PCI DSS Compliance

In this section:

Introduction

The Parasoft PCI DSS Compliance artifact is a set of assets for your DTP infrastructure that enable you to demonstrate compliance with PCI DSS coding requirements. The artifact is shipped as part of the Security Compliance Pack. Contact your Parasoft representative to download and license the Security Compliance Pack.

About PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is a collection of coding requirements for software that processes payment card transactions. The standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. Refer to the the PCI Security Standards Council website for details about the standard: https://www.pcisecuritystandards.org.

Parasoft facilitates PCI DSS standards by re-orienting code analysis checkers to report violations within the context of PCI DSS requirements. Each code analysis checker maps to one or more requirement, which appear in DTP widgets and reports.

Prerequisites

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

- Parasoft dotTEST 2020.1 or later with appropriate Security Compliance Pack licenses.
- Parasoft Jtest 2020.1 or later with appropriate Security Compliance Pack licenses.

See Security Compliance Pack for additional prerequisites information.

Process Overview

1. Install the Security Compliance Pack into DTP Extension Designer.
2. Deploy the PCI DSS Compliance artifact into your DTP environment. This also deploys the PCI DSS Compliance Assets.
3. Analyze code using the PCI DSS 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 PCI DSS Compliance dashboard and widgets to your DTP interface. The dashboard widgets and shows the reported violations within the context of PCI DSS guidelines.
5. Interact with the widgets and reports to identify code that needs to be fixed to achieve your compliance goals.

PCI DSS Compliance Assets

The following artifacts are included in the package and added to your DTP environment when you install the Security Compliance Pack.

PCI DSS 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.

Dashboard Templates

Dashboard templates include preconfigured widgets to help you quickly view specific information about your projects. Refer the Dashboards section to learn more about dashboards in DTP. See Adding the PCI DSS Dashboards for details about viewing the widgets that appear in the dashboard templates.

- PCI-DSS-dotNET.json
- PCI-DSS-Java.json

Compliance Categories

Individual code analysis rules belong to a category, such as Security, Exceptions, etc. The PCI DSS Compliance artifact includes files that map code analysis rules to PCI DSS-specific categories. You can configure widgets to report violations according to the categories defined in the following files to view them according to their PCI DSS category:

- PCI-DSS-dotNET.xml
- PCI-DSS-Java.xml

Models and Profiles

Profiles provide a range of functions in a DTP infrastructure, such as providing inputs for custom calculations executed by an extension and providing data for compliance reports. Profiles take their structure from models, which define fields, headers, or other components used in the profile. See Working with Model Profiles for information about understanding profiles in DTP Enterprise Pack.

The following profile files are included with the artifact:

- pci-dss-java.json
- pci-dss-dotnet.json
- pci-dss-compliance.model.json

Cross-reference PDFs

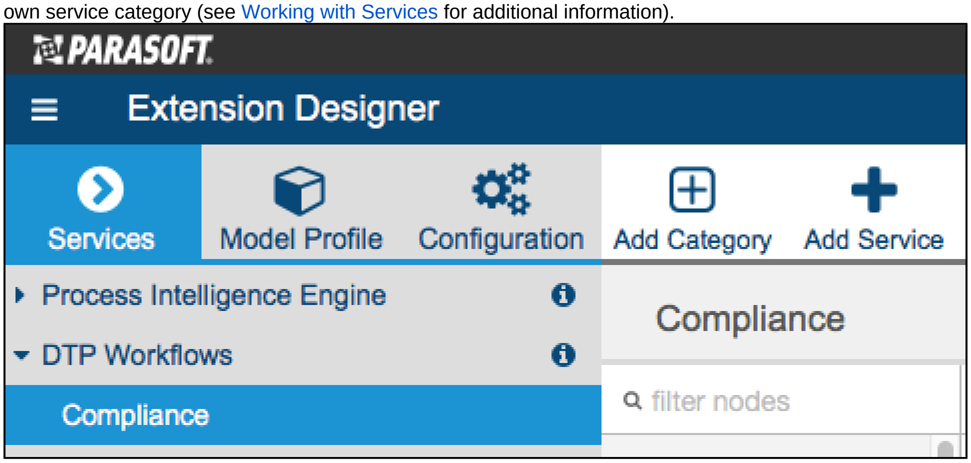
For your convenience, PDFs that show the association between Parasoft rules and PCI DSS requirements are located in the <PACK>/rules/jtest and <PACK>/rules/dottest directories:

