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 5.4.1. Contact your Parasoft representative to download and license the Security Compliance Pack.

In this section:

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 10.4.1 or later with appropriate Security Compliance Pack licenses.
- Parasoft Jtest 10.4.x.

See Security Compliance Pack for DTP 5.4.1 for additional prerequisites information.

Process Overview

1. Analyze code using the OWASP Top 10 2017 test configuration (shipped with your code analysis tool) and report violations to DTP. The test configuration and rulemap.xml file (also shipped with the tool) configures analysis rules to report violations according to OWASP guidelines.
2. Install the Security Compliance Pack (security-compliance-<version>.zip) using Extension Designer. This enables DTP to process the code analysis data to output the compliance deliverables.
3. 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.
4. Interact with the widgets and reports to identify code that needs to be fixed to achieve your compliance goals.

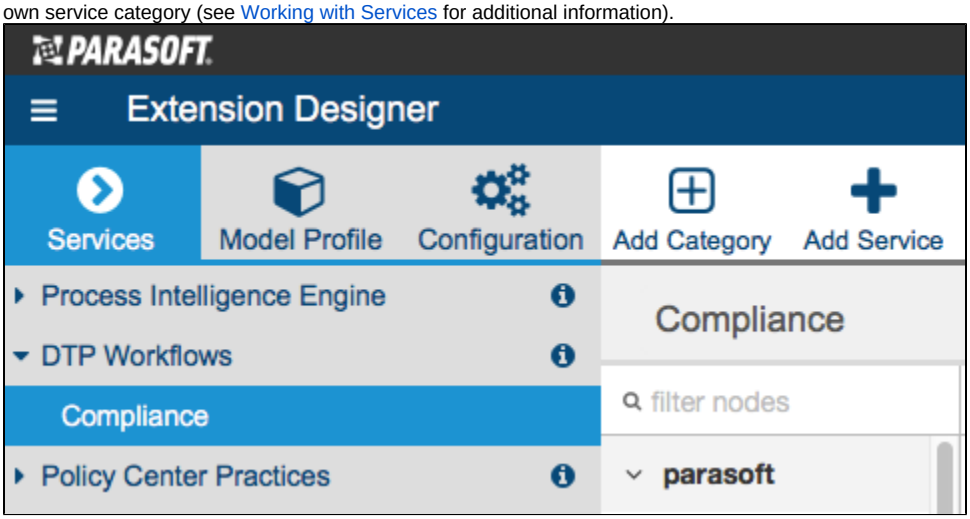
OWASP Compliance Assets

- **OWASP-Top10-dotTEST.xml:** This configuration file provides OWASP-oriented compliance categories for dotTEST code analysis results in DTP interfaces.
- **OWASP-Top10-Jtest.xml:** This configuration file provides OWASP-oriented compliance categories for Jtest code analysis results in DTP interfaces.
- **OWASP-Top10-Score-dotTEST.xml:** This configuration file provides OWASP score compliance categories for dotTEST code analysis results in DTP interfaces.
- **owaspTop10-dotTEST.json:** This file adds the OWASP Top 10 2017 dashboard template for dotTEST code analysis results. See Custom Dashboard Templates for additional information about understanding dashboards.
- **owaspTop10-Jtest.json:** This file adds the OWASP Top 10 2017 dashboard template for Jtest code analysis results.
- **owaspTop10Compliance.def.json:** This file contains the OWASP-specific widget definitions.
- **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-dottest.json:** This is the profile that assigns values for OWASP weaknesses according to the standard.
- **owasp-compliance.model.json:** This file is defines the model type for the owasp-top10-dottest.json profile. See Working with Model Profiles for additional information about models and profiles.

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).



