OpenText™ Fortify Security Assistant Extension for Visual Studio

User Guide

Version : 22.2

PDF Generated on : May 26, 2026

Table of Contents

1. User Guide

Software Version: 22.2.0

Document Release Date: May 2026

Software Release Date: May 2026

1.1. Change Log

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

Software Release / Document Version	Changes
22.2.0	Updated: • Fortify Security Assistant Requirements - Supported added for Visual Studio 2026
22.1.0	Updated: • Fortify Security Assistant Requirements - Supported added for Visual Studio 2022
21.1.0	Updated: • Suppressing Categories of Issues - Changes made for how to suppress different types of issues Added: • Working with Security Assistant Issues in the Security Assistant Window - Described the new window that shows detected issues from an analyzed solution
20.1.0	Updated: • Fortify Security Assistant Requirements - Changed the required .NET Framework version

1.2. Introduction

This section contains the following topics:

1.2.1. 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. All detected security issues contain detailed information about security risks and recommendations for how to address each security vulnerability. Use this extension to 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

1.2.2. 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.

1.2.3. Fortify Security Assistant Requirements

Fortify Security Assistant requires the following:

- 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 either:

  - Download the Fortify Security Content directly from the Fortify Rulepack update server or from a Micro Focus Fortify Software Security Center server.
  - Use a local copy of Fortify Security Content

    You might use this option if you do not have a network connection to a server. For instructions, see Obtaining Fortify Security Content from the Local System.

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

Software	Versions
Visual Studio	2026 Community, Professional, and Enterprise 2022 Community, Professional, and Enterprise 17.14 or later 2019 Community, Professional, and Enterprise
.NET Framework	4.7.2 or later

1.3. Installation and Configuration

This section contains the following topics:

1.3.1. 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.

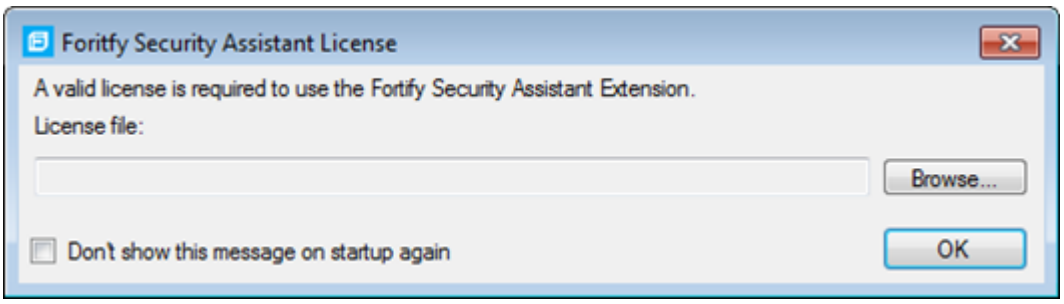
To install the Fortify Security Assistant extension:

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

Note

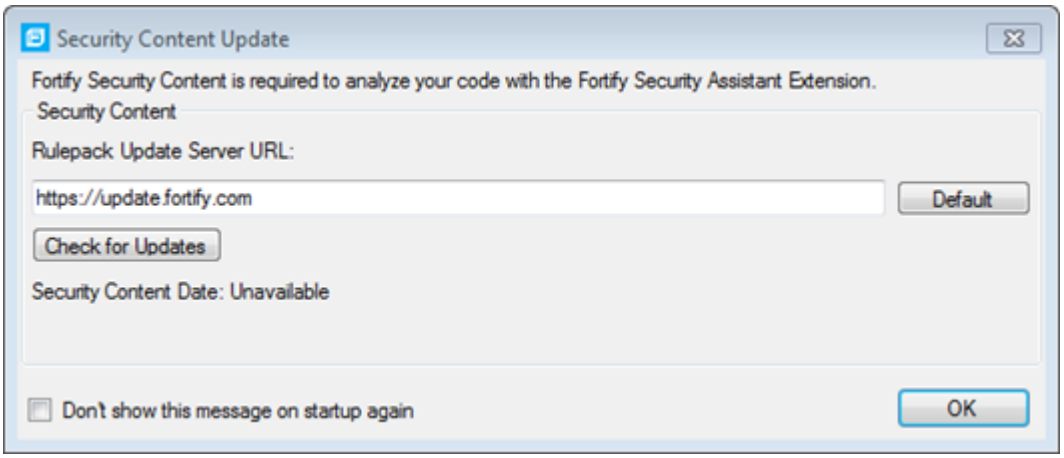
To install this extension as an administrator and allow all users to use the extension, download the VSIX file from the Visual Studio Marketplace and then install it using `VSIXInstaller` with the `/admin` option from the Command Prompt.