- PCI_DSS_3.2.pdf

Deploying the PCI DSS Compliance Assets

The PCI DSS Compliance assets are installed as part of the Security Compliance Pack installation (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).



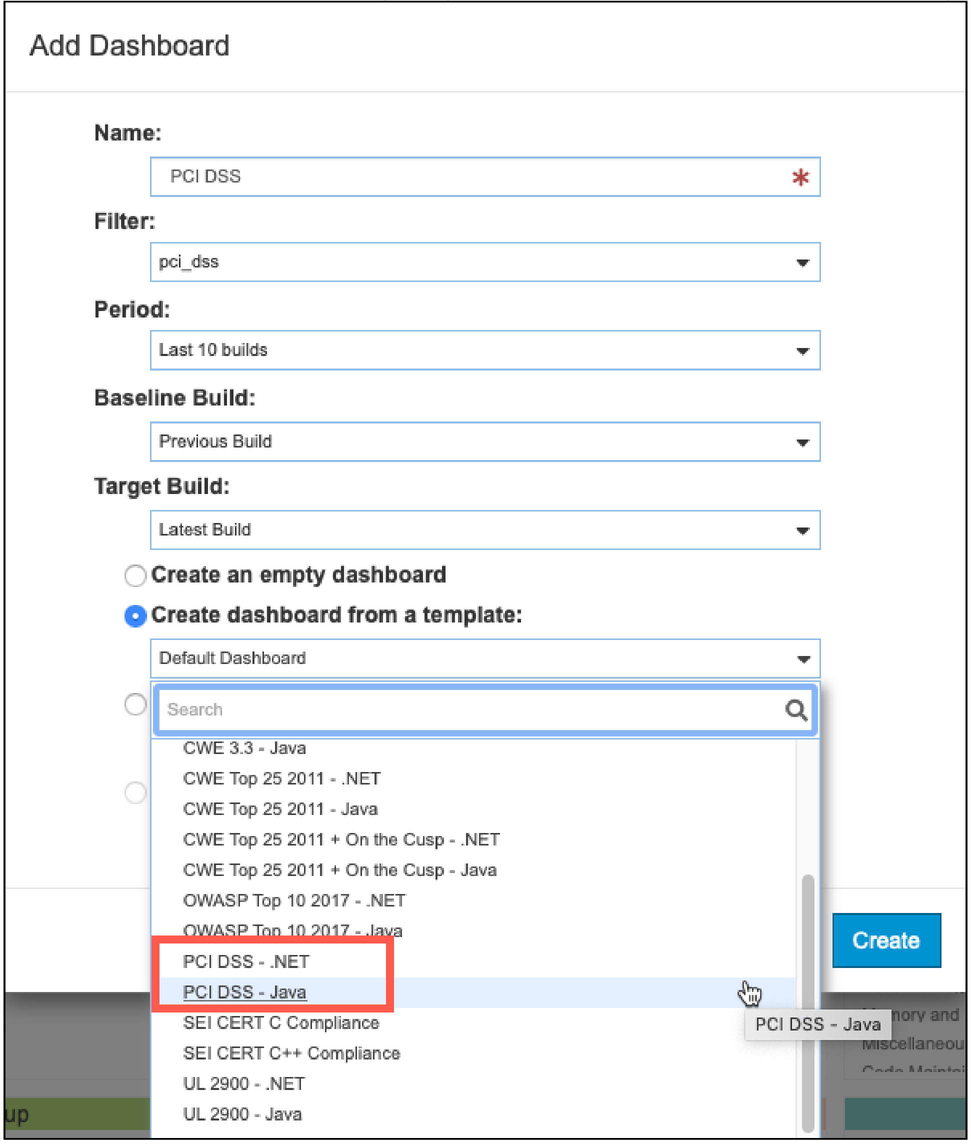
3. You can deploy the artifact to an existing service or add a new service. The number of artifacts deployed to a service affects the overall performance. See Extension Designer Best Practices for additional information. Choose an existing service and continue to step 5 or click **Add Service**.
4. Specify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