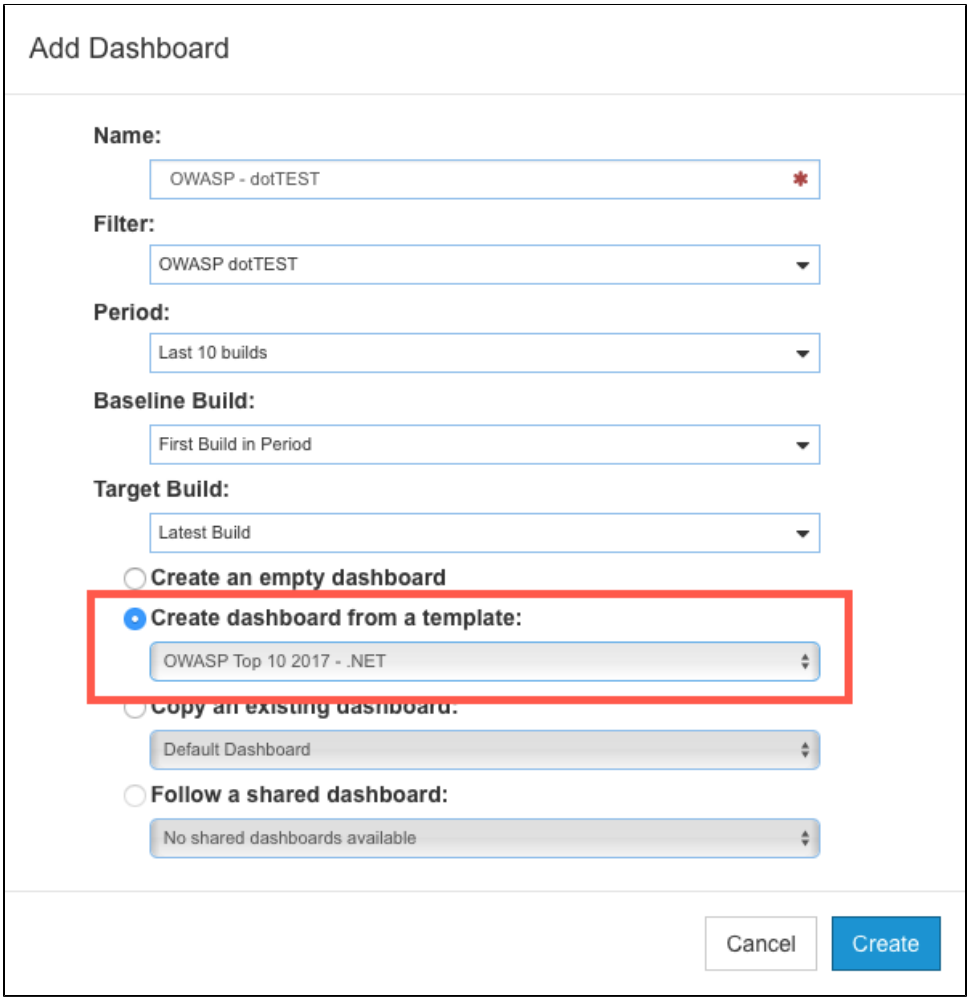
3. You can deploy the artifact to an existing service or add a new service. The number of artifacts deployed to a service affects the overall performance. See Extension Designer Best Practices for additional information. Choose an existing service and continue to step 5 or click **Add Service**.
4. Specify 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 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

OWASP dashboard templates will be added for dotTEST and Jtest code analysis results after installing the Security Compliance Pack. 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.



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

The dashboard template for Jtest code analysis results differs from the dotTEST dashboard template. See Jtest Dashboard and dotTEST Dashboard for information about the widgets displayed in each dashboard.

Jtest Dashboard

The Jtest dashboard template contains native DTP widgets that have been reoriented to OWASP-specific compliance categories per the OWASP-Top10-Jtest.xml file (see OWASP Compliance Assets).

OWASP Top 10 2017 - Compliance Widget

This widget provides a comprehensive overview of the project's compliance with OWASP Top 10 2017 guidelines. It shows the number of OWASP-specific rules that were enabled and passed, as well as how many violations were reported for applicable severity levels. If no violations were reported for a specific severity level, a column will not render for that level. See Compliance by Category/Severity for additional information about this widget, including linked reports.

OWASP Top 10 2017 - Compliance

Compliance Category	Passed / # of Rules	Severity Level 1	2	3	5
A1:2017-Injection	2/4	2/4	0/0	0/0	0/0
A2:2017-Broken Authentication	1/1	1/1	0/0	0/0	0/0
A3:2017-Sensitive Data Exposure	8/13	4/8	2/2	1/2	1/1
A4:2017-XML External Entities (XXE)	0/0	0/0	0/0	0/0	0/0
A5:2017-Broken Access Control	2/3	1/2	0/0	1/1	0/0
A6:2017-Security Misconfiguration	8/12	2/2	1/1	5/9	0/0
A7:2017-Cross-Site Scripting (XSS)	2/3	2/3	0/0	0/0	0/0
A8:2017-Insecure Deserialization	3/3	0/0	0/0	3/3	0/0
A9:2017-Using Components with Known Vulnerabilities	0/0	0/0	0/0	0/0	0/0
A10:2017-Insufficient Logging&Monitoring	1/1	0/0	0/0	1/1	0/0