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).



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**.

  To download Fortify Security Content from a Micro Focus Fortify Software Security Center server, append `/d3srv` to the Fortify Software Security Center URL (for example: `https://my.domain.com:8443/ssc/d3srv`).

  > **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 Rulepack update server and you want to use a local copy of Fortify Security Content. For instructions, see Obtaining Fortify Security Content from the Local System).

1.3.2. Obtaining Fortify Security Content from the Local System

If you do not have a network connection to the Fortify Rulepack update server, 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 Rulepack update server 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 ZIP file:

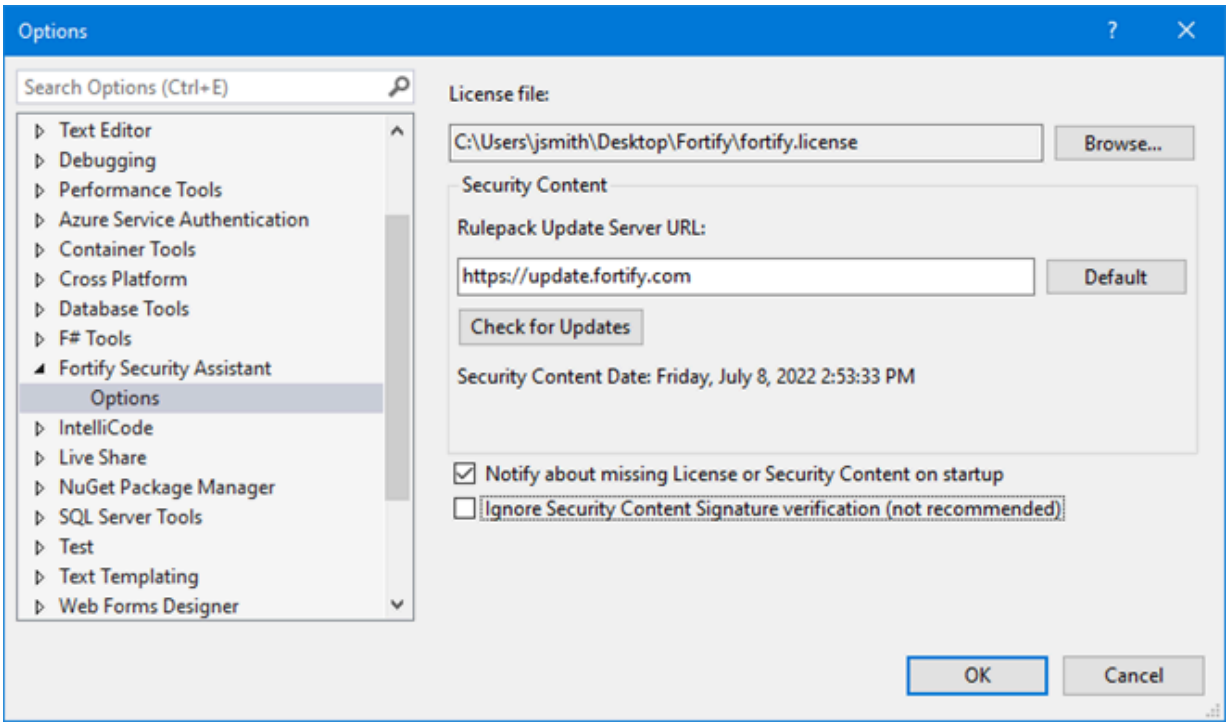
1. Navigate to `C:\Users\<username>\AppData\Local\Fortify\SecurityAssistantVS-<version>`.
2. Place the Fortify Security Content file `rulePacks.zip` in this folder.
3. Restart Visual Studio.