Adding the PCI DSS Dashboards

The PCI DSS dashboard templates for Java and .NET enable you to quickly add a set of preconfigured widgets that monitor PCI DSS compliance. See Dashboard Templates for a list of the templates included with the artifact.

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 PCI DSS - .NET or Java template from the drop-down menu.



Add Dashboard

Name: PCI DSS *

Filter: pci_dss

Period: Last 10 builds

Baseline Build: Previous Build

Target Build: Latest Build

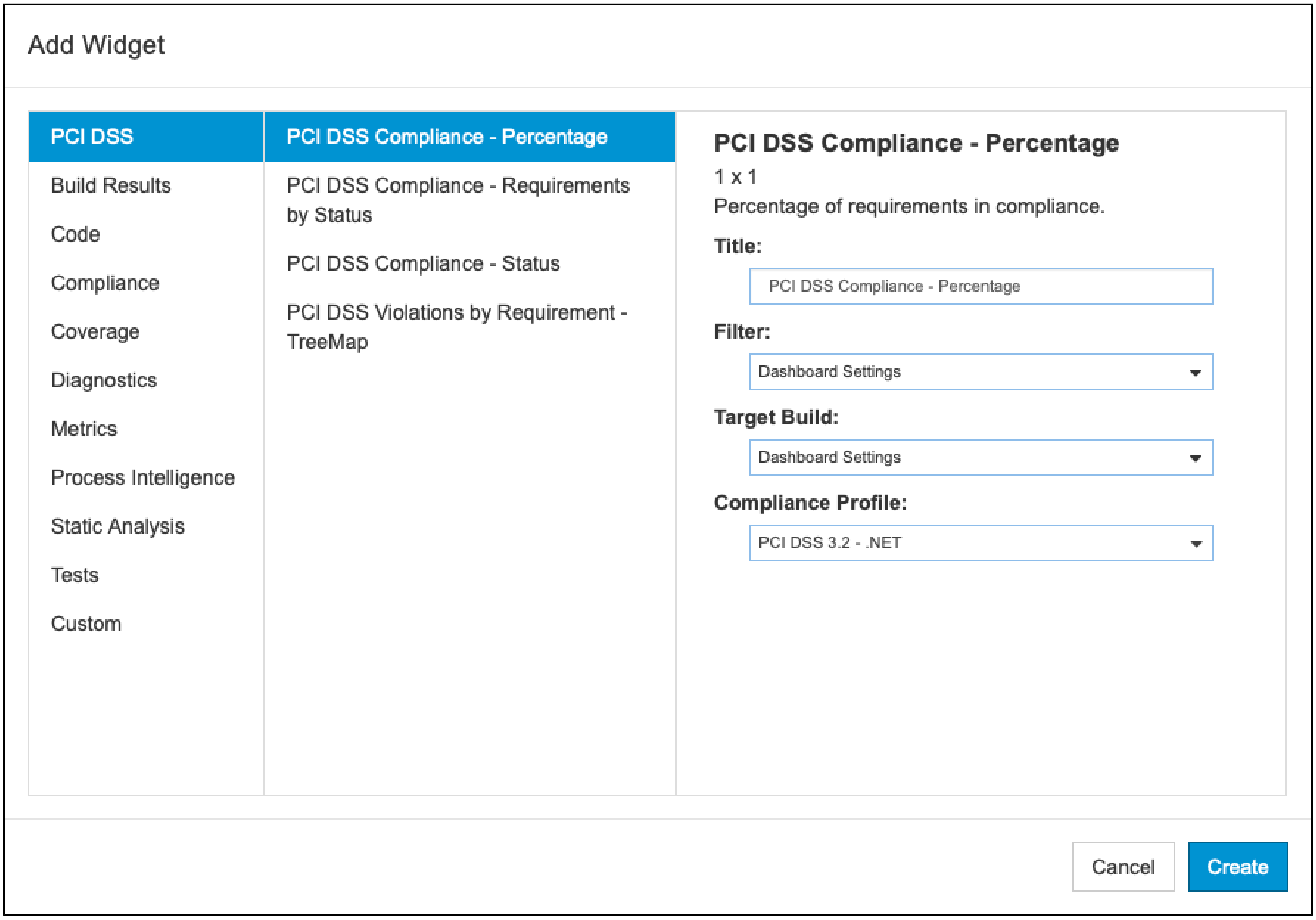
○ Create an empty dashboard

● Create dashboard from a template: Default Dashboard

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

Manually Adding PCI DSS Widgets to an Existing Dashboard

You can add the PCI DSS 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 PCI DSS widgets will appear in the PCI DSS category in the Add Widget overlay:


Add Widget
PCI DSS
Build Results
Code
Compliance
Coverage
Diagnostics
Metrics
Process Intelligence
Static Analysis
Tests
Custom
PCI DSS Compliance - Percentage
PCI DSS Compliance - Requirements by Status
PCI DSS Compliance - Status
PCI DSS Violations by Requirement - TreeMap
Cancel
Create

PCI DSS Compliance - Percentage

1 x 1

Percentage of requirements in compliance.

Title: PCI DSS Compliance - Percentage