Rules in Compliance

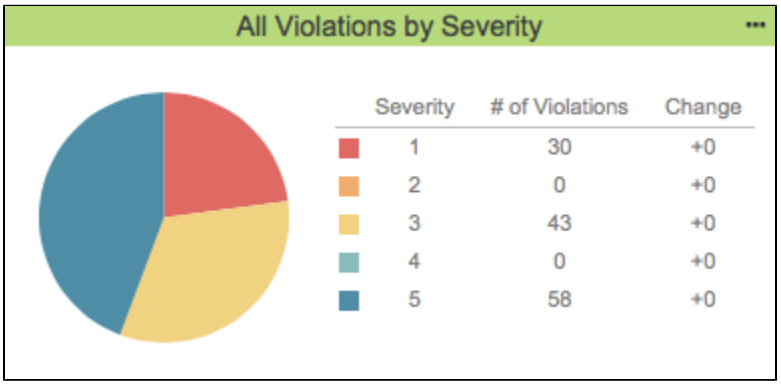
This widget is an implementation of the native DTP Rules in Compliance widget. It shows the percentage of Parasoft rules that are mapped to OWASP weaknesses that are not reporting a violation (are in compliance). See Rules in Compliance - Summary for details about the widget, including linked reports.

Violations - Summary Trend

This widget is an implementation of the native Violations - Summary Trend widget. It shows the number of violations in the build currently set as the target build (latest build by default). The trend line is intended to provide an at-a-glance approximation of whether the violations are increasing or decreasing. See Violations - Summary Trend for details about the widget.

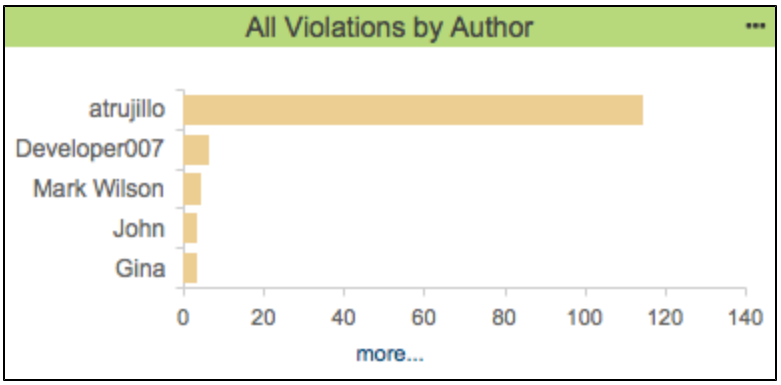
Severities - Pie

The dashboard include the standard Severities - Pie widget, which shows the distribution of violations across Parasoft severity. See Severities - Pie for details about the widget.



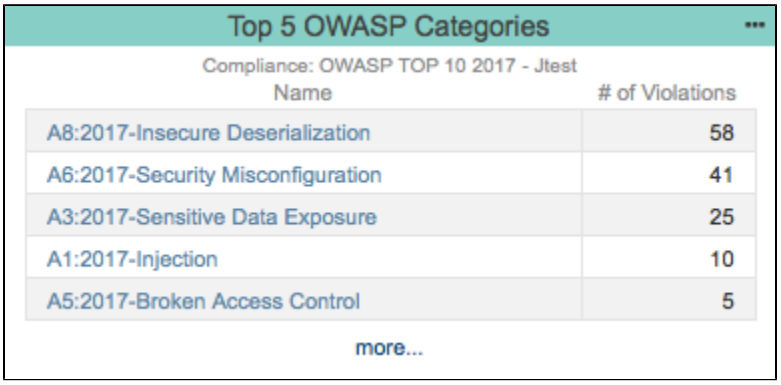
Authors - Top 5 Bar

The dashboard includes an instance of the standard Assignees - Top 5 Bar widget, which shows the distribution of violations across code authors. See Authors - Top 5 Bar for details about the widget.



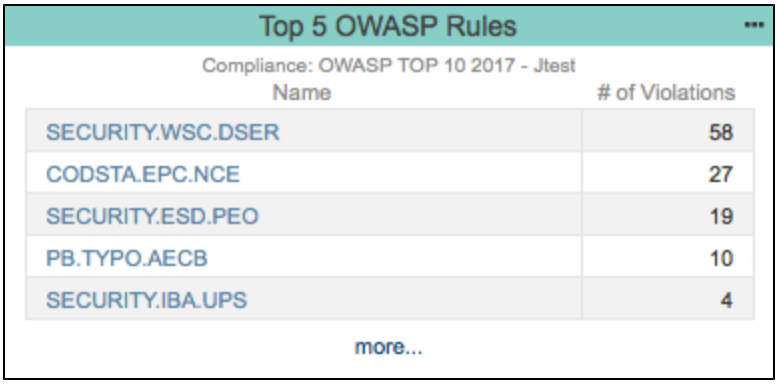
Categories - Top 5 Table

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.



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.

