
Micro Focus Fortify Security Assistant Extension for Visual Studio

Software Version: 21.1.0

User Guide

Document Release Date: June 2021

Software Release Date: June 2021



Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

<https://www.microfocus.com>

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2018 - 2021 Micro Focus or one of its affiliates

Trademark Notices

All trademarks, service marks, product names, and logos included in this document are the property of their respective owners.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

This document was produced on November 17, 2021. To check for recent updates or to verify that you are using the most recent edition of a document, go to:

<https://www.microfocus.com/support/documentation>

Contents

Preface	4
Contacting Micro Focus Fortify Customer Support	4
For More Information	4
About the Documentation Set	4
Change Log	5
Chapter 1: Introduction	6
Fortify Security Assistant Extension for Visual Studio	6
Fortify Security Content	6
Fortify Security Assistant Requirements	6
Chapter 2: Installation and Configuration	8
Installing Fortify Security Assistant	8
Using Fortify Security Content from a Local Package	9
Configuring Fortify Security Assistant	10
Uninstalling Fortify Security Assistant	11
Chapter 3: Using Fortify Security Assistant	12
Finding Security Issues as you Write Code	12
Working with Security Issues in the Error List Window	13
Suppressing Categories of Issues	15
Unsuppressing Categories of Issues	15
Scanning Solutions for Issues	16
Working with Security Issues in the Security Assistant Window	16
Using the Fortify Issue Suppression File	18
Send Documentation Feedback	20

Preface

Contacting Micro Focus Fortify Customer Support

Visit the Support website to:

- Manage licenses and entitlements
- Create and manage technical assistance requests
- Browse documentation and knowledge articles
- Download software
- Explore the Community

<https://www.microfocus.com/support>

For More Information

For more information about Fortify software products:

<https://www.microfocus.com/solutions/application-security>

About the Documentation Set

The Fortify Software documentation set contains installation, user, and deployment guides for all Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following Micro Focus Product Documentation website:

<https://www.microfocus.com/support/documentation>

Change Log

The following table lists changes made to this document. Revisions to this document are published between software releases only if the changes made affect product functionality.

Software Release / Document Version	Changes
21.1.0	Updated: <ul style="list-style-type: none">• "Suppressing Categories of Issues" on page 15 - Changes made for how to suppress different types of issues Added: <ul style="list-style-type: none">• "Working with Security Issues in the Security Assistant Window" on page 16 - Described the new window that shows detected issues from an analyzed solution
20.1.0	Updated: <ul style="list-style-type: none">• "Fortify Security Assistant Requirements" on page 6 - Changed the required .NET Framework version
19.2.0	Updated: <ul style="list-style-type: none">• "Fortify Security Assistant Requirements" on page 6 - Support added for Visual Studio 2019
18.10	Initial release

Chapter 1: Introduction

This section contains the following topics:

Fortify Security Assistant Extension for Visual Studio	6
Fortify Security Content	6
Fortify Security Assistant Requirements	6

Fortify Security Assistant Extension for Visual Studio

Fortify Security Assistant Extension for Visual Studio (Fortify Security Assistant) works with a portion of the Fortify Security Content to provide alerts to potential security issues as you write your code. Fortify Security Assistant provides detailed information about security risks and recommendations for how to secure the potential issue. Fortify Security Assistant can detect issues in C# (.cs), Razor (.cshtml), WebForms (.aspx), .config, .xml, and .ini files.

Fortify Security Assistant includes both structural and configuration analyzers to detect:

- Potentially dangerous uses of functions and APIs
- Insecure application configuration

Fortify Security Content

Fortify Security Assistant uses a knowledge base of rules to enforce secure coding standards applicable to the codebase for static analysis. Micro Focus Fortify Software Security Content consists of Fortify Secure Coding Rulepacks, which describe general secure coding idioms for popular languages and public APIs.

Fortify Security Assistant Requirements

Fortify Security Assistant requires:

- A valid Fortify license file to scan for issues
For information about how to obtain a Fortify license, contact Micro Focus Fortify Customer Support (<https://www.microfocus.com/support>).
- Up-to-date Micro Focus Fortify Software Security Content
You can download the Fortify Security Content directly from Fortify Security Assistant or you can use a local copy if you do not have a network connection to the Fortify Customer Portal. For instructions, see "[Using Fortify Security Content from a Local Package](#)" on page 9.

