

OWASP Compliance

The Parasoft OWASP Compliance artifact is a set of assets for your DTP infrastructure that enable you to demonstrate compliance with OWASP coding guidelines. The artifact is shipped as part of the [Security Compliance Pack for DTP 5.4.2](#). Contact your Parasoft representative to download and license the Security Compliance Pack.

In this section:

- [About OWASP Top 10](#)
- [Prerequisites](#)
- [Process Overview](#)
- [OWASP Compliance Assets](#)
- [Deploying the OWASP Compliance Assets](#)
- [Adding the OWASP Dashboards](#)
- [OWASP Compliance Widgets](#)
- [Viewing the OWASP Compliance Report](#)
- [Profile Configuration](#)

About OWASP Top 10

OWASP Top 10: The Ten Most Critical Web Application Security Risks is a collection of coding guidelines for ensuring web application security. OWASP Top 10 is focused on identifying the most serious web application security risks that affect many organizations. For each risk, OWASP provides information about the likelihood of a security vulnerability resulting from a violation, as well as its technical impact, using a ratings scheme based on the OWASP Risk Rating Methodology.

Where possible, the names of the risks in the Top 10 are aligned with Common Weakness Enumeration (CWE) weaknesses to promote generally accepted naming conventions and to reduce confusion.

See https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project for additional information about OWASP Top 10.

In this documentation, we assume that you are familiar with the OWASP Top 10 guidelines, CWE, and associated terminology.

Prerequisites

Code analysis data is required from one of the following Parasoft tools

- Parasoft dotTEST 10.4.2 or later with appropriate Security Compliance Pack licenses.
- Parasoft Jtest 10.4.2 or later with appropriate Security Compliance Pack licenses.

See [Security Compliance Pack for DTP 5.4.2](#) for additional prerequisites information.

Process Overview

1. Install the [Security Compliance Pack for DTP 5.4.2](#) into DTP Extension Designer.
2. Deploy the OWASP Compliance artifact into your DTP environment. This also deploys the [OWASP Compliance assets](#).
3. Analyze code using the OWASP Top 10 2017 test configuration and report violations to DTP. You can configure your Parasoft tool to use the local test configuration or the test configuration shipped with the Security Compliance Pack.
4. Add the OWASP Compliance dashboard and widgets to your DTP interface. The dashboard widgets and shows the reported violations within the context of OWASP guidelines.
5. Interact with the widgets and reports to identify code that needs to be fixed to achieve your compliance goals.

OWASP Compliance Assets

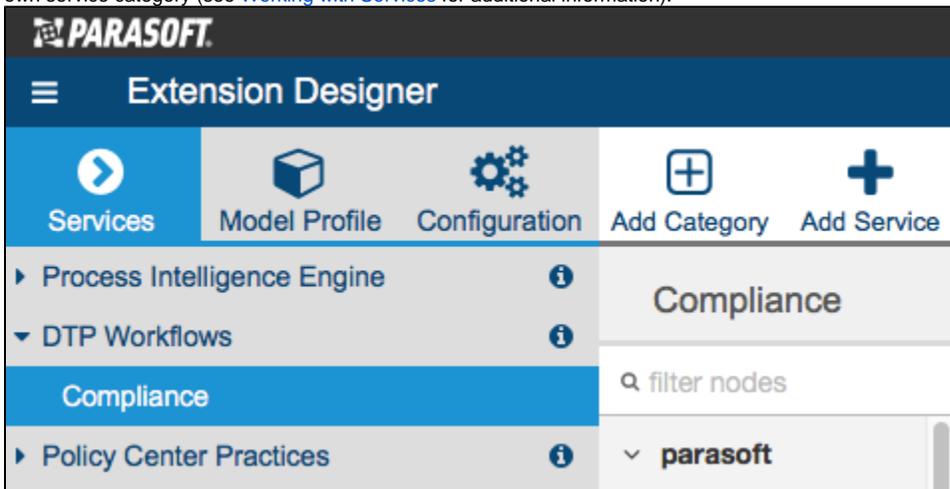
- **OWASP-Top10-dotNET.xml**: This configuration file provides OWASP-oriented compliance categories in DTP interfaces for code analysis performed on .NET projects.
- **OWASP-Top10-Java.xml**: This configuration file provides OWASP-oriented compliance categories in DTP interfaces for code analysis performed on Java projects.
- **OWASP-Top10-Score-dotNET.xml**: This configuration file provides OWASP score compliance categories in DTP interfaces for code analysis performed on .NET projects.
- **OWASP-Top10-Score-Java.xml**: This configuration file provides OWASP score compliance categories in DTP interfaces for code analysis performed on Java projects.
- **owaspTop10-dotNET.json**: This file adds the OWASP Top 10 2017 dashboard template for .NET code analysis results. See [Custom Dashboard Templates](#) for additional information about understanding dashboards.
- **owaspTop10-Java.json**: This file adds the OWASP Top 10 2017 dashboard template for Java code analysis results.
- **OWASP Compliance.json**: This file is the custom logic flow for Extension Designer. Installing the Security Compliance Pack adds the flow to the Extension Designer library. You can then add the flow to a service and deploy it to your DTP infrastructure.
- **owasp-top10-dotnet.json**: This file is the Extension Designer profile for .NET code analysis. It assigns values to violations for OWASP weaknesses according to the standard.

