にアクセスするには、 [編集(Edit)]メニューをクリックし、 [デフォルトのスキャン設定(Default Scan Settings)]または [現在のスキャン設定(Current Scan Settings)]を選択します。その後で、 [監査設定(Audit Settings)]カテゴリで、 [攻撃式(Attack Expressions)]を選択します。

追加の正規表現言語

次のいずれかの言語コードと国コードの組み合わせを選択できます(.NET Frameworkクラスライブラリ内のCultureInfoクラスで使用されるのと同様)。

- zh-cn: 中国語-中国
- zh-tw: 中国語-台湾
- ja-jp: 日本語-日本
- ko-kr: 韓国語-韓国
- pt-br: ポルトガル語-ブラジル
- es-es: スペイン語-スペイン

CultureInfoクラスは、関連する言語、サブ言語、国/地域、暦、および文化的慣習などの文化固有の情報を保持します。また、このクラスは、DateTimeFormatInfo、NumberFormatInfo、CompareInfo、およびTextInfoの文化固有のインスタンスへのアクセスも提供します。これらのオブジェクトには、大文字/小文字の指定、日付と数値の書式設定、文字列の比較など、文化固有の操作に必要な情報が含まれています。

監査設定: 脆弱性フィルタリング

この機能にアクセスするには、 **編集(Edit)**] メニューをクリックして **デフォルト設定(Default Settings)**] または **現在の設定(Current Settings)**] を選択します。その後で、 **監査の設定(Audit Settings)**] カテゴリで、 **脆弱性フィルタリング(Vulnerability Filtering)**] を選択します。

特定のフィルタを適用することで、スキャン中に報告された特定の脆弱性の表示を制限できます。オプションは次のとおりです。

- **標準の脆弱性定義(Standard Vulnerability Definition)** -このフィルタは、類似する要求の同等性を判断できるようにパラメータ名をソートします。たとえば、`http://x.y?a=x;b=y` および`http://x.y?b=y;a=x`の両方のパラメータ「a」でSQLインジェクションの脆弱性が検出された場合、この脆弱性は同等と見なされます。
- **パラメータ脆弱性ロールアップ(Parameter Vulnerability Roll-Up)** -このフィルタは、1つのセッションで検出された複数のパラメータ操作およびパラメータインジェクションの脆弱性を1つの脆弱性に統合します。
- **403ブロッカー(403 Blocker)** -このフィルタは、脆弱なセッションのステータスコードが403 (禁止)の場合に脆弱性を取り消します。
- **応答検査DOMイベントの親子(Response Inspection DOM Event Parent-Child)** -このフィルタは、JavaScriptで検出されたキーワード検索の脆弱性と同じ脆弱性が親セッションですでに検出されている場合に、この脆弱性を無視します。

脆弱性フィルタの追加

フィルタをデフォルト設定に追加するには:

1. **[編集(Edit)]**メニューをクリックして、**[デフォルトのスキャン設定(Default Scan Settings)]**を選択します。
2. **[監査設定(Audit Settings)]**パネルの左側の列で、**[脆弱性フィルタリング(Vulnerability Filtering)]**を選択します。

   使用可能なすべてのフィルタは、**[無効なフィルタ(Disabled Filters)]**リストまたは**[有効なフィルタ(Enabled Filters)]**リストのいずれかに一覧表示されます。
3. フィルタを有効にするには、**[無効なフィルタ(Disabled Filters)]**リストでフィルタを選択し、**[追加(Add)]**をクリックします。

   そのフィルタが**[無効なフィルタ(Disabled Filters)]**リストから削除され、**[有効なフィルタ(Enabled Filters)]**リストに追加されます。
4. フィルタを無効にするには、**[有効なフィルタ(Enabled Filters)]**リストでフィルタを選択し、**[削除(Remove)]**をクリックします。

   そのフィルタが**[有効なフィルタ(Enabled Filters)]**リストから削除され、**[無効なフィルタ(Disabled Filters)]**リストに追加されます。

特定のスキャンの設定を変更することもできます。このためには、スキャンウィザードまたはWebサービススキャンウィザードの下部にある**[設定(Settings)]**ボタンをクリックします。

サイト外の脆弱性の抑止

[許可ホスト(Allowed Hosts)]リストにないホストへのリンクがWebアプリケーションに含まれている場合、OpenText DASTはこれらのホストで受動的な脆弱性を検出することがあります。**[許可ホスト(Allowed Hosts)]**リストにないサイト外ホストのセッションに対してすべての脆弱性を抑止するには、**[サイト外の脆弱性を抑止する(Suppress Offsite Vulnerabilities)]**チェックボックスをオンにします。

許可ホストの詳細については、「"スキャン設定: 許可ホスト" ページ421」を参照してください。

監査設定: スマートスキャン

この機能にアクセスするには、**[編集(Edit)]**メニューをクリックし、**[デフォルトのスキャン設定(Default Scan Settings)]**または**[現在のスキャン設定(Current Scan Settings)]**を選択します。その後で、**[監査設定(Audit Settings)]**カテゴリで、**[スマートスキャン(Smart Scan)]**を選択します。

スマートスキャンの有効化

スマートスキャンは、Webサイトをホストしているサーバのタイプを検出し、その特定のサーバタイプに対する既知の脆弱性をチェックする「インテリジェント」機能です。たとえば、IISサーバで

ホストされているサイトをスキャンする場合、OpenText DASTはIISが影響を受けやすい脆弱性のみを検索します。ApacheやiPlanetなどの他のサーバに影響を及ぼす脆弱性はチェックしません。

このオプションを選択すると、次に説明する1つ以上の識別方法を選択できます。

HTTP応答で正規表現を使用する(Use regular expressions on HTTP responses)

以前のリリースのOpenText DASTで採用されたこの方法は、特定のサーバを識別するために設計された定義済みの正規表現に一致する文字列をサーバ応答で検索します。

サーバアナライザのフィンガープリント法を使用し、サンプリングを要求する(Use server analyzer fingerprinting and request sampling)

この高度な方法は、一連のHTTP要求を送信してから、応答を分析してサーバ/アプリケーションタイプを判断します。

カスタムサーバ/アプリケーションタイプの定義(Custom server/application type definitions)

ターゲットドメインのサーバタイプが分かっている場合は、 **[カスタムサーバ/アプリケーションタイプの定義(Custom server/application type definitions)]** セクションを使用してそれを選択できます。この識別方法は、指定されたサーバ用に選択された他の方法を無効にします。

カスタム定義を指定するには:

1. **[追加(Add)]** をクリックします。
   [サーバ/アプリケーションタイプ入力(Server/Application Type Entry)] ウィンドウが開きます。
2. **[ホスト(Host)]** ボックスに、ドメイン名またはホスト、またはサーバのIPアドレスを入力します。
3. (オプション) **[識別(Identify)]** をクリックします。
   OpenText DASTは、サーバに接続し、サーバアナライザのフィンガープリント法を使用してサーバタイプを判断します。成功すると、 **[サーバ/アプリケーションタイプ(Server/Application Type)]** リストで対応するチェックボックスがオンにされます。

   注記: または、 **[正規表現を使用する(Use Regular Expressions)]** オプションを選択した場合は、サーバを識別するために設計された正規表現を入力します。正規表現表記を挿入したり、Regular Expression Editor (式の作成とテストを容易にします)を起動したりするには、▶をクリックします。

4. [サーバ/アプリケーションタイプ(Server/Application Type)]リストから、1つ以上のエントリを選択します。
5. [OK]をクリックします。

第9章:アプリケーション設定

この章では、OpenText DASTがスキャンデータとログファイルを保存する場所を定義する設定と、ライセンス供与やSmartUpdateに関する設定について説明します。これらの設定により、OpenText DASTがOpenText Application Lifecycle Management (ALM)などの他のアプリケーションと対話するための設定も行われます。

アプリケーション設定: 全般

この機能にアクセスするには、 **[編集(Edit)] > [アプリケーション設定(Application Settings)]** をクリックしてから、 **[全般(General)]** を選択します。

全般(General)

[全般(General)] のオプションの説明を次の表に示します。

オプション	説明
ブラウザビューでアクティブコンテンツを有効にする(Enable Active Content in Browser Views)	このオプションは、OpenText DAST内のすべてのブラウザウィンドウでJavaScriptとその他のダイナミックコンテンツの実行を可能にする場合に選択します。 たとえば、あるOpenText DAST攻撃は、ダイナミックに生成されたWebページにスクリプトを埋め込もうとすることによって、クロスサイトスクリプティングをテストします。このスクリプトは、番号「76712」を含むアラートを表示するようにサーバに指示します。アクティブコンテンツが有効で、攻撃が成功した場合(つまり、クロスサイトスクリプティングが可能な場合)は、脆弱なセッションを選択して、 [セッション情報(Session Info)] パネルで **[Webブラウザ(Web Browser)]** をクリックすると、スクリプトが実行され、次の画面が表示されます。  **注記:** このオプションが無効な状態でスキャンを開始するか開いてからこのオプションを有効にすると、スキャンを閉じて再度開く

オプション	説明
	までブラウザはアクティブコンテンツを実行しません。
診断ファイルの作成を有効にする(Enable Diagnostic File Creation)	OpenText DASTアプリケーションで障害が発生した場合、このオプションが選択されていると、OpenText DASTは、障害発生時にメインメモリに保存されていたデータを含むファイルを作成するように強制されます。後で、OpenTextサポート担当者にそのファイルを提供できます。 このオプションを選択する場合は保持すべき診断ファイルの数も指定できます。ファイルの数がこの制限を超えると、最も古いファイルが削除されます。
「次回から表示しない」メッセージをリセットする(Reset "Don't Show Me Again" messages)	デフォルトで、OpenText DASTには、さまざまなプロンプトとダイアログボックスが表示され、実行するアクションの結果として発生する可能性がある特定の結果が知らされます。これらのダイアログボックスには、 [次回から表示しない(Don't show me again)]というラベルのチェックボックスが表示されます。このオプションを選択すると、OpenText DASTは、それらのメッセージの表示を中止します。 **[次回から表示しない」メッセージをリセットする(Reset "Don't Show Me Again" messages)]**をクリックすると、それらのメッセージの表示を再開するようにOpenText DASTに強制できます。
7つの有害な界(7PK)分類を使用する(Use Seven Pernicious Kingdom (7PK) Taxonomy)	このオプションを選択すると、報告された脆弱性を順序付けおよび整理するために、7つの有害な界分類を選択できます。 7つの有害な界(7PK)は、Fortify Software Security Research GroupとGary McGraw博士が共同で策定したソフトウェアセキュリティエラーの分類です。各脆弱性カテゴリには、問題の詳細な説明と、オリジナルのソースとコード抜粋への参照が付随している(該当する場合)ため、問題をより適切に把握できます。 分類スキームの編成は、生物学から借用した用語を使って記述されます。脆弱性のカテゴリは門と呼ばれ、同じテーマを共有する脆弱性カテゴリのコレクションは界と呼ばれます。脆弱性の門は、ソフトウェアセキュリティにとっての重要度順で提示される有害な界に分類されます。 7つの界は次のとおりです。 1. 入力の検証と表現 2. APIの誤用 3. セキュリティ機能

オプション	説明
	4. 時間と状態 5. エラー 6. コードの品質 7. カプセル化 *環境 最初の7つの界は、ソースコードのセキュリティ欠陥に関連するもので、最後の1つは、実際のコード以外のセキュリティ問題を表します。 この分類を定義する主な目的は、セキュリティルールのセットを整理して、セキュリティに影響を及ぼすエラーの種類をソフトウェア開発者が理解しやすくすることです。システム障害の発生方法の理解を深めると、開発者は自分が作成するシステムを分析する能力が高まり、セキュリティ問題の特定と、それが見つかった場合の対応がより迅速になって、その後は同じミスを繰り返さなくなるのが普通です。詳細については、https://vulncat.fortify.com/を参照してください。 OpenText DASTを他のOpenText Fortify製品と統合する場合は7つの有害な界の分類を使用できます。これは統一された分類に対応しているためです。
OpenSSLエンジンの使用(Use OpenSSL Engine)	デフォルトで、OpenText DASTはこのオプションを使用します。OpenSSLエンジンは、TLS 1.3セキュリティプロトコルを使用する必要があるWebサイトをサポートします。OpenSSLは、以前のバージョンのTLSプロトコルと後方互換性があります。 このオプションを有効にすると、[スキャン設定:方法(Scan settings: Method)]で[SSL/TLSプロトコル(SSL/TLS Protocols)]オプションが無効になります。スキャン用の個別のプロトコルを選択することはできません。
HTTP/2サポートを有効にする(Enable HTTP/2 Support)	WebサイトがHTTP/2プロトコルのみをサポートしており、HTTP/1プロトコルを使用すると問題が発生する場合に、このオプションを使用します。
複合スキャン設定の使用	複合設定は、ZIPファイルにパッケージされたJSONバージョンのスキャン設定と、マクロ、クライアント証明書、カスタムポリシーなど、スキャンに必要なバイナリファイルで構成されます。OpenText ScanCentral DASTは複合設定を使用します。デフォルトで、OpenText DASTはXML設定を使用します。このオプションを選択

オプション	説明
	すると、OpenText DASTは、OpenText ScanCentral DASTにインポートして使用する準備が整った複合設定を、変換なしで作成および使用できるようになります。 XML設定をOpenText DAST UIで複合設定に変換することはできません。自動変換するには、OpenText DAST APIエンドポイント(`configuration/scansettings/convert`)を使用するか、設定をOpenText ScanCentral DASTにインポートする必要があります。さらに、XML設定を使用して実行されたスキャンから設定ファイルを保存する場合、 複合スキャン設定の使用(Use Composite Scan Settings)]オプションが有効になっている場合でも、ファイルはXML形式で保存されます。 重要! {/b}このオプションを有効にすると、ZIP設定のみが環境設定のためにOpenText DASTにアクセスできるようになります。XML設定にアクセスするには、このオプションを無効にする必要があります。

OpenText DAST Agent

次の表で、OpenText DAST Agentのオプションについて説明します。

オプション	説明
ターゲットサイトで検出されたWebInspect Agent情報を使用する(Use WebInspect Agent information when encountered on target site)	このオプションが選択されている状態で、OpenText DAST AgentがターゲットサーバにインストールされていることをOpenText DASTが検出すると、OpenText DAST Agent情報が取り込まれ、全体的なスキャン効率が高まります。 OpenText DASTダッシュボード上にOpenText DAST Agentが検出されたかどうかを示す注が表示されます。
脆弱性ウィンドウで重複する脆弱性別に自動的にグループ化する(Automatically group by duplicate vulnerabilities in vulnerability	このオプションが選択され、OpenText DAST Agent情報が使用される場合(上記の設定)は、サマリペインの **検出事項(Findings)**]タブに一覧表示された脆弱性が、チェック別にグループ化されてから、相当する脆弱性別にグループ化されます。

オプション	説明
window)	
WebInspect Agentに攻撃戦略の提案を許可する(Allow WebInspect Agent to suggest attack strategy)	このオプションが選択され、OpenText DAST情報が使用される場合(上記の「ターゲットサイトで検出されたWebInspect Agent情報を使用する」を参照)、エージェントはアクティブモードで動作し、OpenText DASTに攻撃戦略を提案して、精度とパフォーマンスを上げることができます。この機能を使用するには、7つの有害な界分類を使用する必要があります。