Fortify Security Assistant requires the software packages listed in the following table.

Software	Versions
Visual Studio	2019 Community, Professional, and Enterprise 2017 Community, Professional, and Enterprise 15.6 or later
.NET Framework	4.7.2 or later

Chapter 2: Installation and Configuration

This section contains the following topics:

- [Installing Fortify Security Assistant](#) 8
- [Using Fortify Security Content from a Local Package](#) 9
- [Configuring Fortify Security Assistant](#)10
- [Uninstalling Fortify Security Assistant](#)11

Installing Fortify Security Assistant

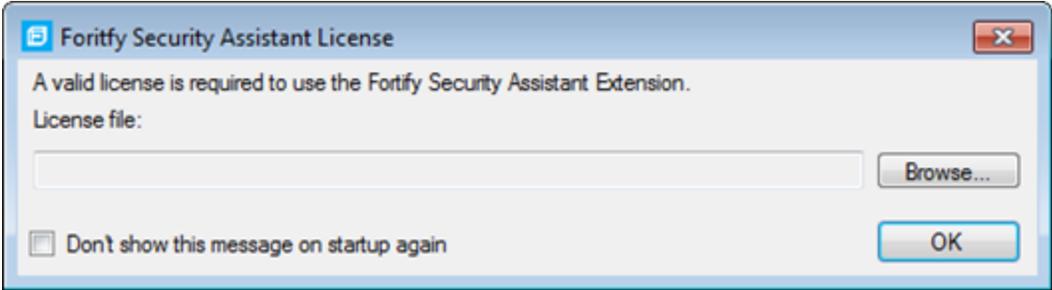
Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To install the Fortify Security Assistant extension:

1. In Visual Studio, select **Extensions > Manage Extensions**.
2. Search the Visual Studio Marketplace for *Fortify Security Assistant*.
3. Download and install the Fortify Security Assistant Extension for Visual Studio.

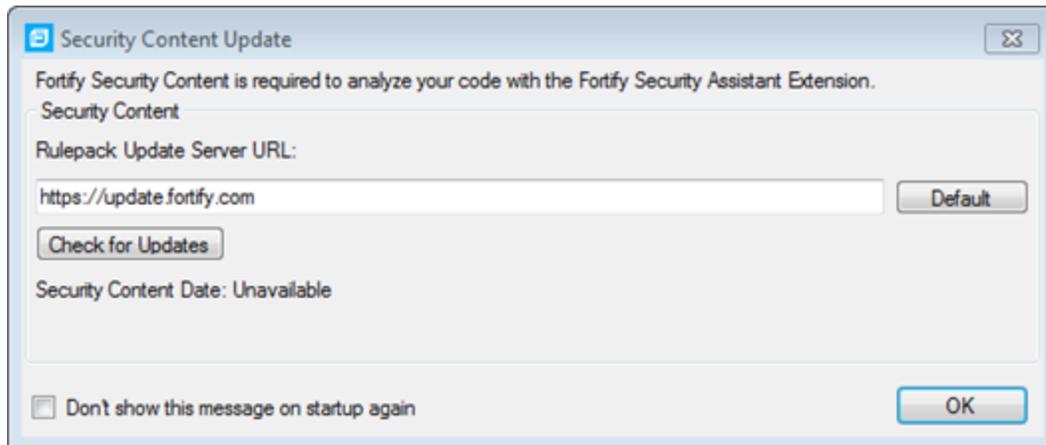
Note: To install this extension as an administrator and allow all users to use the extension, download the VSIX file from the Visual Studio Marketplace and then install it using VSIXInstaller with the /admin option from the Command Prompt.

The first time you install the extension, you are prompted to provide a license file and Micro Focus Fortify Software Security Content. Alternatively, you can specify this information later (see "[Configuring Fortify Security Assistant](#)" on page 10).



The license for Fortify Security Assistant expires annually. You do not need to specify the Fortify license file again until the license expires.