- **owasp-top10-java.json**: This file is the Extension Designer profile for Java code analysis. It assigns values to violations for OWASP weaknesses according to the standard.
- **owasp-compliance.model.json**: This file defines the model type for the owasp-top10-dottest.json profile. See [Working with Model Profiles](#) for additional information about models and profiles.
- **OWASP Top 10-2017 [Parasoft 10.4.2].properties**: This is the test configuration shipped with the compliance pack. You can configure your tool to run this test configuration or the test configuration shipped with your tool.
- **OWASP_Top_10-2017.pdf**: For your convenience, PDFs that show the association between Parasoft rules and OWASP guidelines are located in the <PACK>/rules/test and <PACK>/rules/dottest directories.

Deploying the OWASP Compliance Assets

OWASP Compliance is installed as part of the Security Compliance Pack (see [Installation](#) for instructions). After installing the artifact, you must deploy the assets to your DTP environment.

1. Choose **Extension Designer** from the DTP settings (gear icon) menu.
2. Click the **Services** tab and expand the **DTP Workflows** service category. You can deploy assets under any service category you wish, but we recommend using the DTP Workflows category to match how Parasoft categorizes the assets. You can also click **Add Category** to create your own service category (see [Working with Services](#) for additional information).



3. You can deploy the artifact to an existing service or add a new service. The number of artifacts deployed to a service affects the overall performance. See [Extension Designer Best Practices](#) for additional information. Choose an existing service and continue to step 5 or click **Add Service**.
4. Specify a name for the service and click **Confirm**.
5. The tabbed interface helps you keep artifacts organized within the service. Organizing your artifacts across one or more tabs does not affect the performance of the system. Click on a tab (or click the + button to add a new tab) and click the vertical ellipses menu.
6. Choose **Import> Library> Workflows> Security> OWASP Compliance** and click anywhere in the open area to add the artifact to the service.
7. Click **Deploy** to finish deploying the artifact to your DTP environment.
8. Return to DTP and refresh your dashboard. You will now be able to add OWASP widgets.

Adding the OWASP Dashboards

The OWASP Top 10 2917 - .NET and OWASP Top 10 2917 - Java dashboard templates enable you to quickly add a set of preconfigured widgets that monitor compliance with OWASP Top 10 guidelines (see [OWASP Compliance Widgets](#)). The dashboard template are deployed to your DTP environment as part of the Security Compliance Pack installation. If you do not see the dashboard template, restart DTP Services (see [Stopping DTP Services](#) and [Starting DTP Services](#)).