アプリケーション設定:データベース

この機能にアクセスするには、 **[編集(Edit)] > [アプリケーション設定(Application Settings)]** をクリックしてから、 **[データベース(Database)]** を選択します。

ヒント: OpenText DASTがセンサとしてFortify WebInspect Enterpriseに接続されている場合は、SQLデータベースの設定を上書きできます。詳細については、「"アプリケーション設定:SQLデータベース設定の上書き" ページ504」を参照してください。

スキャン/レポートストレージの接続設定

OpenText DASTスキャンおよびレポートデータを保存するデータベースを選択します。次の選択肢があります。

- **SQL Server Expressを使用する(Use SQL Server Express)** (SQL Server Express Editionの場合)。各スキャンのデータは、別々のデータベースに保存されます。
- **SQL Serverを使用する(Use SQL Server)** (SQL Server Standard Editionの場合)。複数のスキャンのデータは、1つのデータベースに保存されます。複数のデータベース設定を行い、設定のコレクションのそれぞれに「プロファイル名」を割り当てれば、設定を簡単に切り替えることができます。

SQL Serverデータベース特権

データベース接続に対して指定するアカウントは、指定したデータベースのデータベース所有者(DBO)である必要もあります。ただし、このアカウントには、データベースサーバに対するsysadmin (SA)特権は必要ありません。指定されたユーザのためにデータベース管理者(DBA)がデータベースを生成しなかった場合、そのアカウントはデータベースの作成と、セキュリティ許可の操作を行う許可も持っている必要があります。DBAは、OpenText DASTがデータベースをセットアップした後にこれらの許可を取り消すことができますが、アカウントはそのデータベースのDBOであり続ける必要があります。

SQL Server Standard Editionの設定

SQL Server Standard Editionのプロファイルを設定するには:

1. **設定(Configure)**](ドロップダウンリスト右側にある)をクリックします。
   [データベース設定の管理(Manage Database Settings)]ダイアログボックスが表示されます。
2. **追加(Add)**]をクリックします。
   [データベースの追加(Add Database)]ダイアログボックスが表示されます。
3. このデータベースプロファイルの名前を入力します。
4. **サーバ名(Server Name)**]リストからサーバを選択します。

   重要! {/b}SQL Server Browserが有効になっていない場合、データベースサーバはリストに表示されません。この場合は、接続情報を手動で入力する必要があります。接続文字列は次のように書式設定されます。

   ```
   SERVER\INSTANCE,PORT
   ```

   コロンまたはセミコロンではなく、カンマを使用してポート定義が追加されることに注意してください。
5. **サーバにログオンする(Log on to the server)**]グループで、選択したサーバに使用される認証のタイプを指定します。
   - **Windows認証を使用する(Use Windows Authentication)** -ユーザのWindowsアカウント名とパスワードを送信することによってログオンします。
   - **SQL Server認証を使用する(Use SQL Server Authentication)** - SQL Server認証を使用します。この認証は、SQL Serverコンピュータによって維持されている内部ユーザリストに依存します。ユーザ名とパスワードを入力します。
6. 特定のデータベースを入力または選択するか、 **新規(New)**]をクリックしてデータベースを作成します。
7. **OK**]をクリックして、 [データベースの追加(Add Database)]ダイアログボックスを閉じます。
8. **OK**]をクリックして、 [データベース設定の管理(Manage Database Settings)]ダイアログボックスを閉じます。

スキャン表示の接続設定

スキャンのリストを表示する([スキャンの管理(Manage Scans)]ビューまたはReport Generatorウィザードを使用して)と、OpenText DASTはSQL Server Standard Editionおよび/またはSQL Server Express Editionに保存されたスキャンデータにアクセスできます。どちらかまたは両方のオプションを選択できます。

- **SQL Server Expressに保存されたスキャンの表示(Show Scans Stored in SQL Server Express)**: ローカルのSQL Server Express Editionに保存されたスキャンデータにアクセスす

る場合に、このオプションを選択します。

- **SQL Server Standardに保存されたスキャンの表示(Show Scans Stored in SQL Server Standard)**: SQL Server Standard Edition内のデータにアクセスする場合に、このオプションを選択します。詳細については、「"SQL Server Standard Editionの設定" 前のページ」を参照してください。

アプリケーション設定: ディレクトリ

この機能にアクセスするには、 **[編集(Edit)] > [アプリケーション設定(Application Settings)]** をクリックしてから、 **[ディレクトリ(Directories)]** を選択します。

OpenText DASTファイルの保存場所の変更

OpenText DASTファイルが保存される場所を変更できます。場所を変更するには:

1. 情報のカテゴリの横にある省略記号ボタン ... をクリックします。
2. [フォルダの参照(Browse For Folder)] ダイアログボックスを使用して、ディレクトリを選択または作成します。
3. **[OK]** をクリックします。

アプリケーション設定: ライセンス

この機能にアクセスするには、 **[編集(Edit)] > [アプリケーション設定(Application Settings)]** をクリックしてから、 **[ライセンス(License)]** を選択します。

ライセンスの詳細

このセクションでは、OpenText DASTライセンスに関する情報を提供します。ライセンスの特定の条項を変更する場合は、 **[ライセンス供与の設定(Configure Licensing)]** をクリックしてライセンスウィザードを起動します。

ウィンドウの下側のセクションの内容は、現在採用されているライセンス管理のタイプによって異なります。

- OpenTextライセンスサーバに直接接続されている。「"OpenTextへの直接接続" 次のページ」を参照してください。
- ローカルのOpenText™ Fortify License and Infrastructure Manager (LIM)に接続されている。「"LIMへの接続" 次のページ」を参照してください。

OpenTextへの直接接続

オプションの説明を次の表に示します。

オプション	説明
アップデート(Update)	評価版からアップグレードする場合やそれ以外の方法でライセンスの条件を変更する場合は、[**アップデート(Update)**]をクリックします。アプリケーションは、ライセンスサーバに接続して、マシンにローカルに保存されている情報を更新します。
非アクティブ化(Deactivate)	OpenText DASTライセンスは、特定のコンピュータに割り当てられます。このライセンスを別のコンピュータに転送する場合: 1. アクティベーショントークンをコピーします。 この番号を紛失したり、保存場所を忘れたりしないように注意してください。書き留めるか印刷して、安全な場所に保管してください。 2. [**非アクティブ化(Deactivate)**]をクリックします。 アプリケーションは、ライセンスサーバに接続してライセンスを解放し、別のコンピュータにOpenText DASTをインストールできるようにします。 3. 新しいコンピュータで、ライセンス供与用のOpenText DASTアプリケーション設定にアクセスし、アクティベーショントークンを入力します。

LIMへの接続

このコンピュータに割り当てられたOpenText DASTライセンスをLIMに処理させる方法を選択します。オプションの説明を次の表に示します。

オプション	説明
接続ライセンス(Connected License)	LIMに接続できる場合にのみ、コンピュータはFortifyソフトウェアを実行できます。ソフトウェアを起動するたびに、LIMがライセンスプールからこのインストールにシートを割り当てます。ソフトウェアを閉じると、コンピュータからシートが解放されて再びプールに割り当てられるため、別のユーザがそのライセンスを使用できるようになります。
分離ライセンス	コンピュータはどこでも、企業イントラネット(LIMが通常存在する場所)から切断されている場合でさえ、Fortifyソフトウェアを実行できま

オプション	説明
	す。しかし、これは指定された有効期限までです。そのため、ラップトップをリモートサイトに持ち込んでソフトウェアを実行することができます。企業イントラネットに再接続すると、アプリケーションライセンスの設定にアクセスして、 [分離(Detached)]から [接続(Connected)]に再設定できます。

LIMを使用するためのOpenText DASTの設定の詳細については、『OpenText™ Dynamic Application Security Testingインストールガイド』を参照してください。

アプリケーション設定: Server Profiler

この機能にアクセスするには、 **[編集(Edit)] > [アプリケーション設定(Application Settings)]** をクリックしてから、 **[Server Profiler]** を選択します。

スキャンを開始する前に、OpenText DASTは、Server Profilerを呼び出して、ターゲットWebサイトの事前テストを実行し、特定のスキャン設定を変更すべきかどうかを判断できます。変更が必要だと思われる場合、Server Profilerは提案のリストを返します。これらの提案は、受け入れることも拒否することもできます。

この事前テストを有効にするには、ステップ4で **[プロファイル(Profile)]** をクリックします(または **[Profilerを自動的に実行する(Run Profiler Automatically)]** を選択します)。

デフォルトで、10個の特定のモジュールが有効になります。モジュールを除外するには、関連付けられたチェックボックスをオフにします。

モジュール

Server Profilerモジュールの説明を次の表に示します。

モジュール	説明
大文字と小文字を区別するサーバのチェック	このモジュールでは、ホストサーバがURLを識別する際に大文字と小文字を区別するかどうかを判別します。たとえば、一部のサーバ(IISなど)は、www.mycompany.com/samplepage.htmとwww.mycompany.com/SamplePage.htmを区別しません。プロファイラにより、サーバが大文字と小文字を区別しないと判別された場合は、OpenText DASTの大文字と小文字を区別する機能を無効にできます。そうすることによって、Web探索の速度と精度が向上します。
「最大フォルダ深さ」設定のチェック	最大フォルダ深さ設定は主に、プログラムによってURLにサブフォルダを追加するサイトを対象とします。このような制限がない場合、

モジュール	説明
	OpenText DASTはそれらのダイナミックフォルダを無制限にWeb探索します。このモジュールでは、その制限を超える有効なURLがサイトに含まれているかどうかを判別します。含まれている場合は、設定を大きくすることができます。
クライアント認証プロトコルの検証	このモジュールでは、必要な認証(サインイン)プロトコル(ある場合)を判別します。OpenText DASTは、ADFS CBT、自動、ダイジェスト、HTTP基本、Kerberos、およびNTLMをサポートしています。
追加のホストのチェック	このモジュールは、ターゲットサイトで追加のホストサーバへの参照を検索し、それらを許可ホストとして含めることができるようにします。
ナビゲーションパラメータの表示	このモジュールは、ターゲットサイトでページのコンテンツを指定するためにURL内のクエリパラメータが使用されているかどうかを判断します。使用されている場合は、分析中に検出されたパラメータと値のリストを表示します。OpenText DASTがスキャン中に使用する1つ以上のパラメータを選択できます。
非標準の「ファイルが見つからない」応答のチェック	このモジュールは、存在しないリソースをクライアントから要求された場合に、サイトが404以外の応答コードを返すかどうかを判断します。これを認識すると、OpenText DASTは不必要な応答を監査しなくなります。
URLに埋め込まれたセッション状態のチェック	一部のサーバは、クッキーを使用する代わりにセッション状態をURLに埋め込みます。OpenText DASTは、正規表現を使用してURLを分析することによって、このプラクティスを検出します。このモジュールは、正規表現に対する変更が必要かどうかを判断しようとします。
スレッド数の分析	このモジュールは、スレッド数を小さくすべきかどうかを判断します。高速スキャンが有効な場合、スレッド数が比較的に大きくなると、サーバリソースが使い果たされる可能性があります。
無効な監査除外のチェック	OpenText DAST設定では、特定のファイル拡張子を持つページを監査から除外します("監査設定:セッション除外" ページ469を参照)。指定された拡張子は、通常、要求のURLにクエリパラメータが含まれていないページ用です。設定が間違っていると、監査が不完全になります。監査除外される拡張子を持つページに実際にはクエリパラメータがある場合、プロファイラはそれを検出でき、それらの除外を削除するよう推奨します。
最大応答サイズの検証	OpenText DASTスキャン設定では、許容される最大応答サイズを指定します。デフォルトは1,000キロバイトです。このモジュールは最

モジュール	説明
	大値より大きい応答の検出を試みて、それが見つかった場合に制限の引き上げを推奨します。
特定のアプリケーションの設定の最適化	このモジュールは、スキャンしているのがよく知られたテストサイト(WebGoat、Hacme Bankなど)であるかどうかを判断し、OpenText DASTにそのサイト専用に設計された事前入力設定ファイル(テンプレート)があるかどうかを判断します。これらのテンプレートは、スキャンのWeb探索、監査、およびパフォーマンスを最適化するように設定されています。
末尾のスラッシュの追加/削除	このモジュールは、ターゲットサイトで開始URLの末尾のスラッシュが必須か禁止かを判断します。
クロスサイトリクエストフォージェリのチェック	クロスサイトリクエストフォージェリは、ワンクリック攻撃やセッションライディングとも呼ばれますが、多くの場合、CSRFと省略されます。CSRFは、Webサイトが信頼するユーザから不正なコマンドが送信されるWebサイトエクスプロイトの一種です。特定のサイトに対するユーザの信頼を悪用するクロスサイトスクリプティングとは異なり、CSRFは、サイトがユーザのブラウザ内で持っている信頼を悪用します。CSRFの詳細については、「"CSRF" ページ427」を参照してください。
WebSphereサーバのチェック	WebSphereサーバには、追加の設定変更が必要です。このProfilerでは、これらの変更が必須かどうかを検出します。

アプリケーション設定:ステップモード

この機能にアクセスするには、 **[編集(Edit)] > [アプリケーション設定(Application Settings)]** をクリックしてから、 **[ステップモード(Step Mode)]** を選択します。

ステップモードのオプションの説明を次の表に示します。

オプション	説明
デフォルト監査モード(Default Audit Mode)	次のいずれかを選択します。 • **ブラウズ時の監査(Audit as you browse)**: ターゲットWebサイトを移動している間に、OpenText DASTがアクセス先のページを同時に監査します。 • **手動監査(Manual Audit)**: このオプションを使用すると、ステップモードスキャンを一時停止してOpenText DASTに戻り、特定のセッションを選択して監査することができます。

オプション	説明
プロキシリスナ(Proxy Listener)	次のオプションを選択します。 • **ローカルIPアドレス(Local IP Address)**: ステップモードではプロキシが必要です。プロキシで使用するIPアドレスを指定します。 • **ポート(Port)**: プロキシで使用すべきポートを指定するか、 **[ポートを自動的に割り当てる(Automatically Assign Port)]**を選択します。

アプリケーション設定:2要素認証

この機能にアクセスするには、 **[編集(Edit)] > [アプリケーション設定(Application Settings)]**をクリックしてから、 **[2要素認証(Two-Factor Authentication)]**を選択します。

2要素認証コントロールセンター

「ユーザが持っているもの」としての2要素認証には、WebアプリケーションにログインするユーザにSMS応答または電子メール応答を送信するアプリケーションサーバが関与します。スキャンで2要素認証を使用するには、Node.jsサーバをアプリケーションサーバから受信したSMSおよび電子メール応答を処理するコントロールセンターとして設定する必要があります。詳細については、「"2要素認証の使用" ページ222」を参照してください。

コントロールセンターを設定するには:

1. **[ローカルIPアドレス(Local IP Address)]**ドロップダウンリストで、IPアドレスを選択します。

   注記: これらのIPアドレスは、OpenText DASTがインストールされているマシンで使用できます。

2. 次のいずれかを実行します。
   - 特定のポートを使用するには、**[ポート]**リストからポートを選択します。
   - OpenText DASTにポートを選択させるには、 **[ポートを自動的に割り当てる(Automatically Assign Port)]**チェックボックスをオンにします。

     重要! {/b}モバイルアプリケーションがサーバにアクセスするには、コントロールセンターのポートをファイアウォールで公開する必要があります。

3. **[初期化]**をクリックします。
   コントロールセンターが起動します。

モバイルアプリケーション

アプリケーションサーバがSMS応答を送信する場合は、**Fortify2FA**モバイルアプリケーションをインストールし、それに2要素認証設定をダウンロードする必要があります。設定後、モバイルアプリケーションはSMS応答を受信し、コントロールセンターに転送します。