After you specify the Fortify license, you are prompted to update Fortify Security Content.



To specify the Fortify Security Content, you can either:

- Click **Check for Updates** to download the Fortify Security Content directly from the specified **Rulepack update server URL**.

Note: If you get an error that indicates the downloaded security content is unverified, you might have an invalid license file. Contact Micro Focus Fortify Customer Support for assistance.

- Click **OK** if you do not have a network connection to the Fortify Customer Portal and you want to use a local copy of Fortify Security Content. For instructions, see "[Using Fortify Security Content from a Local Package](#)" below).

Using Fortify Security Content from a Local Package

If you do not have a network connection to the Fortify Customer Portal, Fortify Security Assistant can use the Micro Focus Fortify Software Security Content from a local copy. The file must have the name `rulePacks.zip`.

You can download the Fortify Security Content from the Fortify Customer Portal using your credentials provided by Micro Focus Fortify Customer Support. The Fortify Security Content for Fortify Security Assistant is a separate download with the product name SA_DOTNET.

To configure Fortify Security Assistant to use Fortify Security Content from a local package:

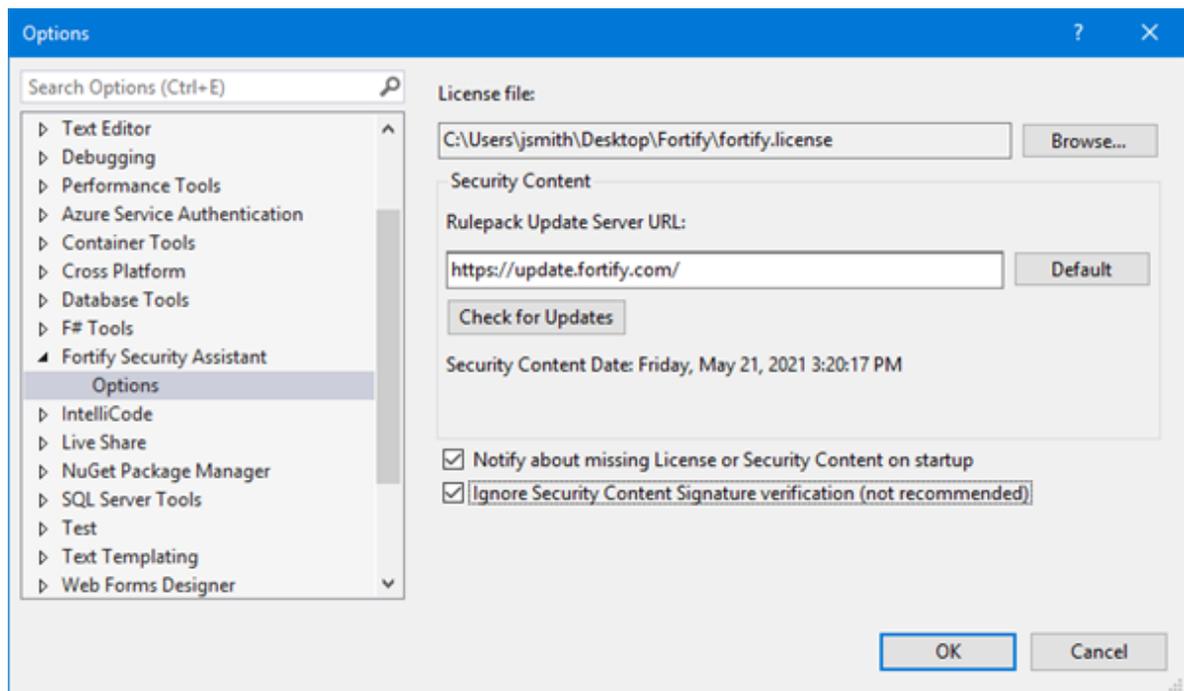
1. Navigate to `C:\Users\<username>\AppData\Local\Fortify\SecurityAssistantVS-<version>`.
2. Place the Fortify Security Content file `rulePacks.zip` in this folder.
3. Restart Visual Studio.