1.3.3. 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 Rulepack update server, you must be connected to the Internet and have your network connections configured to access the Fortify Rulepack update server (https://update.fortify.com). To update Fortify Software Security Content from a local file, see Using Fortify Security Content from a Local Package.

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:
    1. In the **Rulepack Update Server URL** box, type a URL from which you can download Fortify Security Content.

        To download Fortify Security Content from a Micro Focus Fortify Software Security Center server, append `/d3srv` to the Fortify Software Security Center URL (for example: `https://my.domain.com:8443/ssc/d3srv`).

If you want to obtain the Fortify Security Content from a URL other than the Fortify Rulepack update server or , 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 Rulepack update server.

2. 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.

1.3.4. 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.

1.4. 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 Projects for Issues).

This section contains the following topics:

1.4.1. 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).

To review the security issues:

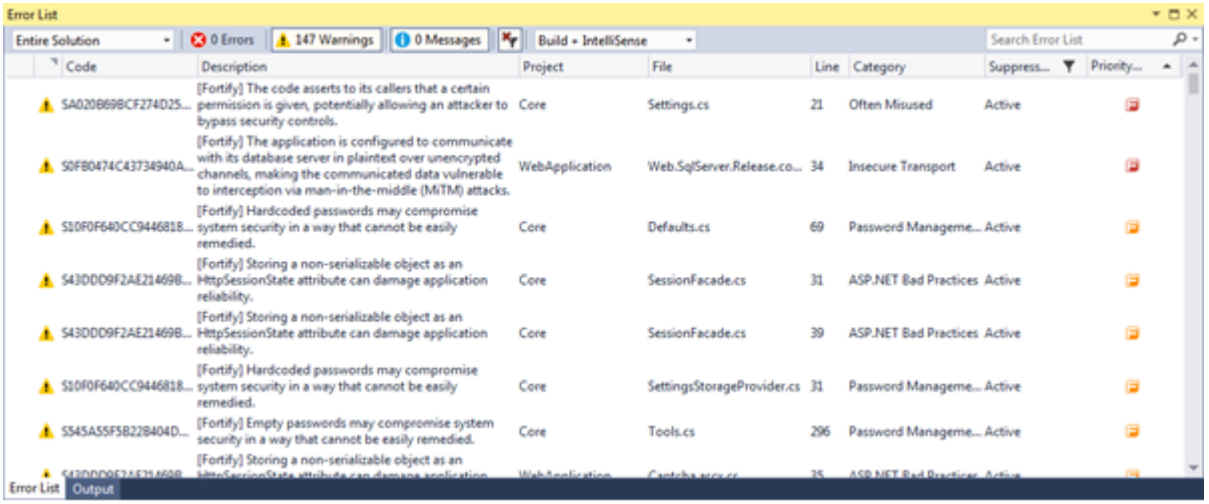
- Pause your cursor over the highlighted code to open a tooltip that briefly describes the issue as shown in the following example:

- 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 Assistant Issues in the Error List.

1.4.2. 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.