Filter: Dashboard Settings

Target Build: Dashboard Settings

Compliance Profile: PCI DSS 3.2 - .NET

The following configurations are available:

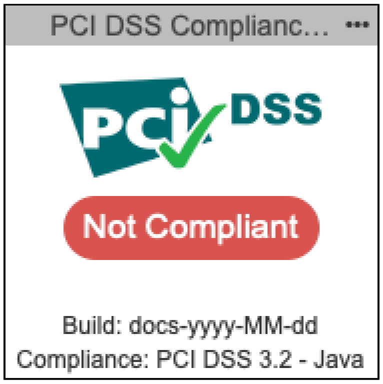
Title	Enter a new title to replace the default title that appears on the dashboard.
Filter	Choose a specific filter or Dashboard Settings from the drop-down menu. See Creating and Managing Filters for additional information.
Target Build	Choose a specific build from the drop-down menu. The build selected 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.

PCI DSS Compliance Widgets

See Dashboard Templates for a list of the dashboard templates shipped with the compliance artifact. The following widgets are included on one or more the dashboards:

PCI DSS Compliance Status

This widget shows the current state of compliance with PCI DSS.



Build: docs-yyyy-MM-dd
Compliance: PCI DSS 3.2 - Java

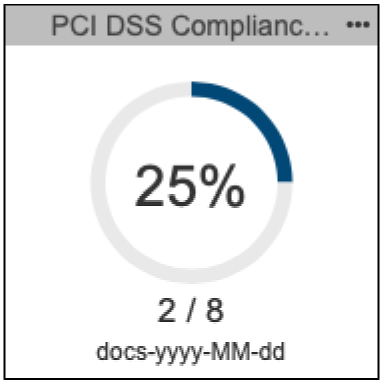
There are seven possible states:

- **No rules enabled**: Code analysis has not been reported to DTP or the test configuration was not executed.
- **N/A:** The assets have not been deployed to a service or the service is not running. See Deploying the PCI DSS 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 PCI DSS Compliance Report.