1. Click **Add Dashboard** from the DTP toolbar and specify a name when prompted.
2. (Optional) You can configure the default view for the dashboard by specifying the following information:
 - a. Choose the filter associated with your project in the filter drop-down menu. A filter represents a set of run configurations that enabled custom views of the data stored in DTP. See [DTP Concepts](#) for additional information.
 - b. Specify a range of time from the Period drop-down menu.
 - c. Specify a range of builds from the Baseline Build and Target Build drop-down menus.

3. Enable the **Create dashboard from a template** option and choose either the OWASP Top 10 2017 - .NET or Java template from the drop-down menu.

The screenshot shows a web form titled "Add Dashboard". It contains several input fields and radio button options. The "Name:" field contains "OWASP - dotTEST". The "Filter:" dropdown is set to "OWASP dotTEST". The "Period:" dropdown is set to "Last 10 builds". The "Baseline Build:" dropdown is set to "First Build in Period". The "Target Build:" dropdown is set to "Latest Build". There are three radio button options: "Create an empty dashboard", "Create dashboard from a template:", and "Copy an existing dashboard.". The "Create dashboard from a template:" option is selected and highlighted with a red rectangle. Below this option is a dropdown menu showing "OWASP Top 10 2017 - .NET". Below the "Copy an existing dashboard." option is a dropdown menu showing "Default Dashboard". Below the "Follow a shared dashboard:" option is a dropdown menu showing "No shared dashboards available". At the bottom right of the form are two buttons: "Cancel" and "Create".

4. Click **Create** to finish adding the dashboard.

Manually Adding OWASP Widgets to an Existing Dashboard

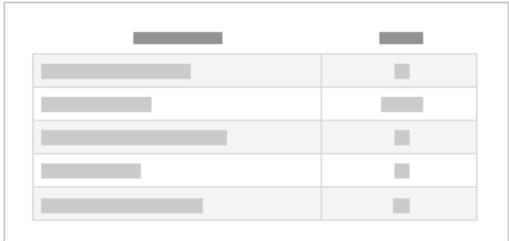
You can also add the OWASP widgets shipped with the artifact to an an existing dashboard. See [Adding Widgets](#) for general instructions on adding widgets to a dashboard. After deploying the artifact, the OWASP widgets will appear in the OWASP category in the Add Widget overlay:

Add Widget

OWASP	Compliance by Category/Severity
Build Results	OWASP Compliance - Percentage
Code	OWASP Compliance - Risk
Compliance	OWASP Compliance - Status
Coverage	OWASP Compliance - Weaknesses by Status
Diagnostics	OWASP Violations by Weakness - TreeMap
Metrics	
Process Intelligence	
Static Analysis	
Tests	
Custom	

Compliance by Category/Severity

4 x 2



Shows the number and percentage of rules in compliance grouped by rule categories and severity.

Title:

Filter:

Compliance:

The following configurations are available:

Title	Enter a new title to replace the default title that appears on the dashboard.
Filter	Choose a specific filter or Dashboard Settings from the drop-down menu. See Creating and Managing Filters for additional information.
Target Build	Choose a specific build from the drop-down menu. The build selected for the entire dashboard is selected by default. See Using Build Administration for additional information about understanding builds.
Compliance Profile	Specify a compliance profile (see Profile Configuration). The compliance profile data is used in compliance reports.
Exploitability	Choose an exploitability category (1 - 3) that you want to view. Refer to the OWASP guidelines for details. Only applies to the OWASP Compliance - Weakness by Status widget.
Prevalence	Choose a prevalence category (1 - 3) that you want to view. Refer to the OWASP guidelines for details. Only applies to the OWASP Compliance - Weakness by Status widget.
Detectability	Choose a detectability category (1 - 3) that you want to view. Refer to the OWASP guidelines for details. Only applies to the OWASP Compliance - Weakness by Status widget.
Impact	Choose an impact level (1 - 3) that you want to view. Refer to the OWASP guidelines for details. Only applies to the OWASP Compliance - Weakness by Status widget.