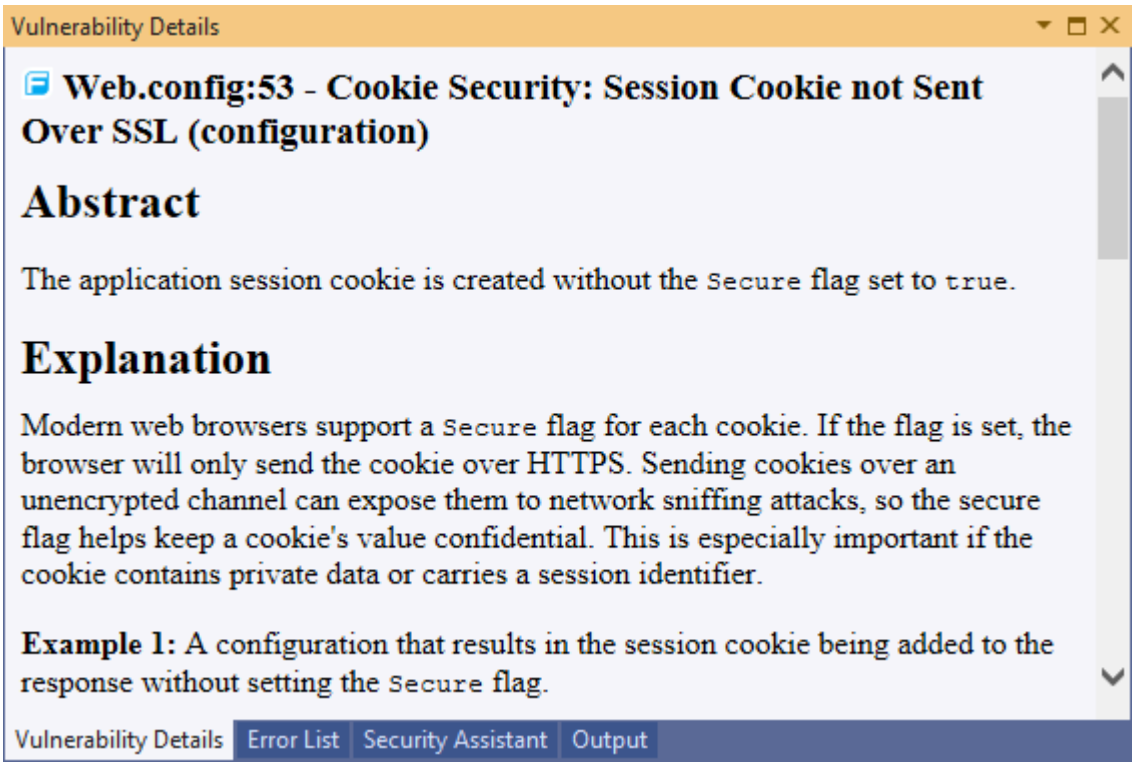
The following table describes the Fortify information provided for each issue.

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.
Priority Order	A colored icon indicates the Fortify Priority Order used to categorize the severity of a vulnerability. • 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**.

1.4.2.1. 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 Issues).

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.

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).

1.4.2.2. 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).

1.4.3. 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.

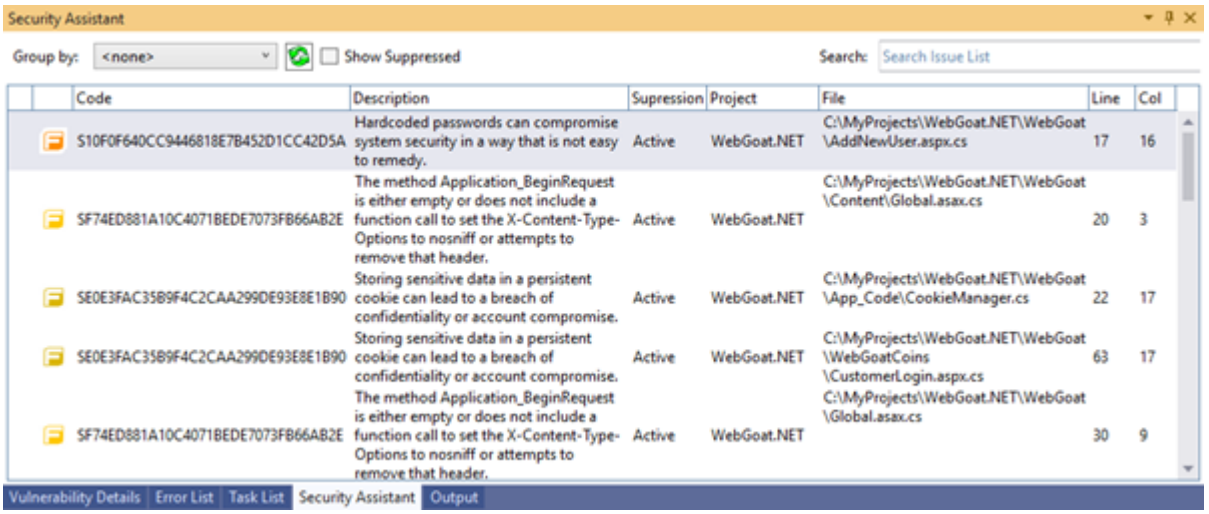
To scan a solution for issues:

- 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 Assistant Issues in the Security Assistant Window.

1.4.4. 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.



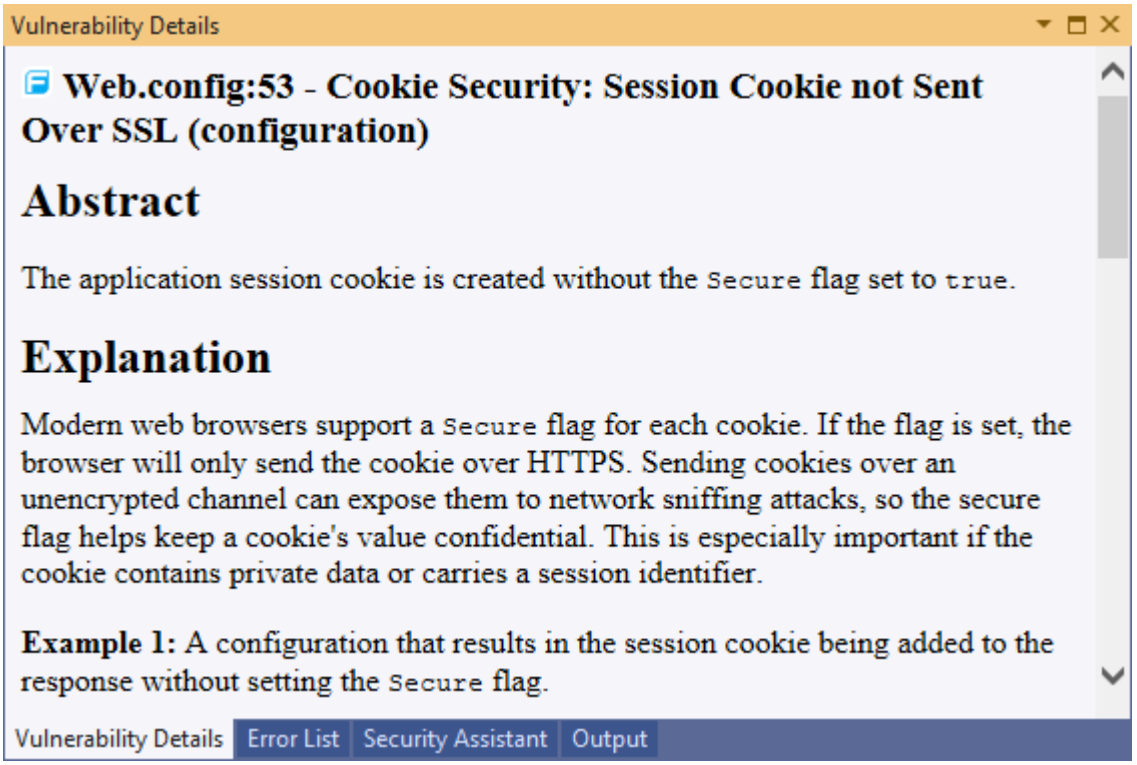
The following table describes the Fortify information provided for each issue.

Column	Description
Fortify Priority Order	A colored icon indicates the Fortify Priority Order used to categorize the severity of a vulnerability. • Critical • High • Medium • 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.

- Search for issues by typing a string in the **Search** box. This searches for the string in any column.

1.4.5. 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:

  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:

Example

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

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

Example

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

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

Example

```
/*.config
```

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

Example

```
/test/**
```

For more info, visit https://docs.microfocus.com