Configuring Fortify Security Assistant

To scan projects or solutions, you must have a valid Fortify license file and up-to-date Micro Focus Fortify Software Security Content. To download security content from the Fortify Customer Portal, you must be connected to the Internet and have your network connections configured to access the Fortify Customer Portal (<https://update.fortify.com>). To update Fortify Software Security Content from a local file, see "Using Fortify Security Content from a Local Package" on the previous page.

To configure Fortify Security Assistant:

1. From the Fortify Security Assistant extension menu, select **Options**.



2. To specify the license file, click **Browse** next to the **License file** box and navigate to the license file on your system.
3. To update security content:

- a. In the **Rulepack Update Server URL** box, type a Rulepack update server URL.

If you want to obtain the Fortify Security Content from a URL other than the Fortify Customer Portal, you must have a public key so that Fortify Security Assistant can verify the security content. Place the public key in the

C:\Users*<username>*\AppData\Local\Fortify\SecurityAssistantVS-*<version>*\keys directory. You can bypass the Fortify Security Content verification by selecting **Ignore Security Content Signature verification**.

Note: Click **Default** to set the URL to the Fortify Customer Portal.

- b. Click **Check for Updates**.

Note: If you get an error that indicates the downloaded security content is unverified, you might have an invalid license file. Contact Micro Focus Fortify Customer Support for assistance.

4. Click **OK**.

Fortify Security Assistant re-inspects the solution to refresh any issues reported so that it matches your configuration settings.

Uninstalling Fortify Security Assistant

Note: These instructions describe a third-party product and might not match the specific, supported version you are using. See your product documentation for the instructions for your version.

To uninstall the Fortify Security Assistant Visual Studio extension:

1. In Visual Studio, select **Extensions > Manage Extensions**.
2. In the left pane, select **Installed**.
3. Select **Fortify Security Assistant for Visual Studio**, and then click **Uninstall**.
4. Click **Yes** to confirm the pending uninstallation.

Chapter 3: Using Fortify Security Assistant

Fortify Security Assistant notifies you of any detected issues as you write your code. You can also have Fortify Security Assistant examine an entire solution and then you can review possible security issues (see ["Scanning Solutions for Issues" on page 16](#)).

This section contains the following topics:

- [Finding Security Issues as you Write Code](#) 12
- [Working with Security Issues in the Error List Window](#) 13
- [Scanning Solutions for Issues](#) 16
- [Working with Security Issues in the Security Assistant Window](#) 16
- [Using the Fortify Issue Suppression File](#) 18

Finding Security Issues as you Write Code

As you write your code, Fortify Security Assistant provides notifications of potential security issues. Fortify Security Assistant displays these issues in the code as a tooltip and in the Error List window for open files. You can also perform an analysis on the current solution (see ["Scanning Solutions for Issues" on page 16](#)).

To review the security issues:

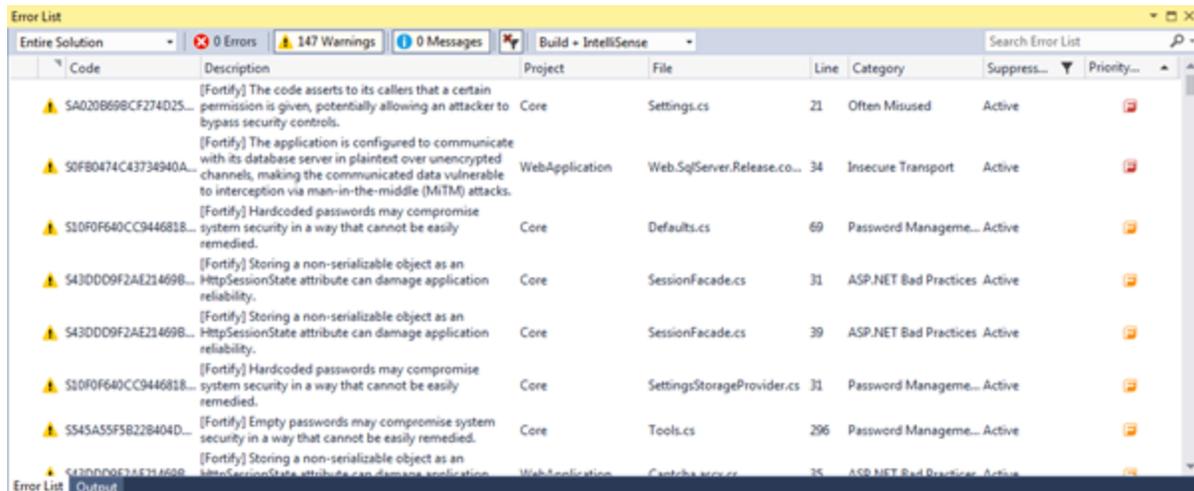
- Pause your cursor over the highlighted code to open a tooltip that briefly describes the issue as shown in the following example:

```
<!-- set up users -->
<authentication mode="Forms">
  <forms name="customer_login" timeout="10" loginUrl="~/WebGoatCoins/CustomLogin.aspx" requireSSL="false"
  P S4D329B36258E4B24B1B3A35F42BCB858: [Fortify] The application session cookie is created without the Secure flag set to true.
  <user name="admin" password="admin" />
  <user name="mario" password="luigi" />
  <user name="bob" password="password" />
  </credentials>
</forms>
</authentication>
```