OWASP Compliance Widgets

The dashboard template includes a mix of OWASP-specific widgets shipped with the artifact and native DTP widgets configured to show OWASP compliance categories specified in the OWASP-Top10-dotNET.xml and OWASP-Top10-Java.xml files (see [OWASP Compliance Assets](#)).

OWASP Compliance Risk

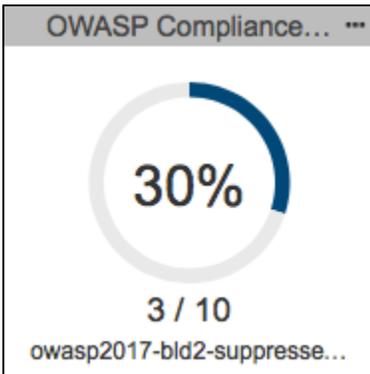
This widget is included with the OWASP Compliance artifact. It provides a chart showing the distribution of violations according to its risk as defined in the OWASP standard.

OWASP Compliance - Risk			
Exploitability	Weakness Prevalence	Weakness Detectability	Technical Impacts
Easy: 11	Widespread: 9	Easy: 13	Severe: 4
Average: 2	Common: 4	Average: 0	Moderate: 9
Difficult: 0	Uncommon: 0	Difficult: 0	Minor: 0

Mouse over a cell in the chart to view the number of violations and suppressions for the specified risk level. Click on a cell to open the [OWASP Compliance Report](#) filtered according to the risk.

OWASP Compliance Percentage

This widget is included with the OWASP Compliance artifact. It shows the percentage of OWASP weaknesses that the code is in compliance with. Click on the widget to open the [OWASP Compliance Report](#).



OWASP Compliance Status

This widget is included with the OWASP Compliance artifact. It shows the current state of compliance with OWASP Top 10.



There are seven possible states:

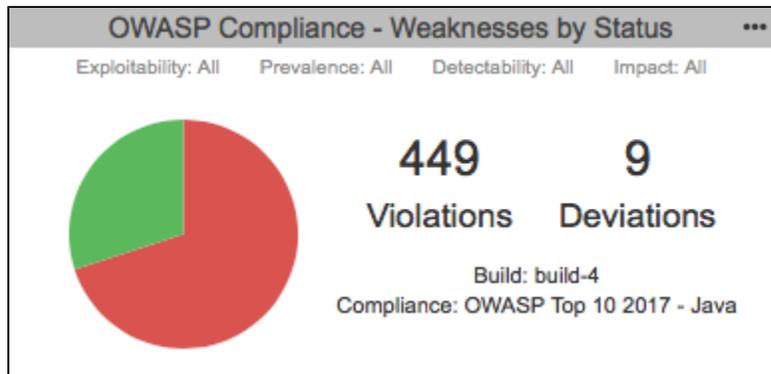
- **No rules enabled:** Code analysis has not been reported to DTP or the OWASP Top 10 test configuration was not executed by Jtest or dotTEST.
- **N/A:** The OWASP assets have not been deployed to a service or the service is not running. See [Deploying the OWASP Compliance Assets](#).
- **Compliant with Deviations:** Any violations reported are acceptable and have been suppressed. See [Deviations Report](#) for additional information about deviations/suppressions.
- **Compliant with Violations:** Any violations reported do not represent a significant risk.
- **Compliant:** No violations are reported and no suppressions have been applied.
- **Not Compliant:** Violations have been reported that represent a significant risk.

- **Missing rule(s) in analysis:** Parasoft code analysis rules documented in the profile were not included in the specified build. Make sure all rules are enabled in Jtest or dotTEST and re-run analysis.

Click on the widget to open the [OWASP Compliance Report](#).

OWASP Compliance - Weakness by Status

This widget is included with the OWASP Compliance artifact. The red segment of the pie chart represents the weaknesses that the code is not compliant with. The green segment represents weaknesses that the code is in compliance with. The widget also shows the number of violations and deviations.