注記: 現在、モバイルアプリケーションはAndroid OSでのみ使用できます。

モバイルアプリケーションを設定するには、次の手順を実行します。

1. **[携帯電話番号(Mobile Phone Number)]**ボックスに、SMS応答を受信する電話番号を入力します。
2. **[QRコードの生成]**をクリックします。
   コントロールセンターは、2要素認証設定とモバイルアプリケーションをダウンロードするリンクを含むクイックレスポンス(QR)コードを生成します。
3. モバイルアプリケーションをインストールして設定します。詳細については、「"Fortify2FAモバイルアプリのインストールと設定" 下」を参照してください。

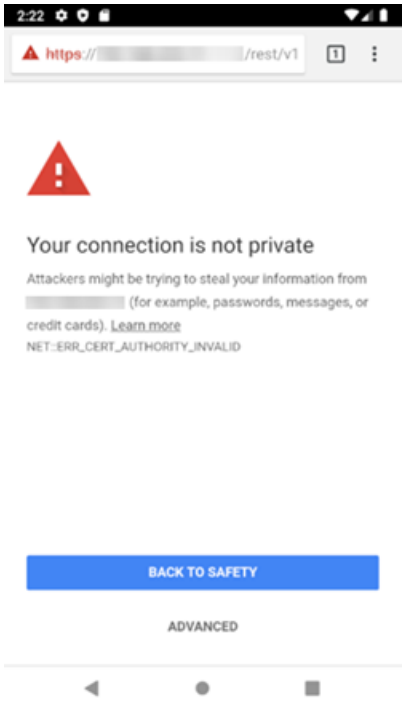
   ヒント: スキャンで複数のスレッドを使用する場合は、複数の電話を使用することをお勧めします。マルチユーザスキャンに同じ電話番号を使用すると、スキャン時間に影響する場合があります。
4. (オプション)別の電話用にモバイルアプリケーションを設定するには、手順1~3を繰り返します。

Fortify2FAモバイルアプリのインストールと設定

SMS応答を受信する電話にモバイルアプリケーションをインストールして設定するには、次の手順を実行します。

1. 携帯電話のカメラを使用して、**[2要素認証モバイルアプリケーション(Two-factor Authentication Mobile Application)]**の設定内のQRコードをスキャンします。
   リンクが表示されます。
2. リンク(または**[開く]**ボタン)をクリックして、アプリをダウンロードするためのサイトにアクセスします。

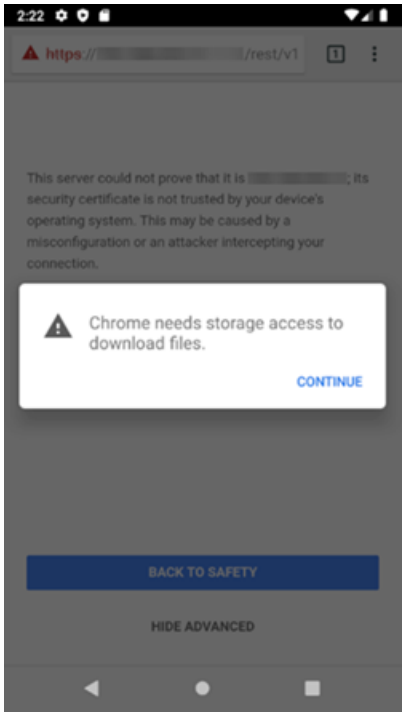
自己署名証明書に関する警告が表示されます。



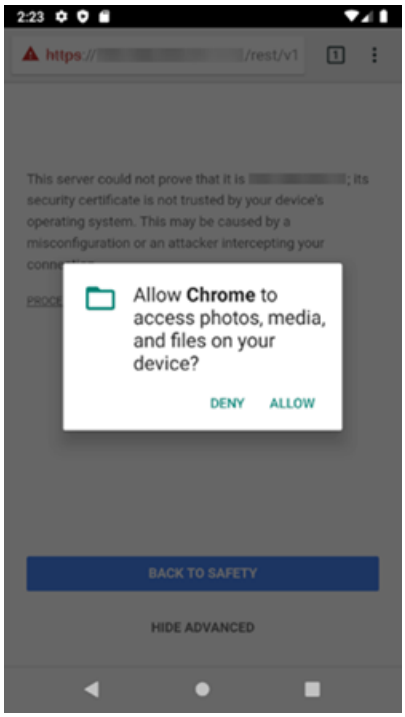
3. **[詳細]**をクリックします。
   次に進むためのリンクと共に追加情報が表示されます。

4. **[*<ip_address>*に続行する(安全でない)]**をクリックします。

ダウンロードファイルへのストレージアクセスを要求するプロンプトが表示されます。



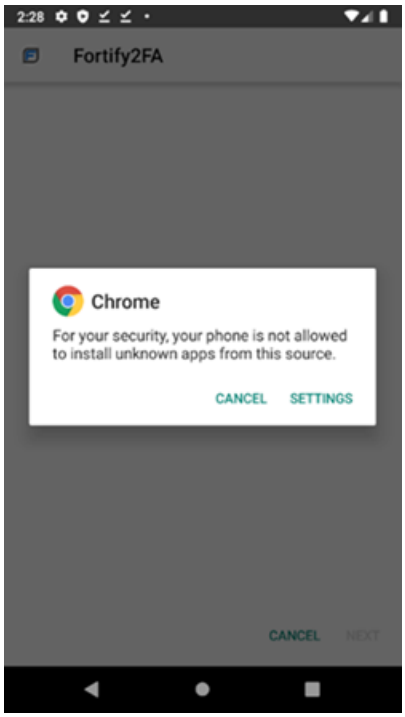
5. [次へ]をクリックします。
プロンプトがデバイス上の写真、メディア、およびファイルへのアクセスを要求します。



6. [許可]をクリックします。

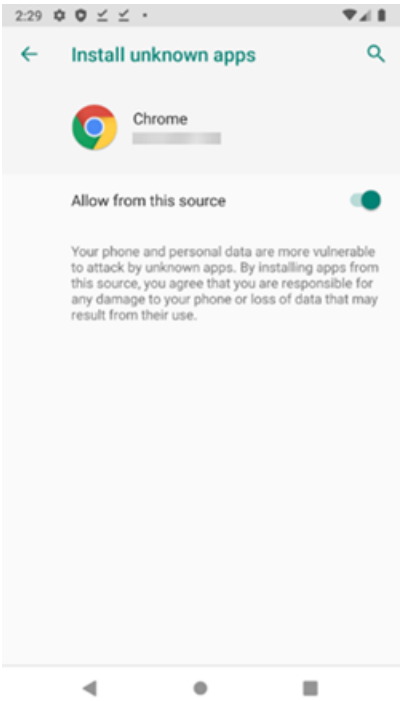
fortify-2fa.apkファイルがダウンロードされます。

7. [開く]をクリックします。
   不明なアプリのインストールについてプロンプトが表示されます。

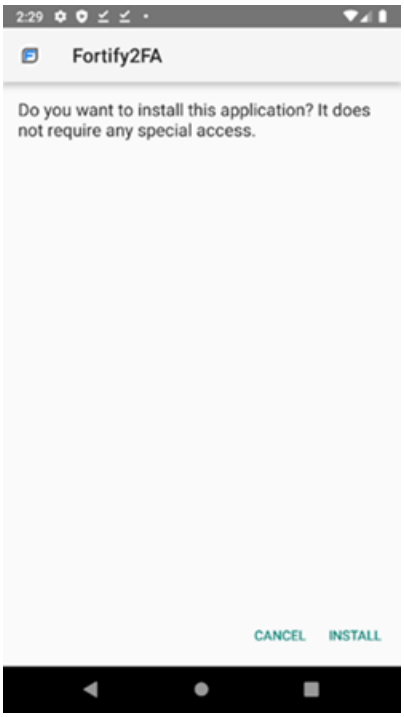


8. [設定]をクリックします。

[不明なアプリのインストール]設定が表示されます。

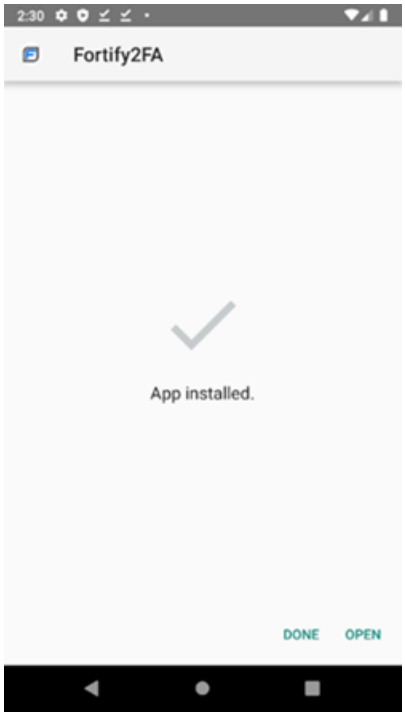


9. **[このソースから許可]**を有効にする。
   アプリケーションをインストールするかどうかを確認するプロンプトが表示されます。

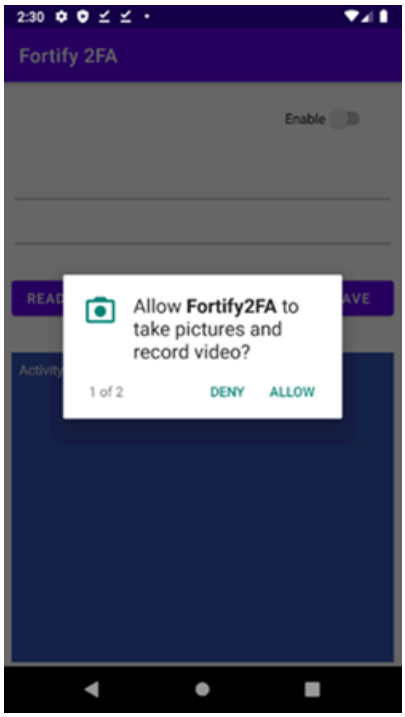


10. **[インストール]**をクリックします。

アプリがインストールされていることを示すメッセージが表示されます。

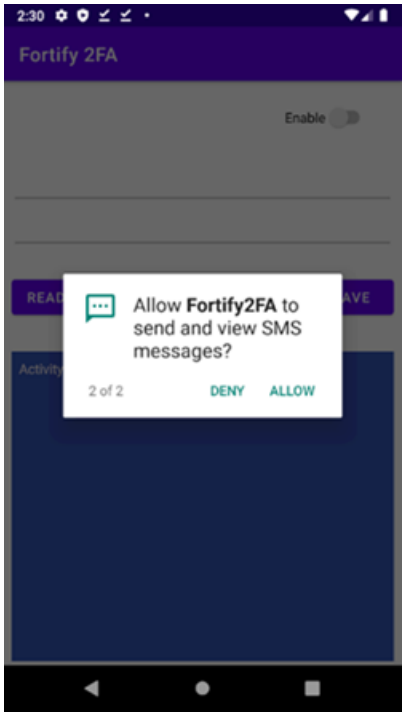


11. [開く]をクリックします。
写真やビデオ撮影の許可を要求するプロンプトが表示されます。

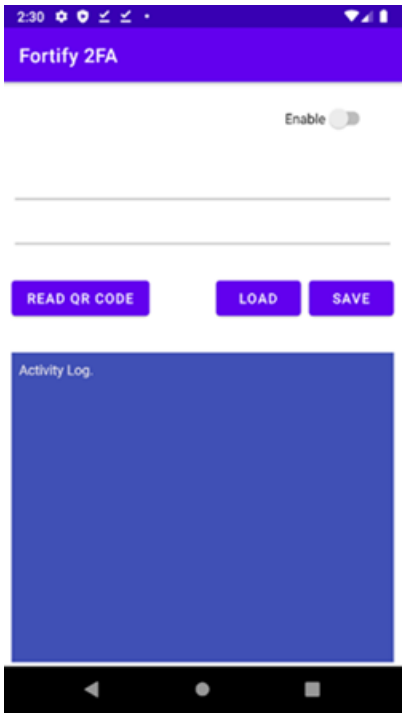


12. [許可]をクリックします。

SMSメッセージの送信と閲覧の許可を要求するプロンプトが表示されます。



13. **[許可]**をクリックします。
アプリを設定する準備が整いました。



14. **[QRコードの読み込み]**をクリックして、**2要素認証モバイルアプリケーション**設定のQRコードをスキャンします。
2要素認証設定は、**Fortify2FA**モバイルアプリケーションで設定されます。

アプリケーション設定:ログ記録

この機能にアクセスするには、**[編集(Edit)] > [アプリケーション設定(Application Settings)]** をクリックしてから、**[ログ記録(Logging)]** を選択します。

[ログ記録(Logging)] のオプションの説明を次の表に示します。

オプション	説明
ログのクリア(Clear Logs)	このボタンをクリックすると、すべてのログがクリアされます。
最小ログレベル(Minimum Logging Level)	OpenText DASTがアプリケーション内で発生するさまざまな機能とイベントをログに記録する方法を指定します。選択肢は、[デバッグ(Debug)]、[情報(Info)]、[警告(Warn)]、[エラー(Error)]、および[重大(Fatal)](詳細度の高いものから低いものの順)です。
ログパージのしきい値(Threshold for Log Purging)	**[パージしない(Never Purge)]** を選択しないと、すべてのログによって使用されているディスク容量の合計が指定のサイズを超えた場合、またはログの数が指定の数を超えた場合に、OpenText DASTによってすべてのログが削除されます。または、ログファイルを **[パージしない(Never Purge)]** を選択することもできます。
ローリングログファイルの最大サイズ(Rolling Log File Maximum Size)	個々のログファイルに割り当てる最大サイズをキロバイト単位で指定します。ファイルがこの制限に達すると、OpenText DASTは単純にそのファイルへの書き込みを停止します。

アプリケーション設定:プロキシ

この機能にアクセスするには、**[編集(Edit)] > [アプリケーション設定(Application Settings)]** をクリックしてから、**[プロキシ設定(Proxy Settings)]** を選択します。

OpenText DAST Webサービスは、アップデートとサポートのコミュニケーションに使用されます。[プロキシ設定(Proxy Settings)] でこれらのサービスへのアクセス方法を設定します。

プロキシサーバを使用しない

これらのサービスへのアクセスにプロキシサーバを使用しない場合は、**[直接接続(プロキシ無効)(Direct Connection (proxy disabled))]** を選択します。

プロキシサーバを使用する

プロキシサーバを使用してこれらのサービスにアクセスする必要がある場合は、次の表に示すオプションを選択します。

オプション	説明
プロキシ設定の自動検出(Auto detect proxy settings)	WPAD (Web Proxy Autodiscovery)プロトコルを使用してプロキシ自動設定ファイルを探し、ブラウザのWebプロキシ設定を行います。
システムのプロキシ設定を使用する(Use System Proxy settings)	ローカルマシンからプロキシサーバ情報をインポートします。 **注記:** システムのプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Windowsの[LANにプロキシサーバを使用する]設定が選択されていない場合、プロキシは使用されません。
Firefoxプロキシ設定を使用する(Use Firefox proxy settings)	Firefoxからプロキシサーバ情報をインポートします。 **注記:** Firefoxプロキシ設定を使用することにしても、プロキシサーバ経由のインターネットアクセスが保証されるわけではありません。Firefoxブラウザの接続設定が「プロキシーを使用しない」に設定されている場合、プロキシは使用されません。
PACファイルを使用してプロキシを設定する(Configure a proxy using a PAC file)	[URL]ボックスで指定した場所にあるPAC (Proxy Automatic Configuration)ファイルからプロキシ設定をロードします。
プロキシを明示的に設定する(Explicitly configure proxy)	要求された情報を入力することによって、プロキシを設定します。このトピックの「"プロキシの設定" 下」を参照してください。