- Open the Error List window (the **Warnings** tab) to see possible security issues in open files. For more information about reviewing Fortify Security Assistant detected issues in the Error List window, see ["Working with Security Issues in the Error List Window" on the next page](#).

Working with Security Issues in the Error List Window

Fortify Security Assistant displays all the security issues detected as you write code and for open files in the **Error List** window's **Warnings** tab.



The following table describes the Fortify information provided for each issue.

Column	Description
Description	A brief description of the issue. Fortify Security Assistant prepends each detected issue with [Fortify].
Category	The Fortify category.
Suppression State	Indicates whether the issue has been suppressed (hidden). To change whether suppressed issues are visible or not, click the filter icon in the Suppression State column, and then select or clear the Suppressed check box.

Column	Description
Priority Order	<p>A colored icon indicates the Fortify Priority Order used to categorize the severity of a vulnerability.</p> <ul style="list-style-type: none">•  Critical•  High•  Medium•  Low

When you review the detected issues, you can do the following:

- To see a detailed description of an issue, right-click the issue, and then select **View Vulnerability Details**.

The **Vulnerability Details** window opens and provides a detailed description of the issue, examples, and recommendations for how to fix the issue.



Note: If the **Vulnerability Details** window is already open, click an issue to see the corresponding details in this window.

- To locate the line of code where the issue was found, double-click the issue.

Tip: To change how the issues are grouped, right-click the **Error List**, and then select **Grouping**.

Suppressing Categories of Issues

As you review the issues, you might want to completely suppress some exposed issues. It is useful to suppress issues if you are sure that the vulnerability category is not, and will never be, an issue of concern. You might also want to suppress warnings for specific issue categories that might not be high priority or of immediate concern.

You can suppress issue categories for the entire solution. The issue category is not reported again for the solution unless you unsuppress it (see ["Unsuppressing Categories of Issues" below](#)).

To suppress a configuration issue category:

1. Open the **Error List** window if it is not currently open.
2. In the **Error List** window, right-click an issue, and then select **Suppress Category**.

Note: To suppress structural issues, use Visual Studio's feature of suppressing code analysis violations. For instructions, see the Visual Studio documentation.

Categories of configuration issues that you suppress are stored in a `.FortifyIgnore` file with your Visual Studio solution file. You can share this file with other members of your organization. For more information about this Fortify issue suppression file, see ["Using the Fortify Issue Suppression File" on page 18](#).

Suppressed issues are no longer highlighted in the code as a Fortify issue. The visibility of suppressed issues in the **Error List** or **Security Assistant** window depends on the setting for the **Suppression State** column).

Unsuppressing Categories of Issues

To unsuppress a configuration issue category:

1. Open the **Error List** window if it is not currently open.
2. To make sure that suppressed issues are visible, click the filter icon in the **Suppression State** column, and then select the **Suppressed** check box.
3. Right-click an issue, and then select **Unsuppress Category**.