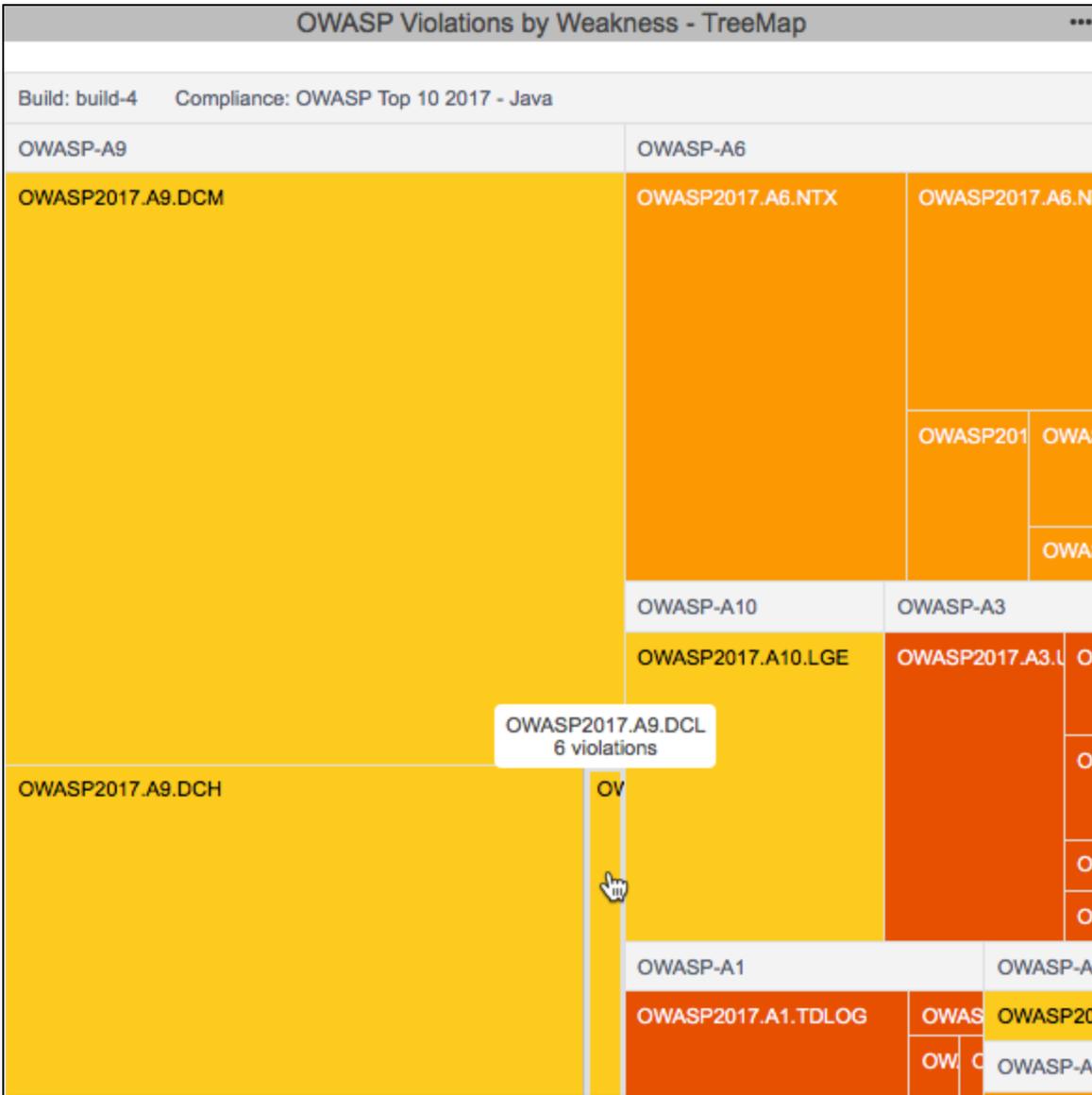


You can perform the following actions:

- Click on a segment in the pie chart to open the [OWASP Compliance Report](#) filtered by the selected status.
- Click on the Violations section to open an unfiltered [OWASP Compliance Report](#).
- Click on the Deviations section to open the [Deviations Report](#).