プロキシの設定

プロキシを設定するには:

1. [**サーバ(Server)**]ボックスにプロキシサーバのURLまたはIPアドレスを入力し、続いて([**ポート(Port)**]ボックスに)ポート番号(8080など)を入力します。
2. [**タイプ(Type)**]リストから、プロキシサーバ経由のTCPトラフィックを処理するプロトコル(SOCKS4、SOCKS5、または標準)を選択します。

重要! {/b}SOCKS4またはSOCKS5プロキシサーバ設定を使用する場合は、スマートアップデートが使用できません。スマートアップデートは、標準プロキシサーバを使用する場合にのみ使用できます。

3. 認証が必要な場合は、 **認証(Authentication)**]リストからタイプを選択します。オプションは次のとおりです。
   - **自動**

     注記: 自動検出を指定すると、スキャンの処理が遅くなります。把握している別の認証メソッドを指定すると、スキャンのパフォーマンスは大幅に向上します。
   - **ダイジェスト**
   - **HTTP基本(HTTP Basic)**
   - **NT LAN Manager (NTLM)**
   - **Kerberos**
   - **ネゴシエート(Negotiate)**
4. プロキシサーバで認証が必要な場合は、適格なユーザ名とパスワードを入力します。

アプリケーション設定:レポート

この機能にアクセスするには、 **編集(Edit)]> [アプリケーション設定(Application Settings)]** をクリックしてから、 **[レポート(Reports)]**を選択します。

オプション

レポートオプションの説明を次の表に示します。

オプション	説明
常にお気に入りを保存するように要求する(Always prompt to save favorites)	「お気に入り」は、1つ以上のレポートとその関連パラメータの単なる名前付きコレクションです。Report Generatorを使用する場合は、レポートとパラメータを選択してから、 **[お気に入り(Favorites)]> [お気に入りに追加(Add to favorites)]**を選択して組み合わせを作成できます。このオプションを選択すると、レポートを追加または削除してお気に入りが変更されるたびに、それを保存するようOpenText DASTから要求されます。
脆弱性テキストのスマート切り捨て(Smart truncate vulnerability text)	生成されたレポートに、非常に長いHTTP要求メッセージと応答メッセージが含まれている場合があります。スペースを節約し、脆弱性に関連する適切なデータに焦点を当てるために、脆弱性を識別または確認するデータ(赤い強調表示で識別)の前後のメッセージコ

オプション	説明
	ンテンツを除外できます。 次の例では、「スマート」切り捨てと20文字のパディングサイズを使用したクロスサイトスクリプティング脆弱性のレポートを示します。ヘッダは常に全体が報告されます。残りのメッセージテキストは、脆弱性、その前の20文字、およびその後の20文字を除き、削除されます。保持されたテキストは、「...TRUNCATED...」という表記で囲まれます。これによって、切り捨てが発生したことを示します。オリジナルのメッセージの長さは、2,377文字(Content-Length: 2377)だったことに注意してください。 **Response:** `HTTP/1.1 200 OK` `Date: Tue, 04 Aug 2009 17:35:10 GMT` `Server: Microsoft-IIS/6.0` `X-Powered-By: ASP.NET` `Content-Length: 2377` `Content-Type: text/html` `Cache-control: private` `...TRUNCATED...l>Household Checking<script>alert(53316)</script></td>` `</tr>` `<tr>...TRUNCATED...` レポートでスマート切り捨てを使用するには、 **[脆弱性テキストのスマート切り捨て(Smart truncate vulnerability text)]** を選択してから、脆弱性を識別または確認するデータの前後に保持する文字数を指定します。1つの要求または応答で最大10件の脆弱性を報告できます。 **注記:** この機能が説明どおりに機能するのは、RequestTextデータフィールドとResponseTextデータフィールドを含むレポートコントロールのTruncateVulnerabilityプロパティがTrueに設定され、MaxLengthプロパティが0に設定されている場合のみです。TruncateVulnerabilityがTrueに設定され、MaxLengthプロパティが0以外の場合は、パディングサイズのアプリケーション設定がMaxLength値によって上書きされます。

ヘッダとフッタ

すべてのレポートでデフォルトで使用されるヘッダとフッタを含むテンプレートを選択します。また、必要に応じて、要求されたパラメータを入力します。

OpenText DAST Master Reportは、次のイメージを使用してレポートを作成します。

- カバーページのイメージはカバーページの中央に表示されます。イメージの上辺が一番上から約3.5インチの位置に表示されます。

- ヘッダロゴのイメージは、各ページのヘッダの左側に表示されます。

アプリケーション設定:センサとしての実行

この機能にアクセスするには、**[編集(Edit)]** > **[アプリケーション設定(Application Settings)]** をクリックしてから、**[センサとしての実行(Run as a Sensor)]** を選択します。

センサ

この設定情報は、OpenText DASTをセンサとしてFortify WebInspect Enterpriseに統合するために使用されます。情報を入力してセンササービスを開始したら、OpenText DASTグラフィカルユーザインタフェースではなく、Fortify WebInspect Enterpriseコンソールを使用してスキャンを実行する必要があります。

次の表に、オプションの説明を示します。

オプション	説明
マネージャURL (Manager URL)	Fortify WebInspect Enterprise ManagerのURLまたはIPアドレスを入力します。
センサ認証(Sensor Authentication)	ユーザ名(ドメイン\ユーザ名の形式)とパスワードを入力してから、**[テスト(Test)]** をクリックしてエントリを検証します。
プロキシの有効化 (Enable Proxy)	OpenText DASTがプロキシサーバを経由して、Fortify WebInspect Enterprise Managerにアクセスする必要がある場合は、**[プロキシの有効化(Enable Proxy)]** を選択してから、サーバのIPアドレスとポート番号を入力します。認証が必要な場合は、有効なユーザ名とパスワードを入力します。
データベース設定の上書き(Override Database Settings)	通常、OpenText DASTは、スキャンデータをデータベースコネクティビティ用のアプリケーション設定で指定されたデバイスに保存します。詳細については、「"アプリケーション設定:データベース" ページ 484」を参照してください。 ただし、OpenText DASTがセンサとしてFortify WebInspect Enterpriseに接続されている場合は、このオプションを選択してから、**[設定(Configure)]** をクリックして代替デバイスを指定できます。詳細については、「"アプリケーション設定:SQLデータベース設定の上書き" 次のページ」を参照してください。
サービスアカウント (Service Account)	次のいずれかのオプションを選択して、サービスを実行するアカウントを指定します。 • **ローカルシステムアカウント(Local system account)**:

オプション	説明
	LocalSystemアカウントは、サービスコントロールマネージャによって使用される定義済みのローカルアカウントです。このサービスは、ローカルリソースに無制限にアクセスできます。 • **このアカウント(This account)**: アカウントを特定し、パスワードを提供します。
センサステータス(Sensor Status)	このエリアにはセンササービスの現在のステータスが表示され、サービスを開始または停止するためのボタンが表示されます。 OpenText DASTをセンサとして設定したら、 **開始(Start)**]をクリックします。 **注記:** 通常、OpenText DASTがセンサとして設定されている場合は、OpenText DASTをスタンドアロンアプリケーションとして起動すると、センササービスが停止します。その後、OpenText DASTを閉じると、サービスが再起動して、再び、OpenText DASTをFortify WebInspect Enterprise Managerの制御下に置きます。ただし、OpenText DASTをスタンドアロンアプリケーションとして実行している間にスマートアップデートを実行した場合、サービスは自動的に再起動されません。 **開始(Start)**]ボタンをクリックする(または、タスクバーの通知エリアにあるFortifyアイコンを右クリックして **センサの開始(Start Sensor)**]を選択する)必要があります。

アプリケーション設定:SQLデータベース設定の上書き

この機能にアクセスするには、 **編集(Edit)]> アプリケーション設定(Application Settings)]> センサとして実行(Run as a Sensor)]> 設定(Configure)]**をクリックします。

データベース設定の上書き(Override database settings)

通常、OpenText DASTは、スキャンデータをデータベースコネクティビティ用のアプリケーション設定で指定されたデバイスに保存します。詳細については、「"アプリケーション設定:データベース" ページ484」を参照してください。

ただし、OpenText DASTがセンサとしてFortify WebInspect Enterpriseに接続されている場合は、このオプションを選択してから、 **設定(Configure)**]をクリックして代替デバイスを指定できます。詳細については、「"アプリケーション設定:センサとしての実行" 前のページ」を参照してください。

SQLデータベースの設定

センサとしてのOpenText DASTのSQLデータベース設定を行うには:

1. [アプリケーション設定(Application Settings)]ウィンドウで、**[データベース設定の上書き(Override Database Settings)]**を選択し、**[設定(Configure)]**をクリックします。
   [SQL設定(Configure SQL Settings)]ダイアログボックスが表示されます。
2. 次のいずれかのオプションを選択します。
   - **SQL Server Expressを使用する(Use SQL Server Express)**
   - **SQL Serverを使用する(Use SQL Server)**
3. **[SQL Server Expressを使用する(Use SQL Server Express)]**を選択した場合は、**[OK]**をクリックしてタスクを完了し、[アプリケーション設定(Application Settings)]ウィンドウに戻ります。
4. **[SQL Serverを使用する(Use SQL Server)]**を選択した場合は、**[サーバ名(Server Name)]**を入力するか、リストからサーバ名を選択します。
5. サーバ名を更新するには、**[更新(Refresh)]**クリックします。
6. [サーバにログオンする(Log on to the server)]エリアで、次のいずれかの認証オプションを選択します。
   - **Windows認証を使用する(Use Windows Authentication)**
   - **SQL Server認証を使用する(Use SQL Server Authentication)**
7. **[ユーザ名(User name)]**と**[パスワード(Password)]**を入力して、サーバにログオンします。[データベースに接続する(Connect to a Database)]エリアで、リストから**データベース名を選択または入力する**か、**[新規(New)]**をクリックしてデータベースを参照します。
8. **[OK]**をクリックします。

アプリケーション設定:スマートアップデート

この機能にアクセスするには、**[編集(Edit)]>[アプリケーション設定(Application Settings)]**をクリックしてから、**[スマートアップデート(Smart Update)]**を選択します。

オプション

[スマートアップデート(Smart Update)]のオプションの説明を次の表に示します。

オプション	説明
言語	SecureBaseのセキュリティとレポートのコンテンツをローカライズする言語を選択します。詳細については、「"別の言語の選択" 次のページ」を参照してください。

オプション	説明
サービス(Service)	スマートアップデートサービスのURLを入力します。デフォルト値は: https://smartupdate.fortify.microfocus.com/
起動時にスマートアップデートを有効にする(Enable Smart Update on Startup)	このオプションを選択すると、OpenText DASTの起動時にアップデートが自動的にチェックされます。

オフラインのOpenText DASTの更新手順を含む詳細については、"SmartUpdate" ページ324を参照してください。

別の言語の選択

セキュリティとレポートのコンテンツに別の言語を選択するときは、OpenText DASTで元のSecureBaseコンテンツをアーカイブし、新しいSecureBaseを作成し、SmartUpdateを実行して、ローカライズされたコンテンツを新しいSecureBaseに取り込みます。新しいSecureBaseインスタンスを使用するには、その後でOpenText DASTを再起動する必要があります。

別の言語を選択するには:

1. [**言語(Language)**]リストからターゲット言語を選択します。
2. [**OK**]をクリックします。
   警告ダイアログボックスが表示され、SmartUpdateを実行するよう求められるとともに、OpenText DASTが再起動して新しいSecureBaseインスタンスに変更されることが通知されます。

   注記: 空のSecureBaseにデータが取り込まれた後で言語を切り替える場合、更新されたチェックデータを利用できることがOpenText DASTによって検出されると、SmartUpdateを実行することが求められます。それに加えて、言語を切り替えると、OpenText DASTの再起動が必要です。
3. 次のいずれかを実行します。
   - 新しいSecureBaseを作成するには、ローカライズされたコンテンツをこの新しいSecureBaseに取り込み、OpenText DASTを再起動し、[**OK**]をクリックします。
   - このプロセスをキャンセルして元のSecureBaseを使用し続けるには、[**キャンセル(Cancel)**]をクリックします。

アプリケーション設定: サポートチャネル

この機能にアクセスするには、[**編集(Edit)**] > [**アプリケーション設定(Application Settings)**]をクリックしてから、[**サポートチャネル(Support Channel)**]を選択します。

OpenText DASTサポートチャネルを使用すると、OpenText DASTがOpenTextに対してデータを送信したり、メッセージをダウンロードしたりできるようになります。これは、主に、ログと「誤検出」レポートの送信や「新機能」通知の受信に使用されます。

サポートチャネルを開く

[OpenTextへの接続を許可する(Allow connection to OpenText)]オプションを選択して、OpenText DASTサポートチャネルを開きます。その後で、次の項目を指定できます。

- サポートチャネルURL (Support Channel URL) -デフォルトは次のとおりです。
  https://supportchannel.fortify.microfocus.com/service.asmx
- アップロードディレクトリ(Upload Directory) -デフォルトは次のとおりです。
  C:\ProgramData\HP\HP WebInspect\SupportChannel\Upload\
- ダウンロードディレクトリ(Download Directory) -デフォルトは次のとおりです。
  C:\ProgramData\HP\HP WebInspect\SupportChannel\Download\

アプリケーション設定: OpenText ALM

この機能にアクセスするには、 [編集(Edit)] > [アプリケーション設定(Application Settings)]をクリックしてから、 [OpenText ALM]を選択します。

OpenText DASTとOpenText Application Lifecycle Management (ALM)を統合するには、ALMサーバ、プロジェクト、欠陥の優先度、およびその他の属性を記述した1つ以上のプロファイルを作成する必要があります。次いで、OpenText DASTの脆弱性をALM欠陥に変換して、ALMデータベースに追加できます。

ALMライセンスの使用

プロファイルの作成や編集では、ALMに発行されたライセンスが使用されます。ただし、ALMアプリケーション設定を閉じると、ライセンスは解放されます。同様に、脆弱性をALMに送信すると、ライセンスが使用されますが、脆弱性の送信後には解放されます。

作業を開始する前に

プロファイルを作成する前に、ALMクライアント登録アドインがOpenText DASTと同じマシンにインストールされていることを確認してください。詳細については、ALMのマニュアルを参照してください。

プロファイルの作成

プロファイルを作成するには:

1. [追加(Add)]をクリックしてから、 [プロファイルの追加(Add Profile)]ダイアログボックスにプロファイル名を入力します。

2. ALMサーバのURLを入力または選択します。前にALMサイトを訪問したことがなければ、リストは空です。URLを入力するには、「http://<*qc-server*>/qcbin/」という形式を使用します。URLに「start_a.htm」(またはその他のファイル名)を追加しないでください。
3. サーバにアクセス可能なユーザ名とパスワードを入力し、 **認証(Authenticate)**]をクリックします。