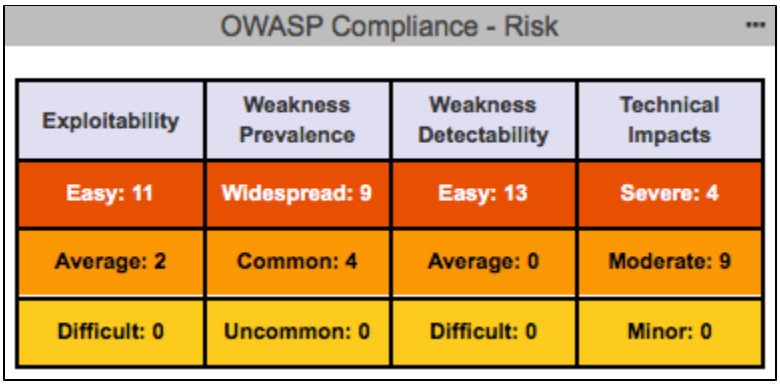


dotTEST Dashboard

The dotTEST 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-dotTEST.xml file (see OWASP Compliance Assets).

OWASP Compliance Risk

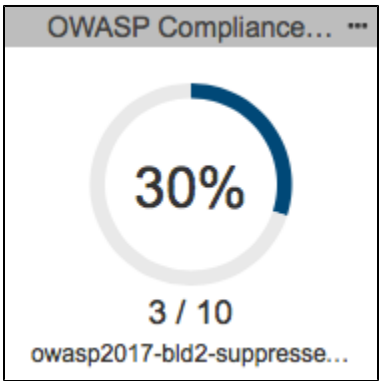
This widget is included with the OWASP Compliance artifact. It provides a chart showing the distribution of violations according to its risk as defined in the OWASP standard.



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:

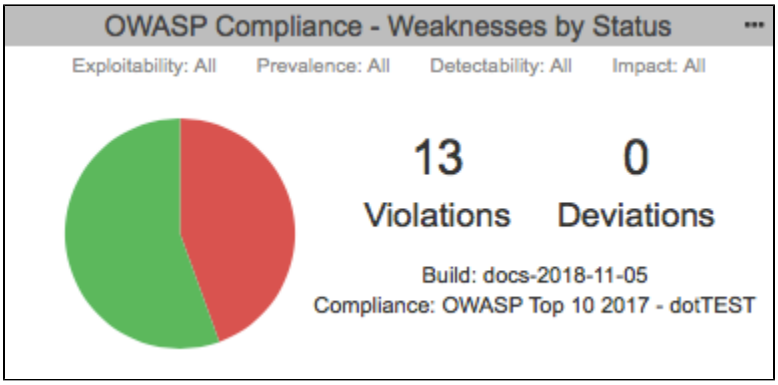
- **No rules enabled**: Code analysis has not been reported to DTP or the OWASP Top 10 test configuration was not executed by dotTEST.

- **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 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.