OWASP Violations in Compliance - Treemap

This widget shows the violations grouped by compliance in a tree map. Each tile is assigned a color and represents a compliance category. See [Configuring Security Compliance Pack Widgets](#) for details on how to configure this widget.



Rules in Compliance

This widget is an implementation of the native DTP Rules in Compliance widget. It shows the percentage of Parasoft rules that are mapped to OWASP weaknesses that are not reporting a violation (are in compliance). See [Rules in Compliance - Summary](#) for details about the widget.



Categories - Top 5 Table

The dashboard includes an instance of the native Categories - Top 5 Table widget configured for OWASP Top 10. It shows the five OWASP categories with the most violations. See [Categories - Top 5 Table](#) for details about the widget.

Top 5 OWASP Categories	
Compliance: OWASP TOP 10 2017 - Java	
Name	# of Violations
A9:2017-Using Components with Kno...	253
A6:2017-Security Misconfiguration	92
A10:2017-Insufficient Logging&Monito...	39
A3:2017-Sensitive Data Exposure	33
A1:2017-Injection	24
more...	

Rules - Top 5 Table

The dashboard includes an instance of the native Rules - Top 5 Table widget configured for OWASP Top 10. It shows the five Parasoft rules mapped to OWASP categories with the most violations. See [Rules - Top 5 Table](#) for details about the widget.

Top 5 OWASP Violations	
Compliance: OWASP TOP 10 2017 - .NET	
Name	# of Violations
OWASP2017.A4.PDTDP	163
OWASP2017.A9.DCM	161
OWASP2017.A6.NCSAE	161
OWASP2017.A9.DCH	86
OWASP2017.A6.LGE	72
more...	

Viewing the OWASP Compliance Report

The main OWASP compliance report provides details about your OWASP compliance status and serves as the primary document for demonstrating compliance.

OWASP Compliance Report

Filter: test-owasp-project Target Build: owasp2017-bld2-suppressed-2vio Compliance Profile: OWASP Top 10 2017 - .NET Analysis Tool: Parasoft dotTEST 10.4.1
Revision Date: 2019-01-28

Project Compliance: ✖ Not Compliant

[Weakness Detection Plan](#) [Deviation Report \(Total: 2\)](#) [Build Audit Report](#)

Exploitability: Prevalence: Detectability: Impact: Compliance:

Weakness	Exploitability	Prevalence	Detectability	Impact	Compliance	# of Violations	# of Deviations	
							In-Code Suppressions	DTP Suppressions
OWASP-A1	Easy: 3	Common: 2	Easy: 3	Severe: 3	✖ Not Compliant	72	0	0
OWASP-A2	Easy: 3	Common: 2	Average: 2	Severe: 3	✔ Compliant	0	0	0
OWASP-A3	Average: 2	Widespread: 3	Average: 2	Severe: 3	✔ Compliant	0	0	0
OWASP-A4	Average: 2	Common: 2	Easy: 3	Severe: 3	✖ Not Compliant	163	0	0
OWASP-A5	Average: 2	Common: 2	Average: 2	Severe: 3	✖ Not Compliant	2	0	0
OWASP-A6	Easy: 3	Widespread: 3	Easy: 3	Moderate: 2	✖ Not Compliant	250	0	0
OWASP-A7	Easy: 3	Widespread: 3	Easy: 3	Moderate: 2	✖ Not Compliant	70	0	0
OWASP-A8	Difficult: 1	Common: 2	Average: 2	Severe: 3	✖ Not Compliant	45	1	1
OWASP-A9	Average: 2	Widespread: 3	Average: 2	Moderate: 2	✖ Not Compliant	253	0	0
OWASP-A10	Average: 2	Widespread: 3	Difficult: 1	Moderate: 2	✔ Compliant	0	0	0

10 items

You can perform the following actions:

- Use the drop-down menus to sort by a weakness property.
- Click on a link in the # of Violations, In-Code Suppression, or DTP Suppressions column to view the violations in the [Violations Explorer](#).
- Click on a link in the Weakness column to open the [Weakness Detection Plan](#). The link goes directly to the specific weakness so that you can review the Parasoft code analysis rule or rules detecting the weaknesses.
- Open one of the OWASP Compliance sub-reports ([Weakness Detection Plan](#), [Deviations Report](#), [Build Audit Report](#)).
- Click **Download PDF** to export a printer-friendly PDF version of the report data. If you added a custom graphic to DTP as described in [Adding a Custom Graphic to the Navigation Bar](#), the PDF will also be branded with the graphic.

Weakness Detection Plan

The Weakness Detection Plan shows which static analysis rules are used to enforce the OWASP guidelines and is intended to describe how you are enforcing each guideline. This report uses the data specified in the compliance profile (see [Profile Configuration](#)). In the profile, you can configure the values associated with each weakness property to better reflect the specific challenges associated with your project. The Analysis Tool column should refer to the static analysis rule.

OWASP Weakness Detection Plan

Compliance Profile: OWASP Top 10 2017 - dotTEST Revision Date: 2018-11-16 Analysis Tool: Parasoft dotTEST 10.4.1

Weakness	Description	Exploitability	Prevalence	Detectability	Impact	Score	Analysis Tool
OWASP-A1	Injection	Easy: 3	Common: 2	Easy: 3	Severe: 3	8	OWASP2017.A1.TDCMD OWASP2017.A1.TDFNAMES OWASP2017.A1.TDLDP OWASP2017.A1.TDNET OWASP2017.A1.TDSQL OWASP2017.A1.TDSQLC OWASP2017.A1.AUPS OWASP2017.A1.VPPD
OWASP-A2	Broken Authentication	Easy: 3	Common: 2	Average: 2	Severe: 3	7	OWASP2017.A2.HPW
OWASP-A3	Sensitive Data Exposure	Average: 2	Widespread: 3	Average: 2	Severe: 3	7	OWASP2017.A3.RSFSS OWASP2017.A3.SSFP OWASP2017.A3.ACCA OWASP2017.A3.DNCCKS OWASP2017.A3.ICA OWASP2017.A3.UOWR OWASP2017.A3.HARDCONN
OWASP-A4	XML External Entities (XXE)	Average: 2	Common: 2	Easy: 3	Severe: 3	7	OWASP2017.A4.PDTDP
OWASP-A5	Broken Access Control	Average: 2	Common: 2	Average: 2	Severe: 3	6	OWASP2017.A5.TDSQL OWASP2017.A5.TDFNAMES OWASP2017.A5.AUEP OWASP2017.A5.ICA OWASP2017.A5.UAA

Deviations Report

Your code can contain violations and still be OWASP-compliant as long as the deviations from the standard are documented and that the safety of the software is unaffected. Deviations are code analysis rules that have been suppressed either directly in the code or in the DTP Violations Explorer. See the dotTEST and Jtest documentation for details on suppressing violations in the code. See [Suppressing Violations](#) in the Violations Explorer documentation for information about suppressing violations in DTP.

OWASP Deviation Report

Filter: OWASP dotTEST Target Build: docs-OWASP Top 10 2017 Compliance Profile: OWASP Top 10 2017 - .NET Analysis Tool: Parasoft dotTEST 10.4.1 Revision Date: 2018-12-12

Only Deviations:

OWASP-A1 Injection ! - 1 Deviations

Rule ID: OWASP2017.A1.VPPD
Deviation Type: DTP Suppression
Action: None
Risk/Impact: Undefined
Suppression Reason: Example suppression
Suppression Author: admin

Modification History

<p>User: admin Date: 2018-11-20 12:06:32 PM</p>	<p>Field: Suppression Author Old Value: N/A New Value: admin</p> <p>Field: Suppression Date Old Value: N/A New Value: 2018-11-20T12:06:32.265</p> <p>Field: Suppression Reason Old Value: N/A New Value: Example suppression</p>
---	---

OWASP-A2 Broken Authentication ✔ - No Deviations

OWASP-A3 Sensitive Data Exposure ✔ - No Deviations

OWASP-A4 XML External Entities (XXE) ✔ - No Deviations

OWASP-A5 Broken Access Control ✔ - No Deviations

Click on the **Deviations Report** link in the OWASP Compliance report to open the Deviations Report.