   認証資格情報が受け入れられると、サーバによって **ドメイン(Domain)**]リストと **プロジェクト(Project)**]リストが設定されます。
4. **接続(Connect)**]をクリックしてから、 **欠陥報告(Defect Reporting)**]グループで件名を選択します。
5. **欠陥の優先度(Defect priority)**]リストから、このプロファイルを使用してALMに報告されるすべてのOpenText DAST脆弱性に割り当てられる優先度を選択します。
6. **欠陥の割り当て先(Assign defects to)**]リストを使用して欠陥を割り当てるユーザを選択してから、 **プロジェクトの発見場所(Project found in)**]リストでエントリを選択します。
7. 残りのリストを使用して、OpenText DAST脆弱性評価をALM欠陥評価にマップします。 **発行しない(Do Not Publish)**]を選択した場合は、脆弱性がエクスポートされません。少なくとも1つのファイルマッピングを選択する必要があります。
8. OpenText DAST脆弱性に関連付けられたメモとスクリーンショットをエクスポートするには、 **欠陥に対する脆弱性添付ファイルをアップロードする(Upload vulnerability attachments to defect)**]を選択します。
9. **必須/任意フィールド(Required/Optional Fields)**]グループでエントリをダブルクリックして、要求された情報を入力または選択します。必須フィールドを入力せずに作業を保存しようとすると、OpenText DASTが入力を要求します。

第10章:参照リスト

この章では、OpenText DASTのポリシー、スキャンログのメッセージ、およびHTTPステータスコードの一覧を示します。

OpenText DAST ポリシー

ポリシーとは、OpenText DASTがWebアプリケーションに対して展開する脆弱性チェックと攻撃手法のコレクションです。各ポリシーはSmartUpdate機能によって最新の状態に保たれます。こうして、スキャンの精度が確保されて、ごく最近発見された脅威も検出できるようになります。

OpenText DASTには、パッケージ化された次のポリシーが含まれています。これらを使用して、Webアプリケーションの脆弱性を判断できます。

注記: このリストは、製品に表示されるポリシーと一致しないことがあります。このドキュメントの執筆後にSmartUpdateによって追加または非推奨にされたポリシーが存在する場合があります。

OAST関連チェックについて

インターネットにアクセス可能なネットワークでは、OpenText DASTはOAST関連チェックの実行時にパブリックDNSサービスを使用します。ファイアウォールが**fortify-oast.net**へのアクセスをブロックしないことを確認してください。インターネットにアクセスできないネットワークでは、Fortify OAST on Dockerイメージを使用できます。詳細については、『*OpenText™ Dynamic Application Security TestingおよびOAST on Dockerユーザガイド*』を参照してください。

ベストプラクティス

ベストプラクティスグループには、Webアプリケーションに最も広く見られる厄介なセキュリティ上の脆弱性についてアプリケーションをテストするためのポリシーが含まれています。

- **API**: このポリシーには、APIセキュリティ評価に関連するさまざまな問題を対象としたチェックが含まれています。これには、各種のインジェクション攻撃、トランスポート層セキュリティ、およびプライバシー侵害が含まれますが、クライアントサイドの問題の検出のチェックや攻撃露呈部分の検出(ディレクトリ列挙やバックアップファイル検索のチェックなど)は含まれません。このポリシーによって検出される脆弱性はすべて、攻撃者から直接攻撃の的とされる可能性があります。このポリシーは、Web APIを使用するアプリケーションをスキャンするためのものではありません。
- **CWE Top 25 <バージョン>**: Common Weakness Enumeration (CWE) Top 25 Most Dangerous Software Errors (CWE Top 25)は、MITREが作成したリストです。このリストは、ソフトウェアの脆弱性につながるおそれのある、まん延の度合いと重大性が最も高いソ

フトウェアの弱点を示しています。

- **DISA STIG <バージョン>**: Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)には、アプリケーションの開発過程全体に関するセキュリティガイダンスがあります。このポリシーには、DISA STIG <バージョン>の安全なコーディングの要件をアプリケーションが満たすために役立つ選定されたチェックが含まれます。**ベストプラクティス**グループ内には、DISA STIGポリシーの複数のバージョンが存在する場合があります。
- **General Data Protection Regulation (GDPR)**: EU一般データ保護規則(GDPR、General Data Protection Regulation)は、データ保護指令95/46/ECに代わるものとして、組織が個人データを取り扱うための枠組みを提供しています。以下に挙げるGDPR条項は、アプリケーションセキュリティに関連しており、製品およびサービスの設計および開発中に個人データを保護することを企業に義務付けています。
  - 第25条「データ保護バイデザインおよびデータ保護バイデフォルト」。この条項により、企業は、各特定の処理の目的に必要な個人データのみを取り扱うことをデフォルトで保証するために、適切な技術的および組織的な手段を講じる必要があります。
  - 第32条「取り扱いの安全性」。この条項により、企業は、個人データの偶発的または不法な破壊、損失、改変、不正開示、または不正アクセスからシステムおよびアプリケーションを保護する必要があります。

  このポリシーには、特にGDPRのアプリケーションセキュリティに関連して個人データを特定および保護する上で役立つチェックが精選されています。
- **NIST-SP80053R5**: NIST Special Publication 800-53 Revision 5 (NIST SP 800-53 Rev.5)には、米国連邦政府の機関および情報システムをセキュリティ上の脅威から保護することを目的とするセキュリティ制御およびプライバシー制御のリストが指定されています。このポリシーには、NIST SP 800-53 Rev.5のガイドラインと規格を満たすために監査に含める必要がある選定されたチェックが含まれています。
- **OWASP API Top 10 <年>**: OWASP API Top 10 <年>は、特定の年の、APIに影響する上位のセキュリティリスクのリストを提供します。このリストは、APIセキュリティの脆弱性に関する認識を高め、WEB APIのセキュリティを確保する必要がある開発者、設計者、アーキテクト、マネージャ、組織などの、APIの開発および保守に関与する人々を教育することを目的としています。OWASP API Top 10は、Web APIに影響を与える脆弱性に焦点を当てており、単独での使用を目的としていません。むしろ、他の標準やベストプラクティスと組み合わせて使用することで、関連するすべてのリスクを包括的に捕捉することを目的としています。たとえば、インジェクションなどの入力検証に関連する問題を特定するには、これをOWASP Top 10と組み合わせて使用する必要があります。
- **OWASP Application Security Verification Standard (ASVS)**: Application Security Verification Standard (ASVS)は、設計者、開発者、テスト担当者、セキュリティ専門家、ツールベンダー、およびコンシューマが安全なアプリケーションを定義、作成、テスト、および検証するために使用できる、アプリケーションのセキュリティ要件またはセキュリティテストのリストです。

  このポリシーは、組み込むSecureBaseチェックの各カテゴリに、OWASP ASVSが提示するCWEマッピングを使用しています。CWEは階層的な分類であるため、このポリシーには、「ParentOf」関係を使用してOWASP ASVSが提示するCWEから暗黙的に指定される追加のCWEにマップするチェックも含まれています。

- **OWASP Top 10 <年>**: このポリシーは、Webアプリケーションセキュリティの最低限の基準を提供します。OWASP Top 10は、Webアプリケーションの最も重大なセキュリティ上の欠陥についての幅広いコンセンサスを表します。OWASP Top 10の採用は、おそらく、組織内のソフトウェア開発文化を安全なコードを生み出す文化へと変化させるための最も効果的な最初のステップと言えます。OWASP Top 10のポリシーには、複数のリリースが存在する場合があります。詳細については、「OWASP Top Ten Project」を参照してください。
- **SANS Top 25<年>**: SANS Top 25 Most Dangerous Software Errorsでは、ソフトウェアの深刻な脆弱性を引き起こす最も広く見られる重大なエラーをCWE (Common Weakness Enumeration) ID別に分類して列挙しています。多くの場合、これらのソフトウェアエラーは見つけるのも悪用するのも簡単です。これらのエラーにつきものの危険としては、攻撃者がソフトウェアを完全に乗っ取ったり、データを盗んだり、ソフトウェアを完全に停止させたりできるということがあります。
- **標準**: 標準スキャンは、サーバの自動Web探索を含んでおり、SQLインジェクションやクロスサイトスクリプトなどの既知と未知の脆弱性のチェックのほか、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層での不適切なエラー処理や脆弱なSSL設定についてのチェックを実行します。

タイプ別

タイプ別グループには、特定のアプリケーション層、脆弱性の種類、または汎用機能に焦点を絞って設計されたポリシーが含まれます。たとえば、アプリケーションポリシーには、オペレーティングシステムではなくアプリケーションをテストする目的で設計されたすべてのチェックが含まれます。

- **積極的なSQLインジェクション**: このポリシーは、SQLインジェクションの脆弱性に対するWebアプリケーションのセキュリティを総合的に評価します。SQLインジェクションとは、入力が検証されないという脆弱性を利用してWebアプリケーションから任意のSQLクエリやコマンドを渡し、バックエンドのデータベースで実行させるという攻撃手法です。このポリシーを使用すると、より正確で確実になりますが、スキャン時間は長くなります。
- **Apache Struts**: このポリシーは、Apache Strutsフレームワークに対する、サポートされている既知のアドバイザリを検出します。
- **ブランク**: このポリシーは、ユーザが独自のポリシーを作成するために使用できるテンプレートです。サーバの自動クロールを含み、脆弱性チェックを行いません。このポリシーを編集して、特定の脆弱性のみをスキャンするカスタムポリシーを作成できます。
- クライアント側: このポリシーは、攻撃者が攻撃を仕掛けるためにフィッシングを行うことが必要となるすべての問題を検出することを目的としています。それらの問題は通常はクライアント側に現れるので、フィッシングが必要となります。これには、反射型クロスサイトスクリプティングのチェックと、さまざまなHTML5のチェックが含まれます。このポリシーをサーバ側ポリシーと組み合わせて使用することで、クライアントとサーバの両方をカバーすることができます。 This policy intends to detect all issues that require an attacker to perform phishing in order to deliver an attack. These issues are typically manifested on the client, thus enforcing the phishing requirement. This includes Reflected Cross-site Scripting and various HTML5 checks. This policy may be used in conjunction with the Server-side policy to provide coverage across both the client and the server.

- **重大および高**: 重大および高のポリシーは、運用サーバを危険にさらすことなく、差し迫った緊急の脆弱性を検出するためにWebアプリケーションを迅速にスキャンする場合に使用します。このポリシーは、SQLインジェクションやクロスサイトスクリプティングなど、重大度が「重大」および「高」の脆弱性をチェックします。これは、データベースにデータを書き込んだり、サービス拒否状態を生じさせたりする可能性があるチェックは含んでいないため、運用サーバに対して安全に実行できます。
- **クロスサイトスクリプティング**: このポリシーは、XSS(クロスサイトスクリプティング)の脆弱性について、Webアプリケーションのセキュリティスキャンを実行します。XSSとは、攻撃者が提供した実行可能コード(HTMLコードやクライアント側スクリプトなど)をWebサイトにエコーさせて、ユーザのブラウザにそのコードをロードする攻撃手法です。このような攻撃は、アクセス制御の回避やフィッシング詐欺に利用される可能性があります。
- **DISA STIG *<バージョン>***: Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG)には、アプリケーションの開発過程全体に関するセキュリティガイダンスがあります。このポリシーには、DISA STIG *<バージョン>*の安全なコーディングの要件をアプリケーションが満たすために役立つ選定されたチェックが含まれます。**タイプ別**グループには、DISA STIGポリシーの複数のバージョンが存在する場合があります。
- **モバイル**: モバイルスキャンは、モバイルアプリケーションとそれをサポートするバックエンドサービスの間で観察された通信に基づいて、セキュリティ上の欠陥を検出します。
- **NoSQLおよびNode.js**: このポリシーは、サーバの自動Web探索を含んでおり、NoSQLベースのデータベース(MongoDBなど)や、JavaScriptベースのサーバ側インフラストラクチャ(Node.jsなど)を対象にした既知と未知の脆弱性のチェックを実行します。
- **OAST**: このポリシーには、スキャンロジックでOut-of-Band Application Security Testing技術を使用するすべてのチェックが含まれています。

  注記: インターネットにアクセス可能なネットワークでは、OpenText DASTはパブリックDNSサービスを使用します。インターネットにアクセスできないネットワークでは、Fortify OAST on Dockerイメージを使用できます。詳細については、『*OpenText™ Dynamic Application Security TestingおよびOAST on Dockerユーザガイド*』を参照してください。

- **パッシブスキャン**: パッシブスキャンポリシーは、積極的なエクスプロイトを発生させなくても検出可能なアプリケーションの脆弱性をスキャンします。したがって、運用サーバに対しても安全に実行できます。このポリシーによって検出される脆弱性には、パスの開示の問題、エラーメッセージの問題、および類似した性質を持つその他の問題が含まれます。
- **PCI DSS 4.0**: Payment Card Industry Data Security Standard 4.0 (PCI DSS 4.0: ペイメントカード業界データセキュリティ基準4.0)は、顧客データを保護するために設計された技術要件と運用要件のベースラインを提供します。このポリシーには、PCI DSS 4.0の安全なコーディングの要件を満たすために監査に含める必要があるチェックが含まれています。
- **PCI Software Security Framework *<バージョン>* (PCI SSF *<バージョン>*)**: PCI SSFは、安全な支払いシステムと支払いトランザクション処理ソフトウェアを作成するための要件とガイダンスのベースラインを提供します。このポリシーには、PCI SSFの安全なコーディングの要件を満たすために監査に含める必要があるチェックが含まれています。
- **権限のエスカレーション**: 権限のエスカレーションのポリシーは、攻撃者がデータやアプリケーションへの昇格されたアクセス権を獲得することを許してしまうプログラミングエラーや設計上の欠陥を検出するために、Webアプリケーションをスキャンします。このポリシーは、同一の

要求をさまざまな特権レベルで実行してその応答を比較するチェックを実行します。

- サーバ側: このポリシーには、サーバ側アプリケーションのさまざまな問題を対象とするチェックが含まれています。これには、さまざまなインジェクション攻撃、トランスポート層のセキュリティ、およびプライバシー侵害が含まれますが、ディレクトリ列挙やバックアップファイルの検索などのアタックサーフェスの検出は含まれません。この**ポリシー**によって検出される脆弱性はすべて、攻撃者から直接攻撃の的とされる可能性があります。このポリシーをクライアント側ポリシーと組み合わせて使用することで、クライアントとサーバの両方をカバーすることができます。 This policy contains checks that target various issues on the server-side of an application. This includes various injection attacks, transport layer security, and privacy violation, but does not include attack surface discovery such as directory enumeration or backup file search. All vulnerabilities detected by this policy may be directly targeted by an attacker. This policy may be used in conjunction with the Client-side policy to provide coverage across both the client and the server.
- **SQLインジェクション**: SQLインジェクションポリシーは、SQLインジェクションの脆弱性について、Webアプリケーションのセキュリティスキャンを実行します。SQLインジェクションとは、入力が検証されないという脆弱性を利用してWebアプリケーションから任意のSQLクエリやコマンドを渡し、バックエンドのデータベースで実行させるという攻撃手法です。
- **トランスポート層セキュリティ**: このポリシーは、安全でないSSL/TLS設定や、トランスポート層の重大なセキュリティ脆弱性(Heartbleed攻撃、Poodle攻撃、SSL再ネゴシエーション攻撃など)について、Webアプリケーションのセキュリティ評価を実行します。
- **WebSocket**: このポリシーは、アプリケーション内のWebSocket実装に関連する脆弱性を検出します。