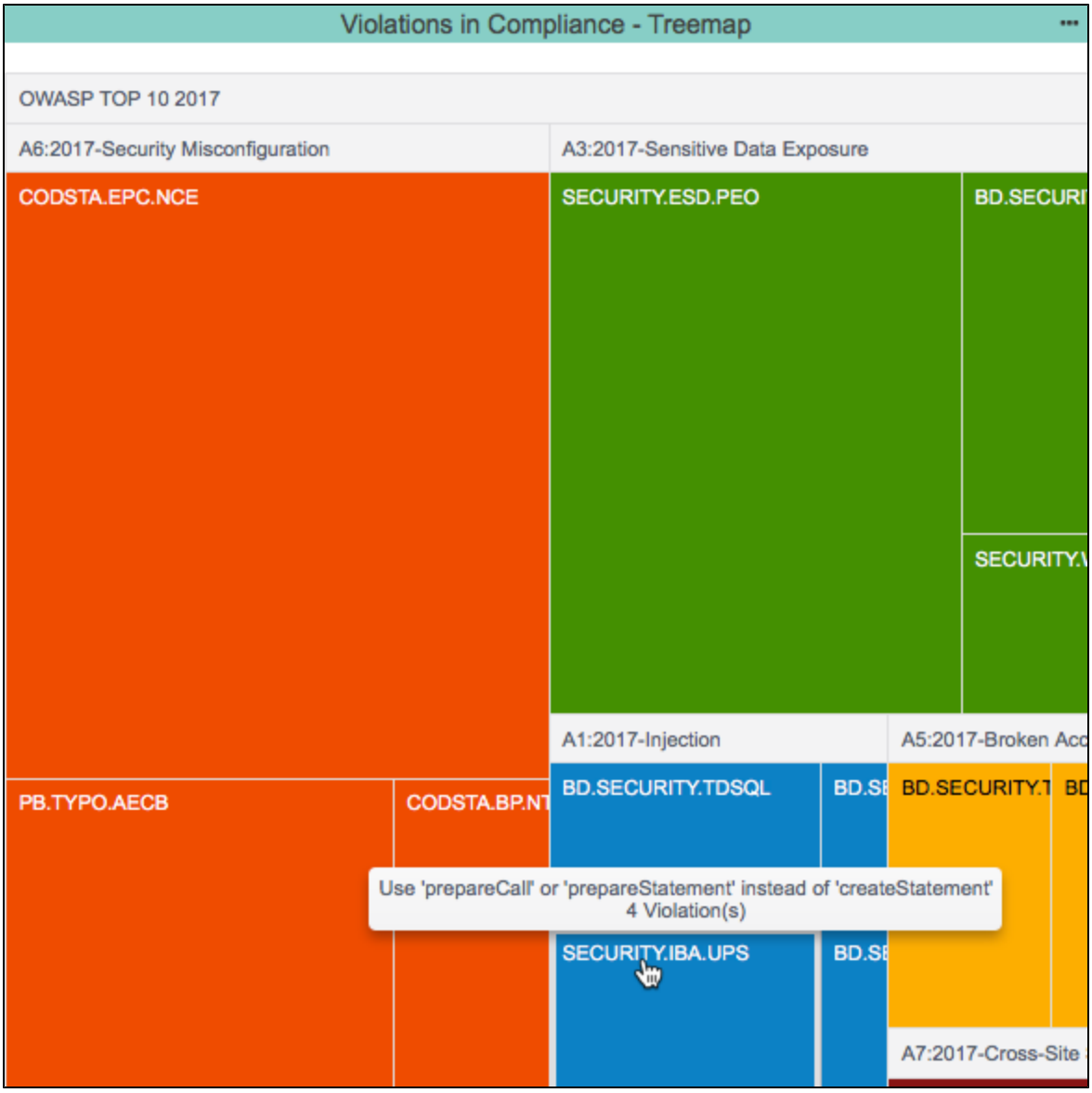


You can perform the following actions:

- 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.

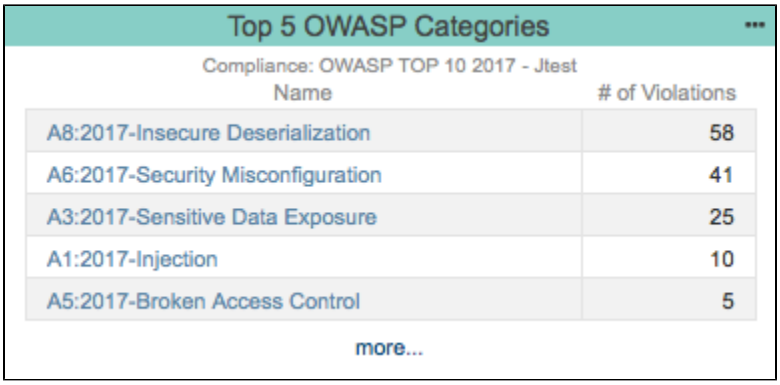


Rules in Compliance

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.

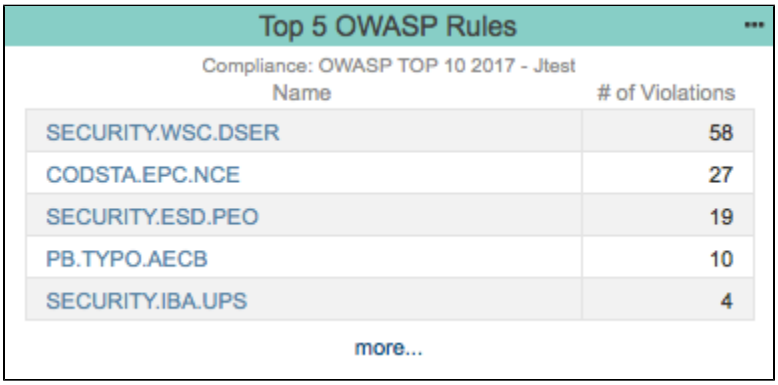
Categories - Top 5 Table

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.