Note: To unsuppress structural issues, use Visual Studio's feature of unsuppressing code analysis violations. For instructions, see the Visual Studio documentation.

To unsuppress all configuration issues for the solution, remove (or rename) the `.FortifyIgnore` file that is located with the solution file (see ["Using the Fortify Issue Suppression File" on page 18](#)).

Scanning Solutions for Issues

You can use Fortify Security Assistant to analyze a solution and identify security issues. You cannot make any code changes during the analysis.

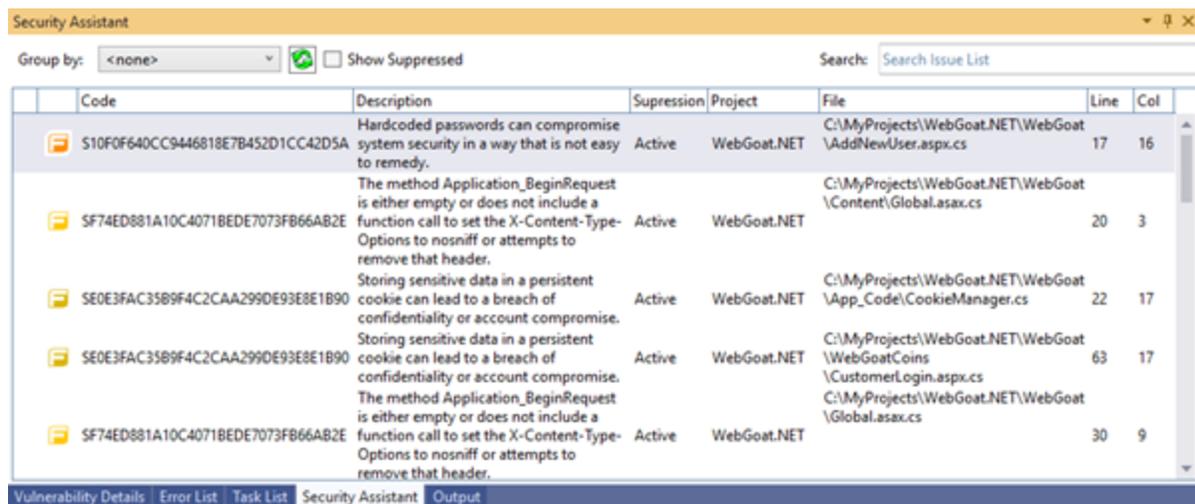
To scan a solution for issues:

- From the Fortify Security Assistant extension menu, select **Analyze Solution**.

Fortify Security Assistant displays any possible issues detected in the **Security Assistant** window. For information about reviewing the security issues in this window, see ["Working with Security Issues in the Security Assistant Window"](#) below.

Working with Security Issues in the Security Assistant Window

After you analyze a solution, Fortify Security Assistant displays all the detected security issues for the solution in the **Security Assistant** window.



The screenshot shows the Security Assistant window with a table of detected security issues. The table has columns for Code, Description, Suppression, Project, File, Line, and Col. The issues listed are:

Code	Description	Suppression	Project	File	Line	Col
S10F0F640CC9446818E7B452D1CC42D5A	Hardcoded passwords can compromise system security in a way that is not easy to remedy.	Active	WebGoat.NET	C:\MyProjects\WebGoat.NET\WebGoat\AddNewUser.aspx.cs	17	16
SF74ED881A10C4071BEDE7073FB66AB2E	The method Application_BeginRequest is either empty or does not include a function call to set the X-Content-Type-Options to nosniff or attempts to remove that header.	Active	WebGoat.NET	C:\MyProjects\WebGoat.NET\WebGoat\Content\Global.asax.cs	20	3
SE0E3FAC35B9F4C2CAA299DE93E8E1B90	Storing sensitive data in a persistent cookie can lead to a breach of confidentiality or account compromise.	Active	WebGoat.NET	C:\MyProjects\WebGoat.NET\WebGoat\App_Code\CookieManager.cs	22	17
SE0E3FAC35B9F4C2CAA299DE93E8E1B90	Storing sensitive data in a persistent cookie can lead to a breach of confidentiality or account compromise.	Active	WebGoat.NET	C:\MyProjects\WebGoat.NET\WebGoat\WebGoatCoins\CustomerLogin.aspx.cs	63	17
SF74ED881A10C4071BEDE7073FB66AB2E	The method Application_BeginRequest is either empty or does not include a function call to set the X-Content-Type-Options to nosniff or attempts to remove that header.	Active	WebGoat.NET	C:\MyProjects\WebGoat.NET\WebGoat\Global.asax.cs	30	9

The following table describes the Fortify information provided for each issue.