カスタム

カスタムグループには、ユーザが作成したすべてのポリシーと、ユーザが変更したカスタムポリシーが含まれます。

危険

危険グループには、運用サーバの障害を引き起こす可能性があるサービス拒否攻撃などの危険をはらんだチェックを含んでいるポリシーが含まれます。このポリシーは、運用以外のサーバおよびシステムのみに使用してください。

- **全チェック**: 全チェックスキャンには、サーバの自動Web探索が含まれており、データベースであるSecureBaseのアクティブなすべてのチェックを実行します。このスキャンには、FortifyのWebアプリケーションとWebサービスの脆弱性のスキャンのための製品で利用可能なコンプライアンスレポートにリストされるすべてのチェックが含まれます。これには、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層での既知と未知の脆弱性のチェックが含まれます。

  注意! {/b}全チェックスキャンには、データベースにデータを書き込んだり、フォームを送信したり、サービス拒否状態を発生させたりする可能性のあるチェックが含まれています。全チェックポリシーはテスト環境でのみ使用することを強くお勧めします。

非推奨になったチェックおよびポリシー

以下のポリシーとチェックは非推奨となっており、保守されていません。

- **積極的なLog4Shell (非推奨)**: このポリシーは、脆弱なバージョンのApache Log4jライブラリにおけるjNDI参照インジェクションに対するWebアプリケーションのセキュリティを総合的に評価します。脆弱なバージョンのLog4jでは、JNDI機能が制限されません。このため、ログメッセージを制御できる攻撃者は、攻撃者の制御下にあるサーバを指したJNDI参照を挿入できるようになります。これは、脆弱なターゲット上でのリモートコード実行につながりかねません。このポリシーを使用すると、Log4Shellエージェントを含むその他のポリシーと比較して、より正確で確実になりますが、多数の要求が生成されるため、スキャン時間は長くなります。
- **アプリケーション(非推奨)**: アプリケーションポリシーは、既知および未知のWebアプリケーション攻撃を送信することで、Webアプリケーションのセキュリティスキャンを実行し、アプリケーション層を評価する特定の攻撃のみを送信します。エンタープライズレベルのWebアプリケーションのスキャンを実行する場合は、アプリケーションのみのポリシーをプラットフォームのみのポリシーと組み合わせて使用することで、スキャンの速度とメモリ使用量を最適化してください。
- **攻撃(非推奨)**: 攻撃スキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で既知および未知の脆弱性のチェックを実行します。アサルトスキャンには、サービス拒否状態を作り出す可能性のあるチェックが含まれます。攻撃スキャンはテスト環境でのみ使用することを強くお勧めします。
- **非推奨のチェック**: テクノロジのライフサイクルが終わりに向かい、技術動向から姿を消していくのに従い、実質的に不要になったチェックをポリシーから削除する必要があります。非推奨のチェックポリシーには、現在の技術的状況に基づいて役目を終えたと見なされたチェックや、コアOpenText DASTフレームワークの最近の拡張機能を活用するスマートで効率的な監査アルゴリズムを使用して再実装されたチェックが含まれます。
- **開発者(非推奨)**: 開発者スキャンには、サーバの自動Web探索が含まれており、Webアプリケーション層に限定した既知および未知の脆弱性のチェックを実行します。このポリシーは、サービス拒否状態を引き起こす可能性のあるチェックは実行しないので、運用システムで安全に実行できます。
- **OpenSSL Heartbleed(非推奨)**: このポリシーは、重大なTLSハートビート読み取りオーバーランの脆弱性について、Webアプリケーションのセキュリティ評価を実行します。この脆弱性により、悪意のあるユーザが、サイトをホストしているサーバに不正な形式のハートビート要求を送信した場合に、サーバメモリ内の重要なサーバおよびWebアプリケーションのデータが漏えいする可能性があります。
- **OWASP Top 10 Application Security Risks - 2010 (非推奨)**: このポリシーは、Webアプリケーションセキュリティの最低限の基準を提供します。OWASP Top 10は、Webアプリケーションの最も重大なセキュリティ上の欠陥についての幅広いコンセンサスを表します。OWASP Top 10の採用は、おそらく、組織内のソフトウェア開発文化を安全なコードを生み出す文化へと変化させるための最も効果的な最初のステップと言えます。このポリシーには、2010 Top 10リストに固有の要素が含まれています。詳細については、「OWASP Top Ten Project」を参照してください。

- **プラットフォーム(非推奨)**: このポリシーは、特にWebサーバおよび既知のWebアプリケーションに対して攻撃を送信することで、Webアプリケーションプラットフォームのセキュリティスキャンを実行します。エンタープライズレベルのWebアプリケーションのスキャンを実行する場合は、プラットフォームのみのポリシーをアプリケーションのみのポリシーと組み合わせて使用することで、スキャンの速度とメモリ使用量を最適化してください。
- **QA(非推奨)**: このポリシーは、QA担当者がWebアプリケーションセキュリティの観点からプロジェクトリリースの決定を下すのに役立ちます。これは、Webアプリケーションの既知および未知の脆弱性のチェックを実行します。ただし、危険性をはらんだチェックは実行しないため、運用システムで安全に実行できます。
- **クイック(非推奨)**: このスキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で、メジャーパッケージの既知の脆弱性と未知の脆弱性のチェックを実行します。クイックスキャンは、サービス拒否状態を生じさせる可能性のあるチェックは実行しないため、運用システムで安全に実行できます。
- **セーフ(非推奨)**: セーフスキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で、メジャーパッケージの既知の脆弱性のほとんどと、未知の脆弱性のいくつかについてのチェックを実行します。セーフスキャンは、機密性の高いシステムでも、サービス拒否状態を引き起こす可能性のあるチェックは実行しません。
- **標準(非推奨)**: 標準(非推奨)ポリシーは、R1 2015リリースで改訂される前のもともとの標準ポリシーと同じものです。標準スキャンには、サーバの自動Web探索が含まれており、Webサーバ層、Webアプリケーションサーバ層、およびWebアプリケーション層で既知および未知の脆弱性のチェックを実行します。標準スキャンは、サービス拒否状態を生じさせる可能性のあるチェックは実行しないため、運用システムで安全に実行できます。

スキャンログのメッセージ

このトピックでは、スキャンログに表示されるメッセージについて説明します。メッセージはアルファベット順に並んでいます。

注記: スキャンログのアラートレベルのメッセージについては、"アラートのトラブルシューティング" ページ545を参照してください。

監査エンジン初期化のエラー

メッセージ全体

Audit Engine initialization error, engine:%engine%, error:%error%" (監査エンジン初期化のエラー、エンジン:%engine%、エラー:%error%")

説明

監査エンジンの初期化中に回復不可能なエラーが発生しました。カスタマサポートへのお問い合わせ

引数の説明

Engine: 初期化を試行したエンジン。

Error: 実際に発生したエラー。

考えられる解決策

該当なし

外部リンク

該当なし

監査エラー

メッセージ全体

Error: Auditor error, session: <session ID> engine:<engine>, error:<error> (エラー: 監査エラー、セッション: <session ID> エンジン:<engine>、エラー:<error>)

説明

監査中にエラーが発生しました。

引数の説明

Session: エラーが発生した際に監査中だったセッション。

Engine: エラーが発生した際に実行されていたエンジン。

Error: 実際に発生したエラー。

考えられる解決策

該当なし

外部リンク

該当なし

自動応答状態の失敗

メッセージ全体

Auto Response State Fail detected. (自動応答状態の失敗が検出されました。)Please add response state rule. (応答状態ルールを追加してください。)

説明

状態の自動検出は失敗しましたが、要求で`Authorization: Bearer`が識別されました。

考えられる解決策

トークンがスタティックトークン値である場合は、このアラートを無視します。

トークンがダイナミックである場合は、応答状態ルールを作成します。詳細については、「"スキャン設定: HTTP解析" ページ422」を参照してください。

外部リンク

該当なし

チェックエラー

メッセージ全体

Error: Check error, session:8BE3AFEC5051507168B66AEC59C8915B, Check:10346, engine: SPI.Scanners.Web.Audit.Engines.RequestModify (エラー: チェックエラー、セッション:8BE3AFEC5051507168B66AEC59C8915B、チェック:10346、エンジン: SPI.Scanners.Web.Audit.Engines.RequestModify)

説明

チェックの処理中にエラーが発生しました。

引数の説明

Session: チェックエラーが発生したセッション。

Check: 問題が発生したチェック。

Engine: エラーが発生した際に実行されていたエンジン。

Error: エラー。

考えられる解決策

SmartUpdateの最新バージョンをインストールします。

外部リンク

該当なし

完了したスキャン後分析モジュール

メッセージ全体

Completed Post-Scan Analysis Module: %module% (完了したスキャン後分析モジュール: %module%)

説明

スキャン後分析モジュールの1つが終了しました。

引数の説明

module: スキャン後分析モジュールの名前。

考えられる解決策

該当なし

外部リンク

該当なし

Web探索と監査の同時実行の開始

メッセージ全体

Info:Concurrent Crawl and Audit Start (情報:Web探索と監査の同時実行の開始)

説明

このメッセージは、Web探索と監査の同時実行が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

Web探索と監査の同時実行の停止

メッセージ全体

Info:Concurrent Crawl and Audit Stop (情報: Web探索と監査の同時実行の停止)

説明

このメッセージは、Web探索と監査の同時実行が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

Web探索の同時実行の開始

メッセージ全体

Info:Concurrent Crawl Start: (情報: Web探索の同時実行の開始)

説明

このメッセージは、Web探索の同時実行が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

Web探索の同時実行の停止

メッセージ全体

Info:Concurrent Crawl Stop (情報: Web探索の同時実行の停止)

説明

このメッセージは、Web探索の同時実行が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

コネクティビティの問題、理由

メッセージ全体

Connectivity issue, Reason: FirstRequestFailed, HTTP Status:404, (コネクティビティの問題、理由: FirstRequestFailed、HTTPステータス:404)

説明 このメッセージは、ネットワークのコネクティビティの問題を示しています。OpenText DASTがリモートホストと通信できませんでした。

引数の説明

Reason: FirstRequestFailed -要求が失敗しました。
HTTP Status: 404 -失敗した要求に対して返されたステータス。

考えられる解決策

- ネットワークハードウェアの電源サイクル
  問題が解決しない場合は、モデムとルータの電源を抜いてから数秒待ち、もう一度差し込みます。場合によっては、これらのデバイスの更新が必要なことがあります。ネットワークの障害、またはネットワーク設定が間違っていることが原因である場合があります。
- Microsoftのネットワーク診断ツールを使用する
  通知エリアのネットワークアイコンを右クリックして [ネットワーク診断]を開き、 [診断と修復]をクリックします。

- ケーブルの確認
  すべてのケーブルが正しく接続されていることを確認します。
- ホストの電源の確認
  別のコンピュータに接続しようとしている場合は、そのコンピュータの電源が入っていることを確認します。
- 接続設定の確認
  新しいソフトウェアをインストールした後に問題が発生した場合は、接続設定が変更されていないか確認してください。 [スタート]ボタン、 [コントロールパネル]、 [ネットワークとインターネット]、 [ネットワークと共有センター]、 [ネットワーク接続の管理]の順にクリックして、 [ネットワーク接続]を開きます。接続を右クリックして、 [プロパティ]をクリックします。管理者のパスワードまたは確認を求めるプロンプトが表示された場合は、パスワードを入力するか、確認します。
- すべてのファイアウォールのトラブルシューティング

外部リンク

ネットワーク接続に関する問題のトラブルシューティング

インターネットコネクティビティ評価ツール

コネクティビティの問題、理由、エラー

メッセージ全体

Connectivity issue, Reason:FirstRequestFailed, Error:Server:zero.webappsecurity.com:80, Error:(11001)Unable to connect to remote host : No such host is known: (コネクティビティの問題、理由:FirstRequestFailed、エラー:Server:zero.webappsecurity.com:80、エラー:(11001)リモートホストに接続できません: ホストが不明です:)

説明

このメッセージは、ネットワークのコネクティビティの問題を示しています。OpenText DASTがリモートホストと通信できませんでした。

引数の説明

Reason: FirstRequestFailed -要求が失敗しました。

Server: 要求が送信されたサーバ。

Error: (11001)Unable to connect to remote host : No such host is known: -コネクティビティの問題が原因で、リモートホストへの通信が失敗しました。

考えられる解決策

- ネットワークハードウェアの電源サイクル
  問題が解決しない場合は、モデムとルータの電源を抜いてから数秒待ち、もう一度差し込みます。場合によっては、これらのデバイスの更新が必要なことがあります。ネット

ワークの障害、またはネットワーク設定が間違っていることが原因である場合があります。

- Microsoftのネットワーク診断ツールを使用する
  通知エリアのネットワークアイコンを右クリックして [ネットワーク診断]を開き、 [診断と修復]をクリックします。
- ケーブルの確認
  すべてのケーブルが正しく接続されていることを確認します。
- ホストの電源の確認
  別のコンピュータに接続しようとしている場合は、そのコンピュータの電源が入っていることを確認します。
- 接続設定の確認
  新しいソフトウェアをインストールした後に問題が発生した場合は、接続設定が変更されていないか確認してください。 [スタート]ボタン、 [コントロールパネル]、 [ネットワークとインターネット]、 [ネットワークと共有センター]、 [ネットワーク接続の管理]の順にクリックして、 [ネットワーク接続]を開きます。接続を右クリックして、 [プロパティ]をクリックします。管理者のパスワードまたは確認を求めるプロンプトが表示された場合は、パスワードを入力するか、確認します。
- すべてのファイアウォールのトラブルシューティング

外部リンク

ネットワーク接続に関する問題のトラブルシューティング

インターネットコネクティビティ評価ツール

Web探索プログラムエラー

メッセージ全体

Error: Crawler error, session: <session ID> error:<error>(エラー: Web探索プログラムエラー、セッション: <session ID> エラー:<error>)

説明

Web探索プログラムがセッションの処理に失敗しました。ユーザは修正できません。カスタマサポートへのお問い合わせ

引数の説明

Session: エラーが発生したセッション。

Error: 実際のエラー。

考えられる解決策

該当なし

外部リンク

該当なし

データベースコネクティビティの問題

メッセージ全体

Error: SPI.Scanners.Web.Framework.Session in updateExisting,retries failed, giving up calling iDbConnetivityHandler.OnConnectivityIssueDetected (エラー: updateExistingのSPI.Scanners.Web.Framework.Session、再試行が失敗しました。iDbConnetivityHandler.OnConnectivityIssueDetectedの呼び出しをキャンセルします)

説明

このメッセージは、データベースが応答を停止したことを示しています。

引数の説明

Errorテキスト: メッセージをトリガしたエラーの説明が含まれます。

考えられる解決策

データベースサーバが実行中で、応答していることを確認します。

外部リンク

該当なし

エンジン駆動型監査の開始

メッセージ全体

Info:Engine Driven Audit Start (情報:エンジン駆動型監査の開始)

説明

このメッセージは、エンジン駆動型監査が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

エンジン駆動型監査の停止

メッセージ全体

Info:Engine Driven Audit Stop (情報:エンジン駆動型監査の停止)

説明

このメッセージは、エンジン駆動型監査が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

エンジン駆動型エンジンの起動

メッセージ全体

Info:Engine Driven Engine Start, Engine: LFI Agent (情報:エンジン駆動型エンジンの起動、エンジン: LFIエージェント)