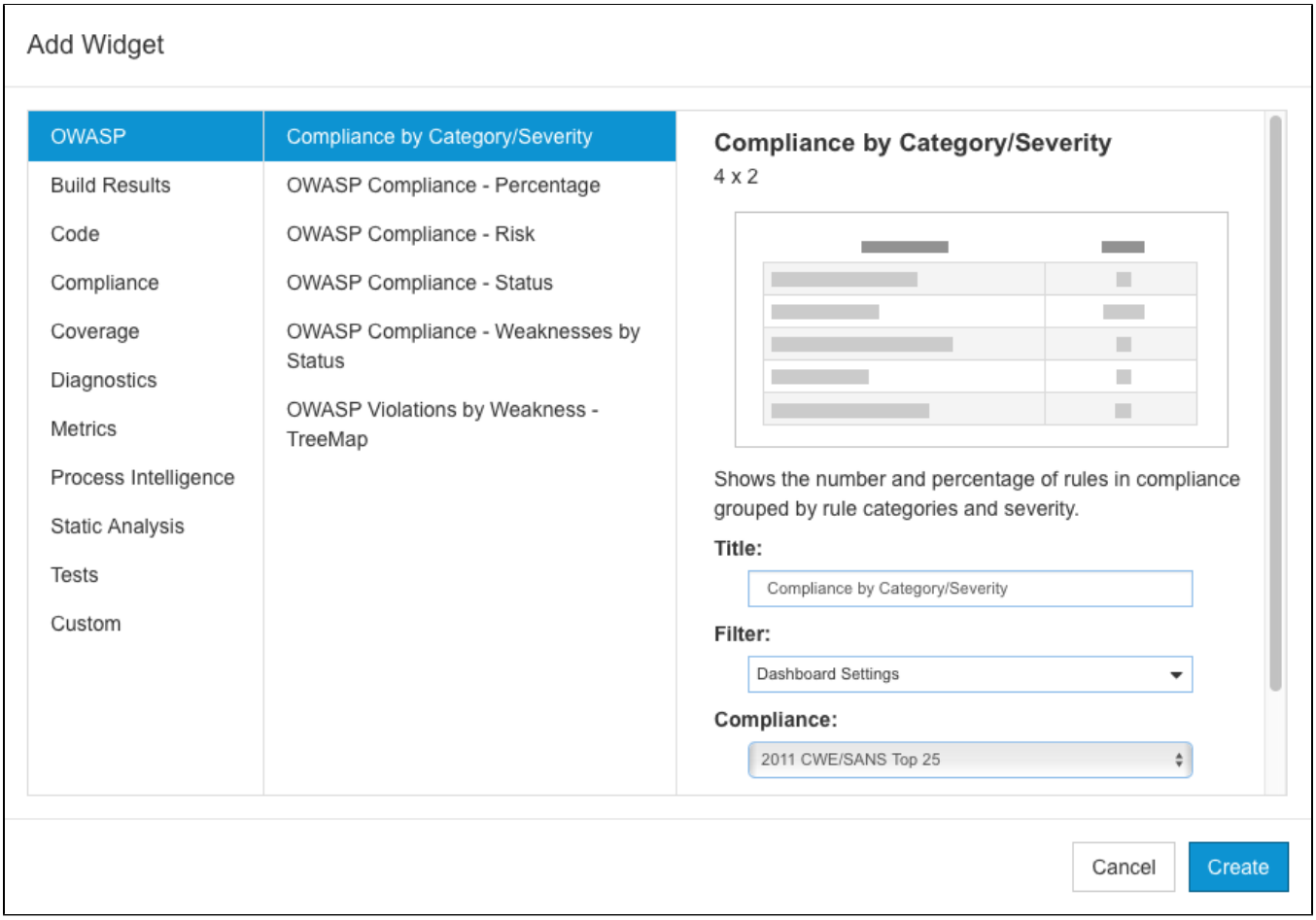
Rules - Top 5 Table

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.



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:

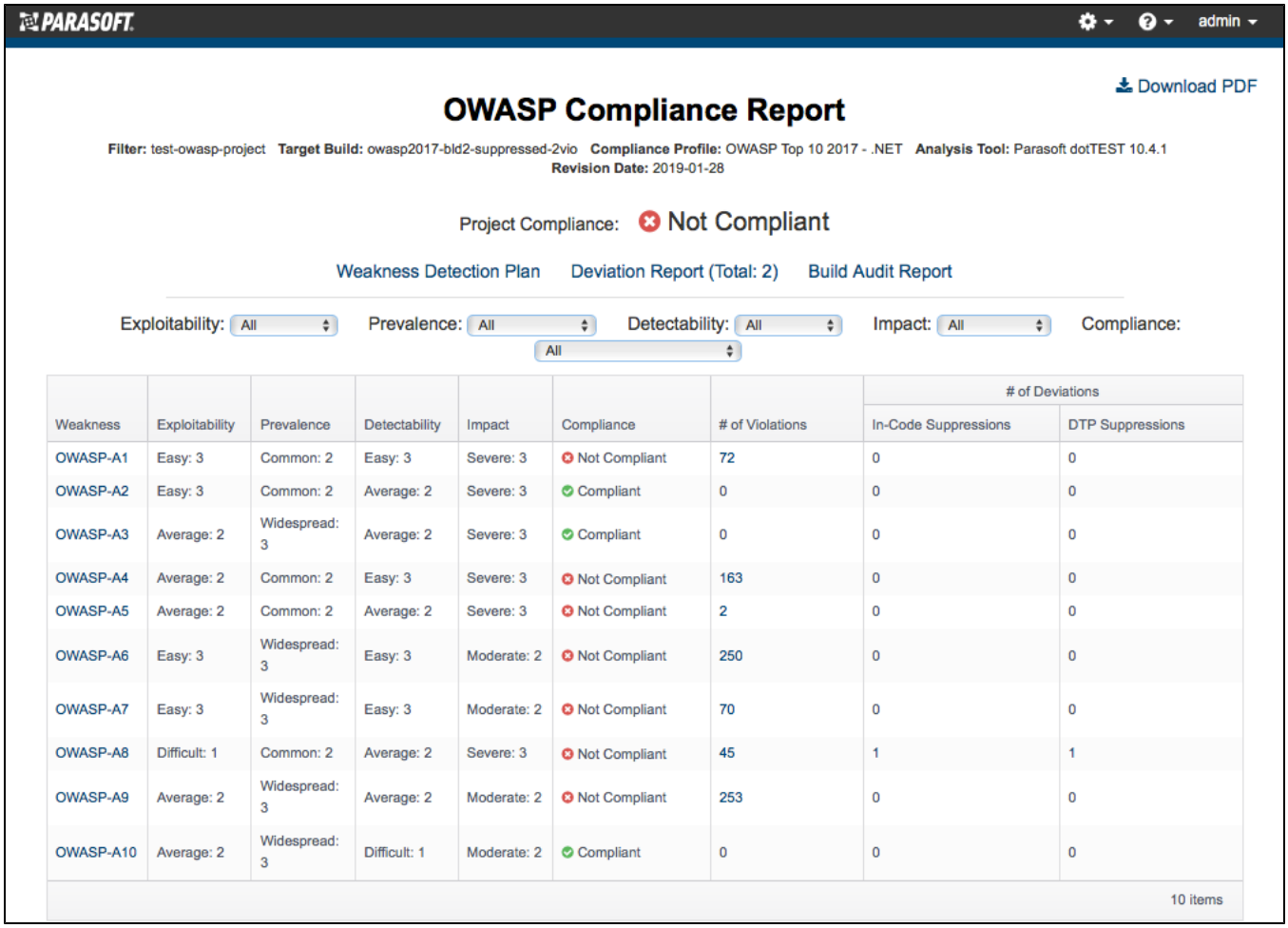


The following configurations are available:

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.

Viewing the OWASP Compliance Report

All reports are only available for compliance data associated with dotTEST code analysis. The main OWASP compliance report provides details about your OWASP compliance status and serves as the primary document for demonstrating compliance.



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.

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.TDLDAP 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 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

User: admin
Date: 2018-11-20 12:06:32 PM

Field: Suppression Author
Old Value: N/A
New Value: admin

Field: Suppression Date
Old Value: N/A
New Value: 2018-11-20T12:06:32.265

Field: Suppression Reason
Old Value: N/A
New Value: Example suppression

OWASP-A2 Broken Authentication ✔ - No Deviations

OWASP-A3 Sensitive Data Exposure ✔ - No Deviations

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

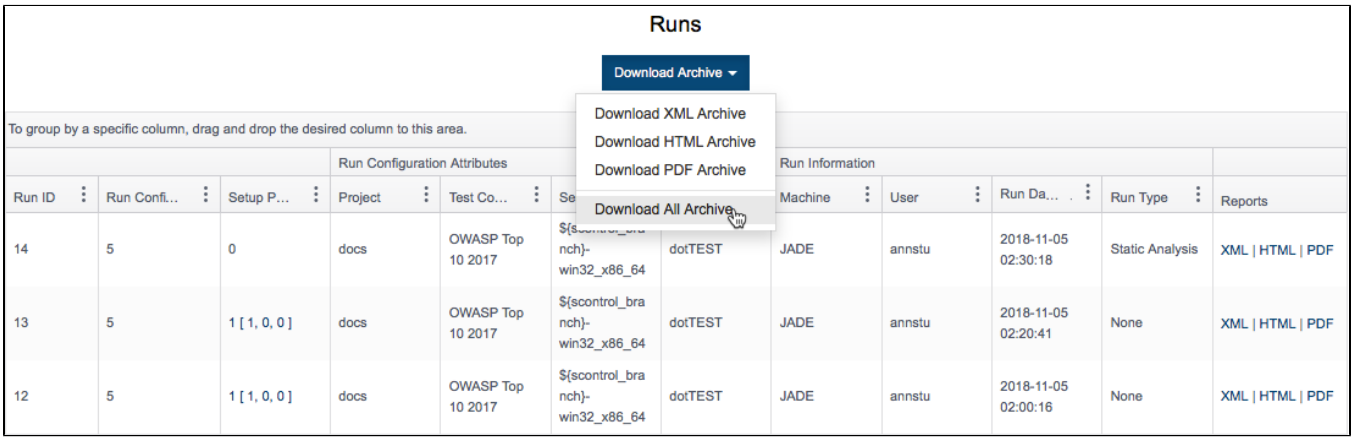
OWASP-A5 Broken Access Control ✔ - No Deviations

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.