Column	Description
Fortify Priority Order	A colored icon indicates the Fortify Priority Order used to categorize the severity of a vulnerability. <ul style="list-style-type: none"><li data-bbox="516 436 672 468">•  Critical<li data-bbox="516 516 646 548">•  High<li data-bbox="516 596 688 627">•  Medium<li data-bbox="516 676 639 707">•  Low
Description	A brief description of the issue.
Suppression State	Indicates whether the issue has been suppressed (hidden). To change whether suppressed issues are visible or not, select or clear the Show Suppressed check box.

When you review the detected issues, you can do the following:

- To see a detailed description of an issue, right-click the issue, and then select **View Vulnerability Details**.

The **Vulnerability Details** window opens and provides a detailed description of the issue, examples, and recommendations for how to fix the issue.



Note: If the **Vulnerability Details** window is already open, click an issue to see the corresponding details in this window.

- To locate the line of code where the issue was found, select the issue.
- To change how the issues are grouped (by Fortify Priority Order or project), select the grouping from the **Group By** list.
- To refresh the issues list after you make changes to the code, click **Refresh** .
- To show or hide suppressed issues in the window, select or clear the **Show Suppressed** check box. For instructions on how to suppress issues, see "[Suppressing Categories of Issues](#)" on page 15.
- Search for issues by typing a string in the **Search** box. This searches for the string in any column.

Using the Fortify Issue Suppression File

You can use the Fortify issue suppression file to suppress categories of configuration issues and to exclude files or directories from having any configuration issues reported. You can share this file with other members of your organization.

Fortify Security Assistant creates the Fortify issues suppression file (`.FortifyIgnore`) in the same directory as your project solution when you first suppress an issue category. You can edit this file using

a text editor. After you make changes to the issue suppression file, re-analyze your solution to apply the suppressions.

Each line in this file can contain either:

- Suppression of a Fortify category
Specify the full Fortify category to suppress issues of that category for all files in the project. Fortify Security Assistant adds a line to the `.FortifyIgnore` file each time you suppress a category in the **Error List** window.

For example:

```
ASP.NET Misconfiguration: Debug Information  
Cookie Security: HTTPOnly not Set on Application Cookie
```

- Suppression of all issues in one or more files
For example, you might want to use this to suppress all issues in files that contain generated code.

The syntax for this type of suppression follows these rules:

- The first character must be a slash (/) or backslash (\).
- Use a single asterisk (*) to represent zero or more file name characters.
- Use two asterisks (**) to represent zero or more directories or all directory contents when specified at the end of the line.
- Paths must be relative to the `.FortifyIgnore` file location. You can use either the slash or backslash as the directory separator.

For example, the following line suppresses all configuration issues for any file with the `.xml` extension in the `Generated` directory:

```
/**/Generated/*.xml
```

The following example suppresses all configuration issues in one specific file:

```
/my/full/path/file.config
```

The following example suppresses all configuration issues in all files with the `.config` extension in the root solution directory:

```
/*.config
```

The following example suppresses all configuration issues for all files in the `test` directory:

```
/test/**
```

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email.

Note: If you are experiencing a technical issue with our product, do not email the documentation team. Instead, contact Micro Focus Fortify Customer Support at <https://www.microfocus.com/support> so they can assist you.

If an email client is configured on this computer, click the link above to contact the documentation team and an email window opens with the following information in the subject line:

Feedback on User Guide (Fortify Security Assistant Extension for Visual Studio 21.1.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to fortifydocteam@microfocus.com.

We appreciate your feedback!