説明

このメッセージは、示されているエンジンが実行を開始したことを示しています。

引数の説明

Engine: 起動中のエンジン。

考えられる解決策

該当なし

外部リンク

該当なし

エンジン駆動型エンジンの停止

メッセージ全体

Info:Engine Driven Engine Stop, Engine: LFI Agent Sessions Processed:406 (情報:エンジン駆動型エンジンの停止、エンジン: LFI Agent、処理済みセッション:406)

説明

指定されたエンジンに対するエンジン駆動型監査が完了しました。

引数の説明

Engine: 停止されたエンジン。

Sessions processed: エンジンによって処理されたセッションの数。

考えられる解決策

該当なし

外部リンク

該当なし

外部の相関関係が有効

メッセージ全体

External Correlation Enabled, Origin:*<product_name>* OriginID:*<numeric_value>* OriginDateTime:*<date_time>* File:*<filename>*.json Mode:CompatibleTypesOnly (外部の相関関係が有効、オリジン:<product_name> OriginID:<numeric_value> OriginDateTime:<date_time> ファイル:<filename>.jsonモード:CompatibleTypesOnly)

説明

外部の相関関係がスキャンに対して自動的に有効になっています。

引数の説明

Origin: Fortify_SASTなど、相関関係のある外部製品。

OriginID: 検出事項を含む外部スキャンのID。

OriginDateTime: 外部スキャンがいつ作成されたか。

File: 外部の検出事項を含むJSONファイル。

考えられる解決策

該当なし

外部リンク

該当なし

外部の検出事項

メッセージ全体

External Finding, Origin:*<product_name>* OriginID:*<numeric_value>* OriginDateTime:*<date_time>* OriginFindingID:*<guid>* FindingType:*<type>* (外部の検出事項、オリジン:<product_name> OriginID:<numeric_value> OriginDateTime:<date_time> OriginFindingID:<guid> FindingType:<type>)

説明

外部スキャンでの検出事項に関する情報を提供します。

引数の説明

Origin: Fortify_SASTなど、相関関係のある外部製品。

OriginID: 検出事項を含む外部スキャンのID。

OriginDateTime: 外部スキャンがいつ作成されたか。

OriginFindingID: 外部スキャンファイル内の検出事項の固有のID。

FindingType: 外部スキャンファイル内の検出事項の種類(XSSなど)。

考えられる解決策

該当なし

外部リンク

該当なし

相関関係のある検出事項

メッセージ全体

Finding Correlated, Check:*<check_id><check_name>* Param:*<parameter_name>* Request:*<http_method><resource_url>* (相関関係のある検出事項、チェック:<check_id><check_name> パラメータ:<parameter_name> 要求:<http_method><resource_url>)

説明

この検出事項は、外部スキャンの検出事項と相関関係があります。

引数の説明

Check: SecureBaseからのチェックIDとチェック名。

Param: 攻撃で使用されたパラメータ名。

Request: HTTP要求メソッド(POST、PUT、GETなど)と攻撃されたリソースのURL。

考えられる解決策

該当なし

外部リンク

該当なし

ライセンスの問題

メッセージ全体

Error: License issue: License Deactivated (エラー: ライセンスの問題: ライセンスが無効です)

説明

ライセンスで問題が発生しました。

引数の説明

Issue: 発生した問題。

考えられる解決策

OpenText DASTが適切にライセンスされていることを確認します。

外部リンク

該当なし

ログメッセージの発生

メッセージ全体:

<Level>: <ScanID> , <Logger>: <Exception>

説明:

例外に関する一般的なメッセージ

引数の説明

ScanID: スキャンID。

Logger: ロガーの名前。

Exception: スローされた例外。

考えられる解決策

該当なし

外部リンク

該当なし

メモリ制限に到達

メッセージ全体

警告: メモリ制限に到達しました: レベル:1、制限:1073610752、割り当て済み:1076625408。

エラー: メモリ制限に到達しました: レベル:0、制限:1073610752、割り当て済み:1076625408。

説明

WIプロセスのメモリ制限に到達しました。

引数の説明

Level: 問題の重大度。

Limit: プロセスのメモリ制限。

Actual: プロセスに実際に割り当てられたメモリ。

考えられる解決策

実行されていないその他のスキャンを終了します。

1つのOpenText DASTインスタンスでは、一度に1つのスキャンだけを実行してください。

外部リンク

該当なし

脆弱性のセッションが見つからない

メッセージ全体

Info: Missing Session for Vulnerability (情報: 脆弱性のセッションが見つかりません)

説明

脆弱性に関連付けられているセッションが見つかりません。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

新しいブラインドSQLチェックが有効になっていない

メッセージ全体

New Blind SQL check (checkid newcheckid%) is not enabled. (新しいブラインドSQLチェック(checkid newcheckid%)が有効になっていません。)A policy with both check %newcheckid% and check %oldcheckid% enabled is recommended. (チェック%newcheckid%とチェック%oldcheckid%が有効なポリシーを推奨します。)

説明

ブラインドSQLインジェクションの新しいチェックが、スキャンポリシーに含まれていません。

引数の説明

newcheckid: 新しいSQLインジェクションチェックの識別子(10962)

oldcheckid: 古いSQLインジェクションチェックの識別子(5659)

考えられる解決策

新しいチェック(10962)を、スキャンポリシーに追加します。

外部リンク

該当なし

永続的クロスサイトスクリプティング監査の開始

メッセージ全体

Info:Persistent Cross-Site Scripting Audit Start (情報:永続的クロスサイトスクリプティング監査の開始)

説明

永続的クロスサイトスクリプティング監査が開始しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

永続的クロスサイトスクリプティング監査の停止

メッセージ全体

Info:Persistent Cross-Site Scripting Audit Stop (情報:永続的クロスサイトスクリプティング監査の停止)

説明

永続的クロスサイトスクリプティング監査が停止しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

スキャン後分析の開始

メッセージ全体

Post-Scan Analysis started. (スキャン後分析が開始しました。)

説明

スキャン後分析が開始しました。使用されているモジュールごとに追加のメッセージが表示されます(認証、マクロ、ファイルが見つからない、など)。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

スキャン後分析の完了

メッセージ全体

Post-Scan Analysis completed. (スキャン後分析が完了しました。)

説明

スキャン後分析が終了しました。使用されているモジュールごとに追加のメッセージが表示されます(認証、マクロ、ファイルが見つからない、など)。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

監査反映の開始

メッセージ全体

Info:Reflect Audit Start (情報:監査反映の開始)

説明

反映フェーズが開始しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

監査反映の停止

メッセージ全体

Info:Reflect Audit Stop (情報:監査反映の停止)

説明

反映フェーズが完了しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

応答状態ルールの失敗

メッセージ全体

Response State Rules Fail detected for %count% rule(s). (%count%ルールに対して、応答状態ルールの失敗が検出されました。)Name of rule(s): %ruleslist%. (ルールの名前: %ruleslist%.)

説明

応答状態ルールは設定されていますが、スキャン中にトリガされませんでした。

引数の説明

count: 失敗したルールの数

ruleslist: 失敗したルールの名前

考えられる解決策

ルール内の正規表現を修正するか、ルールを削除します。詳細については、「"スキャン設定: HTTP解析" ページ422」を参照してください。

外部リンク

該当なし

スキャン完了

メッセージ全体

Info:Scan Complete, ScanID:<id-number> (情報:スキャン完了、ScanID:<id-number>)

説明

このメッセージは、スキャンが正常に完了したことを示しています。

引数の説明

ScanID: スキャンの固有のID

考えられる解決策

該当なし

外部リンク

該当なし

スキャン失敗

メッセージ全体

Info:Scan Failed, ScanID::<id-number> (情報:スキャンが失敗しました、ScanID::<id-number>)

説明

このメッセージは、スキャンが失敗したことを示しています。

引数の説明

ScanID: スキャンの固有のID

考えられる解決策

スキャンが失敗した理由によって異なります(別のメッセージによって示されます)。

外部リンク

該当なし

スキャン開始

メッセージ全体

Info:Scan Start, ScanID:<id-number> Version:X.X.X.X, Location:C:\Program Files\Fortify\Fortify WebInspect\WebInspect.exe (情報:スキャン開始、ScanID:<id-number> バージョン:X.X.X.X、場所:C:\Program Files\Fortify\Fortify WebInspect\WebInspect.exe)

説明

このメッセージは、スキャンの開始を示しています。

引数の説明

ScanID: スキャンの固有のID。

Version: スキャンを実行しているOpenText DASTのバージョン。

Location: OpenText DAST実行可能ファイルの物理的な場所です。

考えられる解決策

該当なし

外部リンク

該当なし

スキャン開始エラー

メッセージ全体

Scan start error: %error% (スキャン開始エラー: %error%)

説明

スキャンの開始中に回復不可能なエラーが発生しました。カスタマサポートへのお問い合わせ

引数の説明

error: 問題の説明。

考えられる解決策

該当なし

外部リンク

該当なし

スキャン停止

メッセージ全体

Info:Scan Stop, ScanID:<id-number> (情報:スキャン停止、ScanID:<id-number>)

説明

このメッセージは、スキャンが停止されたことを示しています。

引数の説明

ScanID: スキャンの固有のID。

考えられる解決策

該当なし

外部リンク

該当なし

スキャナ再試行の開始

メッセージ全体

Info:Scanner Retry Start (情報: スキャナ再試行の開始)

説明

再試行フェーズが開始しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

スキャナ再試行の停止

メッセージ全体

Info:Scanner Retry Stop (情報: スキャナ再試行の停止)

説明

再試行フェーズが停止しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

順次監査の開始

メッセージ全体

Info:Sequential Audit Start (情報:順次監査の開始)

説明

このメッセージは、順次監査が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

順次監査の停止

メッセージ全体

Info:Sequential Audit Stop (情報:順次監査の停止)

説明

このメッセージは、順次監査が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

順次Web探索の開始

メッセージ全体

Info:Sequential Crawl Start (情報:順次Web探索の開始)

説明

このメッセージは、順次Web探索が開始したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

順次Web探索の停止

メッセージ全体

Info:Sequential Crawl Stop (情報:順次Web探索の停止)

説明

このメッセージは、順次Web探索が停止したことを示しています。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

設定の上書き

メッセージ全体

Settings Override, Setting:<setting, Original Value:<original>, New Value:<newValue>, Reason:<reason> (設定の上書き、設定:<setting>、元の値:<original>、新しい値:<newValue>、理由:<reason>)

説明

設定が製品によって変更されました。これは、設定のアップグレードの問題を示している可能性があります。

引数の説明

Setting: 上書きされる設定。

Original Value: 設定の元の値。

New Value: 設定の変更後の値。

Reason: 上書きの理由。

考えられる解決策

工場出荷時のデフォルト値を復元して、カスタム設定値を再適用します。

外部リンク

該当なし

SPAフレームワークの検出

メッセージ全体

The crawl identified the following Single Page Application frameworks: %frameworks%. (Web探索で、次のシングルページアプリケーションフレームワークが特定されました。%frameworks%.)SPA support enabled. (SPAサポートが有効になっています。)

説明

Web探索プログラムにより1つ以上のSPA (シングルページアプリケーション)フレームワークが検出され、スキャンに対してSPAサポートが有効化されました。

引数の説明

frameworks: 検出されたフレームワークのリスト。

考えられる解決策

該当なし

外部リンク

該当なし

起動URLのエラー

メッセージ全体

Start Url Error:%url%, error:%error% (起動Urlのエラー:%url%、エラー:%error%)

説明

起動URLの処理中に回復不可能なエラーが発生しました。URL構文を確認し、間違いなかった場合は、カスタマサポートにお問い合わせください。

引数の説明

url: エラーの原因となったURL。

error: エラーの説明。

考えられる解決策

該当なし

外部リンク

該当なし

開始URLの拒否

メッセージ全体

Start Url Rejected:%url%, reason:%reasons%, session:%session% (開始Urlが拒否されました:%url%、理由:%reasons%、セッション:%session%)

説明

要求拒否設定によりURLが拒否されました。設定を変更するか、別の開始URLを使用する必要があります。

引数の説明

Url: 開始URL

reason: 拒否の理由。

session: エラーが発生したセッション。

考えられる解決策

該当なし

外部リンク

該当なし

スキャン後分析モジュールの開始

メッセージ全体

Starting Post-Scan Analysis Module: %module% (スキャン後分析モジュールを開始しています: %module%)

説明

スキャン後分析モジュールの1つが開始しました。

引数の説明

module: スキャン後分析モジュールの名前。

考えられる解決策

該当なし

外部リンク

該当なし

停止の要求

メッセージ全体

Info:Stop Requested, reason=Pause button pushed (情報:停止が要求されました、理由=一時停止ボタンが押されました)

説明

スキャンが一時停止状態になります。

引数の説明

Reason: 停止の理由。

考えられる解決策

該当なし

外部リンク

該当なし

監査検証の開始

メッセージ全体

Info:Verify Audit Start (情報:監査検証の開始)

説明

検証フェーズが開始しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

監査検証の停止

メッセージ全体

Info:Verify Audit Stop (情報:監査検証の停止)

説明

検証フェーズが完了しました。

引数の説明

該当なし

考えられる解決策

該当なし

外部リンク

該当なし

Webマクロエラー

メッセージ全体

Error: Web Macro Error, Name: Login webmacro Error: RequestAborted (エラー: Webマクロエラー、名前:Login webmacro エラー: RequestAborted)

説明

Webマクロの再生中にエラーが発生しました。

引数の説明

Name: エラーが発生した際に再生されていたマクロの名前。

Error: 発生したエラー。

考えられる解決策

検出されたエラーによって異なります。RequestAbortedエラーの場合、マクロ再生中はサーバは応答しません。この問題が頻繁に発生する場合は、 要求タイムアウト(Request timeout)] の値を大きくする必要があります。その他の解決策については、コネクティビティに関する問題を参照してください。

外部リンク

該当なし

Webマクロステータス

メッセージ全体

Error: Web Macro Status, Name: login.webmacro Expected:302, Actual:200, Url:<URL> (エラー: Webマクロステータス、名前: login.webmacro 想定:302、実際:200、Url:<URL>)

説明

OpenText DASTは、マクロの再生中に、マクロを記録した際に取得した応答と一致しない応答を受信しました。

引数の説明

Name: Webマクロの名前。

Expected: 返されることが想定されたステータスコード。

Actual: 実際に返されたステータスコード。

URL: 要求のターゲットURL。

考えられる解決策

これは、OpenText DASTがすでにログインしている状態でログインを試行したか、OpenText DASTがログインに失敗したことを示している可能性があります。スキャン中にOpenText DASTがログインに成功したかどうかを確認してください。そうでない場合は、ログインマクロを再度記録します。

外部リンク

該当なし

HTTPステータスコード

次のステータスコードのリストは、Hypertext Transfer Protocolバージョン1.1規格(RFC 2616)からの引用です。詳細については、http://www.w3.org/Protocols/を参照してください。