The Deviations Report shows all guideline IDs and headers, but guidelines that have been suppressed will show additional information. You can enable the **Only Deviations** option to only show deviations.

Build Audit Report

The Build Audit Report shows an overview of code analysis violations, as well as test results and coverage information, associated with the build. This report also allows you to download an archive of the data, which is an artifact you can use to demonstrate compliance with OWASP during a regulatory audit.

Runs											
To group by a specific column, drag and drop the desired column to this area.											
Run Configuration Attributes						Run Information					
Run ID	Run Confi...	Setup P...	Project	Test Co...	Se	Machine	User	Run Da...	Run Type	Reports	
14	5	0	docs	OWASP Top 10 2017	\$(scontrol_branch)-win32_x86_64	JADE	annstu	2018-11-05 02:30:18	Static Analysis	XML HTML PDF	
13	5	1 [1, 0, 0]	docs	OWASP Top 10 2017	\$(scontrol_branch)-win32_x86_64	JADE	annstu	2018-11-05 02:20:41	None	XML HTML PDF	
12	5	1 [1, 0, 0]	docs	OWASP Top 10 2017	\$(scontrol_branch)-win32_x86_64	JADE	annstu	2018-11-05 02:00:16	None	XML HTML PDF	

In order to download an archive, the build has to be locked. See [Build Audit Report](#) for additional details about this report.

Profile Configuration

Models and profiles are assets that enable DTP Enterprise Pack to perform custom calculations and data processing tasks. The model defines the attributes to be used in the calculations and acts as the template for a profile. See [Working with Model Profiles](#) to learn more about models and profiles.

The OWASP Compliance artifact ships with a default model and profile for code analysis results from Parasoft dotTEST and Jtest. The model/profile assigns values to the detected weaknesses' exploitability, prevalence, and detectability. It also contains categorization information for mapping Parasoft rules to OWASP weaknesses.

PARASOFT

Extension Designer

Services | Model Profile | Configuration | Add Model | Add Profile | Import Profile | Export Profile

▶ AUTOSAR Compliance
 ▶ CERT Compliance
 ▶ CWE Compliance
 ▶ KPI
 ▶ MISRA Compliance
 ▼ OWASP Compliance

OWASP Top 10 2017 - .NET

Profile Attributes

Analysis Tool: Parasoft dotTEST 10.4.1
Revision Date: 2019-02-12

Profile Data

Weakness	Exploitability	Prevalence	Detectability
OWASP-A1	3	2	3
Weakness: OWASP-A1 Exploitability: 3 Prevalence: 2 Detectability: 3 Impact: 3 Score: 8 Description: Injection Parasoft Category ID: OWASP2017.A1 Parasoft Rule IDs: OWASP2017.A1.TDCMD,OWASP2017.A1.TDFNAMES,OWASP2017.A1.TDLDP,OWASP2017.A1.TDLDAP,OWASP2017.A1.TDLDAP			
OWASP-A2	3	2	2
OWASP-A3	2	3	2
OWASP-A4	2	2	3

The profile includes information necessary for generating compliance reports, as well as displaying data in the widgets shipped with the OWASP artifact. You can modify the profile if you want to re-categorize guidelines to meet your specific goals or specify additional metadata for your reports. Changes will be reflected in the [Weakness Detection Plan](#).

We recommend creating a copy of the default profile and modifying the copy:

1. Click **Export Profile** to download a copy.
2. Rename the copy and click **Import Profile**.
3. Browse for the copy and confirm to upload.
4. Click **Edit** and make your changes.
5. Click **Save**.

You will be able to choose an alternate profile when configuring the widgets shipped with the OWASP artifact.