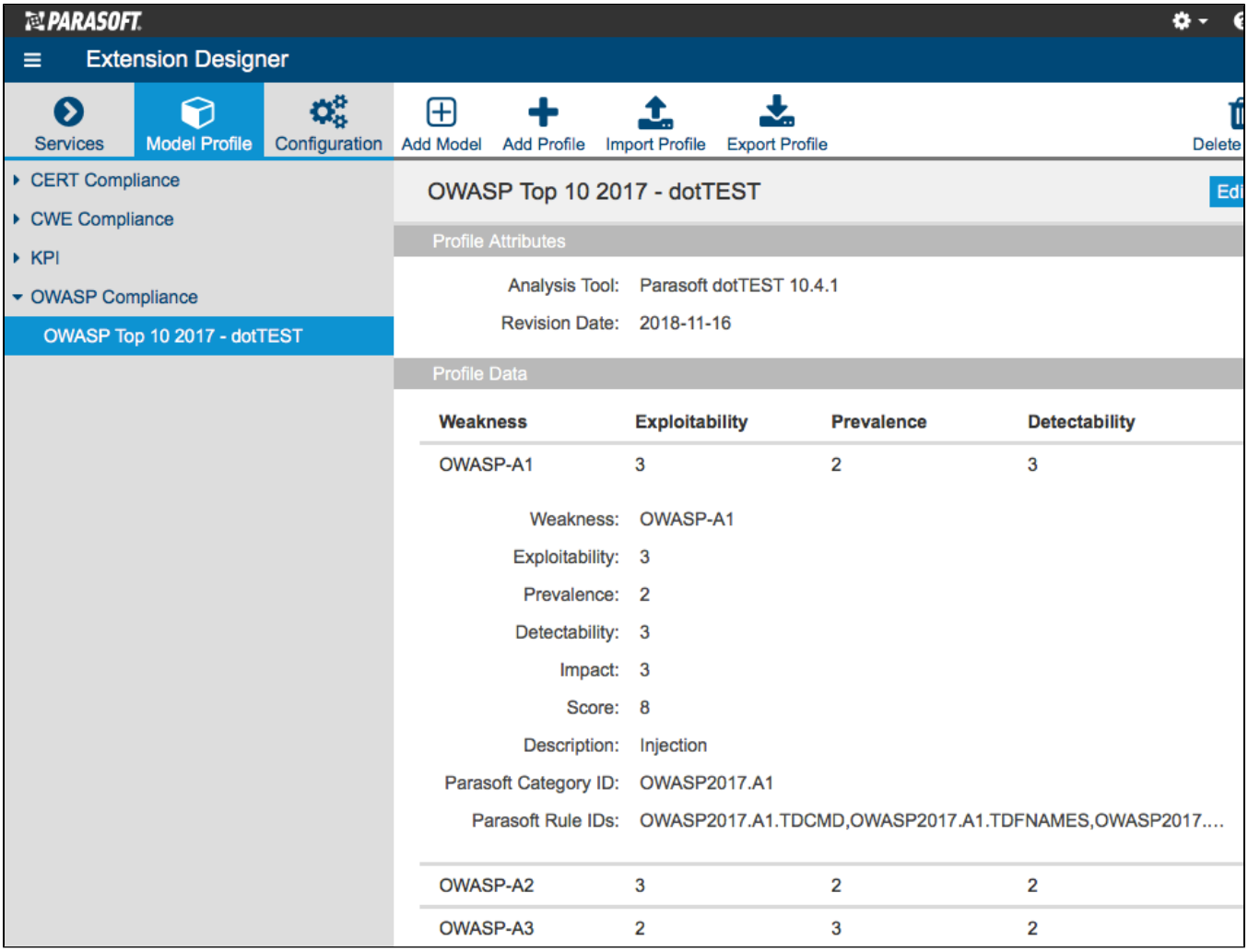
In order to download an archive, the build has to be locked. See Build Audit Report for additional details about this report.

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. 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.

The model profile only applies to data associated with dotTEST code analysis.



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.