コード	定義
100	続行
101	プロトコルの切り替え
200 OK	要求が成功しました

コード	定義
201 Created	要求が完了し、新しいリソースが作成されました
202 Accepted	要求が処理のために受理されましたが、処理は完了していません。
203 Non-Authoritative Information	エンティティヘッダに返されるメタ情報は、元のサーバから取得可能な確定的なセットではなく、ローカルまたはサードパーティのコピーから収集されたものです。
204 No Content	サーバは要求を完了しましたが、エンティティ本体を返す必要はなく、更新されたメタ情報を返すことができます。
205 Reset Content	サーバが要求を完了しました。ユーザエージェントは、要求の送信の原因となったドキュメントビューをリセットする必要があります。
206 Partial Content	サーバがリソースに対する部分的なGET要求を完了しました。
300 Multiple Choices	要求されたリソースは一連の表現のいずれか1つに対応し、それらはそれぞれ独自の場所を持ちます。エージェント駆動型のネゴシエーション情報(セクション12)が提供されるので、ユーザ(またはユーザエージェント)は希望の表現を選択し、その要求を該当する場所にリダイレクトできます。
301 Moved Permanently	要求されたリソースに新しい永続URIが割り当てられました。今後、このリソースを参照するときには、返されたURIのいずれかを使用する必要があります。
302 Found	要求されたリソースは、一時的に別のURIに存在します。
303 See Other	要求に対する応答は別のURIにあり、そのリソースに対するGETメソッドを使用して取得する必要があります。
304 Not Modified	クライアントが条件付きGET要求を実行して、アクセスは許可されたものの文書が未変更だった場合、サーバはこのステータスコードで応答します。
305 Use Proxy	要求されたリソースへのアクセスは、Locationフィールドで指定されたプロキシを介して行う必要があります。
306 Unused	未使用。
307 Temporary Redirect	要求されたリソースは、一時的に別のURIに存在します。

コード	定義
400 Bad Request	構文の形式が正しくないため、サーバはこの要求を理解できませんでした。
401 Unauthorized	この要求にはユーザ認証が必要です。応答には、要求されたリソースに適用可能なチャレンジを含むWWW-Authenticateヘッダフィールド(セクション14.47)が含まれている必要があります。
402 Payment Required	このコードは将来の使用のために予約されています。
403 Forbidden	サーバは要求を理解しましたが、要求の実行を拒否しています。
404 Not Found	サーバはRequest-URIに一致する内容を検出できませんでした。
405 Method Not Allowed	Request-URIで示されたリソースでは、Request-Lineに指定されたメソッドが許可されていません。
406 Not Acceptable	要求で指定されたリソースで生成可能なのは、要求で送信されたAcceptヘッダによれば受け入れ不能なコンテンツ特性を持つ応答エンティティだけです。
407 Proxy Authentication Required	このコードは401 (Unauthorized)と似ていますが、クライアントが最初にプロキシに対して自身を認証する必要があることを示しています。
408 Request Timeout	サーバの待機時間内に、クライアントが要求を生成しませんでした。
409 Conflict	リソースの現在の状態との競合のため、要求を完了できませんでした。
410 Gone	要求されたリソースはすでにサーバ上になく、転送アドレスも不明です。
411 Length Required	サーバは、定義されたContent-Lengthがない要求の受け入れを拒否します。
412 Precondition Failed	1つ以上のrequest-headerフィールドに指定された事前条件が、サーバ上でテストされた際にfalseと評価されました。
413 Request Entity Too Large	要求エンティティの大きさがサーバの処理能力を超えているため、サーバは要求の処理を拒否しています。
414 Request-URI Too Long	Request-URIが長すぎてサーバが解釈できないため、サーバは要求の処理を拒否しています。

コード	定義
415 Unsupported Media Type	要求のエンティティの形式が、要求されたメソッドの要求されたリソースでサポートされていないため、サーバは要求の処理を拒否しています。
416 Requested Range Not Satisfiable	要求にRange request-headerフィールド(セクション14.35)が含まれているものの、このフィールド内のrange-specifier値がどれも選択されたリソースの現在の範囲と重ならず、かつ要求にIf-Range request-headerフィールドが含まれていない場合、サーバはこのステータスコードを含む応答を返します。
417 Expectation Failed	このサーバは、Expect request-headerフィールド(セクション14.20を参照)に指定された条件を満たすことができません。または、サーバがプロキシである場合、このサーバはネクストホップサーバでは要求が満たせないという明白な証拠を持っています。
500 Internal Server Error	サーバが予期しない条件を検出したため、要求を完了できませんでした。
501 Not Implemented	サーバは、要求を実行するために必要な機能をサポートしていません。これは、サーバが要求メソッドを認識せず、どのリソースについてもこれをサポートできない場合の妥当な応答です。
502 Bad Gateway	サーバがゲートウェイまたはプロキシとして機能しているときに、要求を完了しようとしてアクセスした上流サーバから無効な応答を受け取りました。
503 Service Unavailable	サーバの一時的な過負荷または保守のため、サーバは現在要求を処理できません。
504 Gateway Timeout	サーバがゲートウェイまたはプロキシとして機能しているとき、要求を完了するためにはURIで指定された上流サーバ(HTTP、FTP、LDAPなど)かその他の補助サーバ(DNSなど)にアクセスする必要がありましたが、所定の時間内にそこから応答を受け取りませんでした。
505 HTTP Version Not Supported	サーバは、要求メッセージで使用されたHTTPプロトコルバージョンをサポートしていないか、サポートを拒否しています。

第11章:トラブルシューティング

この章には、トラブルシューティングの表、ログインマクロのテストに関する情報、およびOpenText DASTのアンインストールオプションの説明が記載されています。

OpenText DASTのトラブルシューティング

以降の段落では、OpenText DASTおよびOpenText DASTツールのトラブルシューティング情報について説明します。

コネクティビティに関する問題

次の表に、コネクティビティに関する問題の説明を示します。

症状またはエラーメッセージ	考えられる原因	考えられる解決方法
HTTPではなくHTTPSを使用するサイトのテスト中に、マクロレコーダまたはガイド付きスキャンウィザードを使用するとき、サイトへのコネクティビティがありません。	OpenText DASTを実行しているユーザに、Windows MachineKeysフォルダに対する必要なアクセス許可がありません。	許可の変更を、C:\ProgramData\Microsoft\Crypto\RSA\MachineKeysに関して行います。 フォルダのプロパティの[**セキュリティ**]タブで、[**詳細設定**]ボタンを使用して、[**このフォルダー、サブフォルダーおよびファイル**]に関してユーザにフルコントロールを許可するようにアクセス許可を設定します。
[**OpenSSLエンジンを使用する(Use OpenSSL Engine)**]アプリケーション設定が選択されており、ガイド付きスキャンブラウザ、Profilerの結果、またはスキャンログに次のテキストを含むエラーが表示されます。	OpenSSLの不具合が原因で、ターゲットWebアプリケーションでコネクティビティの問題が発生しました。	ターゲットWebアプリケーションへの接続に使用する証明書が、エクスポート可能としてマークされていることを確認します。詳細については、Windowsのマニュアルを参照してください。

症状またはエラーメッセージ	考えられる原因	考えられる解決方法
「このクライアント証明書キーを証明書ストレージへエクスポートできるようにしてください。(Make this client Certificate key exportable in Certificate storage.)」		

スキャン初期化の失敗

次の表に、スキャン初期化に関する問題の説明を示します。

症状またはエラーメッセージ	考えられる原因	考えられる解決方法
SQL Expressをスキャンデータベースとして使用しているときに、スキャンの初期化が失敗します。	SQL Expressサービスが実行されていません。	サービスが実行されていることを確認します。このサービスの名前は「SQL Server (SQLEXPRESS)」などです。
	SQL Expressキャッシュが破損している可能性があります。	キャッシュをクリアするには: 1. すべてのSQL関連のサービスとプロセスを停止します。 2. SQL Expressキャッシュフォルダを削除します。 通常は次のような場所にあります。 C:\Users\ *<username>* \AppData\Local\Microsoft\Microsoft SQL Server Data\SQLEXPRESS 3. マシンを再起動します。
SPI.Parsers.Scriptのロードに関連するエラーが原因でスキャン初期化が失敗しま	Windowsで、Visual Studio 2015、2017、または2019用の	続行する前に、C++再頒布可能パッケージを手動でインストールします。

症状またはエラーメッセージ	考えられる原因	考えられる解決方法
す。	Microsoft Visual C++再頒布可能パッケージを適用できなかった可能性があります。	

スキャン設定の問題

次の表に、スキャンの設定中に発生する可能性がある問題の説明を示します。

症状またはエラーメッセージ	考えられる原因	考えられる解決方法
ガイド付きスキャンで、欠落している.dllファイルに関連するtruclientbrowser.exeシステムエラーが発生します。	Windowsで、Visual Studio 2015、2017、または2019用のMicrosoft Visual C++再頒布可能パッケージを適用できなかった可能性があります。	続行する前に、C++再頒布可能パッケージを手動でインストールします。

アラートのトラブルシューティング

アラートは、必ずしもスキャン品質の問題が発生していることを示しているわけではありません。一部のアラートは誤検出の可能性があります。ただし、アラートから、スキャンに悪影響を及ぼす可能性がある問題を把握できる可能性があります。

アラートの無効化

アラート機能には、サンプル間隔およびアクティブ間隔が含まれます。サンプル間隔アラートは、最大で1分に1回の頻度でスキャンログに記録されます。サンプル間隔アラートはスキャンの機能的な問題を示していない可能性がありますが、受信するアラートの数が問題になる場合は、カスタマサポートに連絡して、個々のアラートまたはアラート機能の無効化の支援を依頼してください。詳細については、「"序文" ページ25」を参照してください。

アラートのトラブルシューティングの表

重要! {/b}スキャン設定を変更する解決策はすべて、将来のスキャンを対象として実行される必要があります。現在のスキャンのスキャン設定を変更することはできません。

次の表に、アラートの考えられる原因と解決方法の説明を示します。

アラート	考えられる原因	考えられる解決方法
過剰なログインが検出されます	ログインマクロの再生回数が、実行された要求の数に対して多すぎます。ログイン資格情報が正しくないか、またはログアウト署名が無効である可能性があります。	次のいずれかを実行します。 • マクロのトラブルシューティング手順を実行します。 • 新しいログインマクロを記録します。 詳細については、『*OpenText™ Dynamic Application Security Testing ツールガイド*』を参照してください。
冗長なコンテンツが検出されました	冗長なコンテンツが検出されました。	冗長ページ検出を有効にすることで、パフォーマンスを向上できる可能性があります。詳細については、「"スキャン設定: 全般" ページ406」を参照してください。
応答時間が長すぎます	Webサーバからの応答に、平均よりも長い時間か、予想よりも長い時間がかかっています。応答時間が長くなると、スキャンにかかる時間が長くなる可能性があります。	ネットワークのコネクティビティ、またはAUT (テスト中のアプリケーション)のパフォーマンスを確認します。
WAFが検出されました	WAF (Webアプリケーションファイアウォール)署名が検出されました。	AUTを保護しているWAFを無効にします。

ログインマクロのテスト

OpenText DASTは、次の場合にログインマクロに対してテストを実行します。

- 自動生成されたマクロ、新しく記録されたマクロ、または既存のマクロがスキャン設定中にテストされる場合
- ログインマクロのスキャン開始時([スキャン設定: 認証(Scan Settings: Authentication)]で **[マクロ検証を有効にする(Enable macro validation)]**が選択されている場合)

注記: マクロテストは、2要素認証を含むマクロに対してはサポートされていません。

実行される検証テスト

次の表で、OpenText DASTが実行するテストについて説明しています。

テスト	失敗した場合の結果
検証ステップが欠落しているかどうかを判断する。	スキャンは続行しますが、警告がスキャンログに書き込まれます。
不正な資格情報が使用された場合の動作を監視する。	
ログイン状態でランディングページにアクセスできるかどうかを判断する。	
ログイン状態なしでランディングページにアクセスできるかどうかを判断する。	
サイトで複数のログインを同時に処理できるかどうかを判断する。テスト対象の同時ログインのデフォルトの数は5です。	
自動生成されたマクロがアプリケーションにログインすることを検証する。	スキャンは停止し、エラーがスキャンログに書き込まれます。
マクロの再生でアプリケーションにログインすることを検証する。	

テストに失敗した後にスキャンが停止した場合、スキャンログで特定のエラーメッセージを調べて、問題を特定して解決できることがあります。エラーメッセージとこのトピックのトラブルシューティングのヒントを使用すると、問題の解決に役立ちます。

トラブルシューティングのヒント

マクロが失敗した場合はいつも、無効なマクロが記録されている可能性があります。ただし、以前は良好だったマクロが失敗した場合は、たいていサイトの変更または資格情報が原因です。

次の表に、各エラーメッセージの考えられる原因と解決方法を示します。

注記: この表には、各エラーメッセージのすべての考えられる原因と解決方法が含まれているわけではありません。追加のトラブルシューティングが必要となることがあります。

エラーメッセージ	考えられる原因	考えられる解決方法
自動ログインの生成に失敗しました(Automatic login generation failed)	指定されたユーザ資格情報が無効であるために、ログインマクロを作成できませんでした。	有効であると判明している資格情報を使用して、 [ログインマクロの自動生成(Auto-gen Login Macro)]オプションを再試行してください。
実行に失敗しました(Execution Failed)	検証要素、ユーザ名、パスワードなどのHTML要素が見つかりませんでした。	ログイン入力要素を識別するため、Web Macro Recorderで新しいマクロを記録します。
	ユーザ名が無効になっている(データベースから削除された)か、パスワードが変更されています。	有効であると判明している資格情報を使用して、Web Macro Recorderで新しいマクロを記録します。
ログイン検証ステップが見つかりません(Logged in verification step not found)	ログインマクロに検証ステップが含まれていません。	Web Macro Recorderでマクロを編集して、ログインが成功したかどうかを示す検証ステップを追加します。
無効なログイン後に検証ステップが失敗しませんでした(Verification step did not fail after invalid login)	無効なログイン試行の後に検証ステップが成功しました。有効な検証ステップは、ログインが成功した場合にのみ成功します。これは、誤ったログイン検証オブジェクトが選択されたことを示しています。	Web Macro Recorderでマクロを編集して、検証ステップに別のオブジェクトを選択します。

Webマクロレコーダのダウンロードの詳細については、『*OpenText™ Dynamic Application Security Testingツールガイド*』を参照してください。

OpenText DASTのアンインストール

アンインストール時に、OpenText DASTの修復またはコンピュータからの削除を選択できます。

削除のオプション

削除(Remove)]を選択する場合は、次のオプションの1つまたは両方を選択できます。

- 製品を完全に削除(Remove product completely) - OpenText DASTアプリケーションとすべての関連ファイル(ローカル(非共有)SQLサーバに保存されているスキャンデータ、設定ファイル、およびログなど)を削除します。
- ライセンスの無効化(Deactivate license) - OpenText DASTライセンスを解放します。これにより、別のコンピュータにOpenText DASTをインストールできるようになります。アプリケーションデータとファイルは削除されません。

ドキュメントのフィードバックを送信する

このドキュメントに関するご意見は、電子メールでドキュメントチームまでお寄せください。

注記: 弊社製品に関する技術的な問題が発生した場合は、ドキュメントチームに電子メールを送信しないでください。代わりに、https://www.microfocus.com/supportに問い合わせてサポートを受けてください。

このコンピュータに電子メールクライアントが設定されている場合は、前のドキュメントチームに連絡するためのリンクをクリックすると、表題の行に以下の情報が付いた状態で電子メールウィンドウが開きます。

ユーザガイド(Dynamic Application Security Testing 25.2.0)に関するフィードバック

電子メールにフィードバックを追加して、 [送信]をクリックします。

電子メールクライアントが使用できない場合は、前の情報をWebメールクライアントの新しいメッセージにコピーして、fortifydocteam@opentext.comにフィードバックを送信してください。

皆様のご意見をお待ちしております。