PCI DSS Compliance Percentage

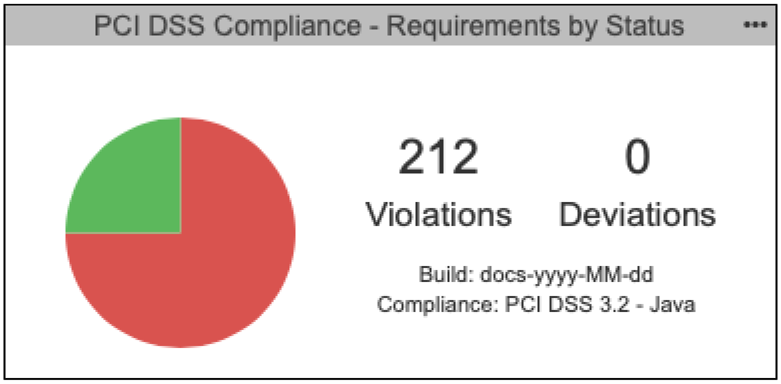
This widget shows the percentage of the code that is in compliance with PCI DSS guidelines. Click on the widget to open the PCI DSS Compliance Report.



docs-yyyy-MM-dd

PCI DSS Compliance - Requirements by Status

This widget shows represents the PCI DSS requirements as a pie chart. The red segment represents the requirements that the analyzed code is not currently complying with. The green segment represents the requirements that the analyzed code is currently complying with. The widget also shows the number of violations and deviations.



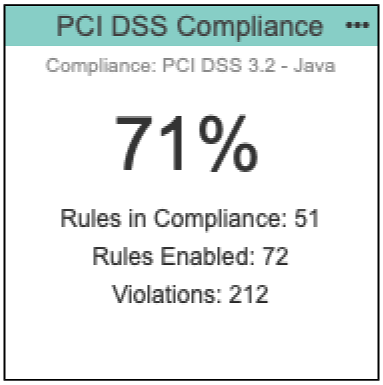
Build: docs-yyyy-MM-dd
Compliance: PCI DSS 3.2 - Java

You can perform the following actions:

- Click on a segment in the pie chart to open the PCI DSS Compliance Report filtered by the selected status.
- Click on the Violations section to open an unfiltered PCI DSS Compliance Report.
- Click on the Deviations section to open the Deviations Report.

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 PCI DSS requirements that are not reporting a violation (are in compliance). See Rules in Compliance - Summary for details about the widget.



PCI DSS Compliance

Compliance: PCI DSS 3.2 - Java

71%

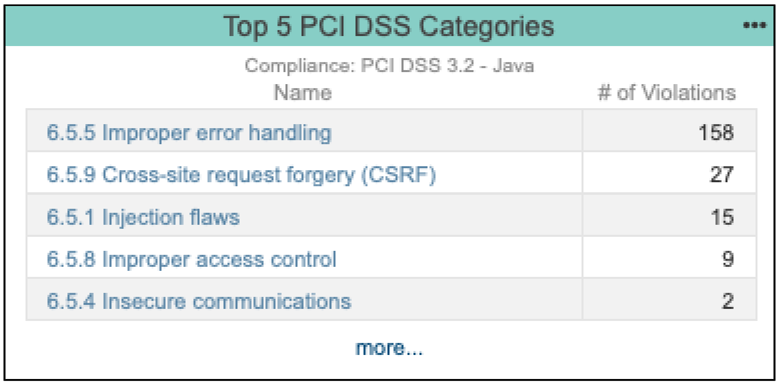
Rules in Compliance: 51

Rules Enabled: 72

Violations: 212

Categories - Top 5 Table

The dashboard includes an instance of the native Categories - Top 5 Table widget configured for PCI DSS. It shows the five PCI DSS categories with the most violations. See Categories - Top 5 Table for details about the widget.



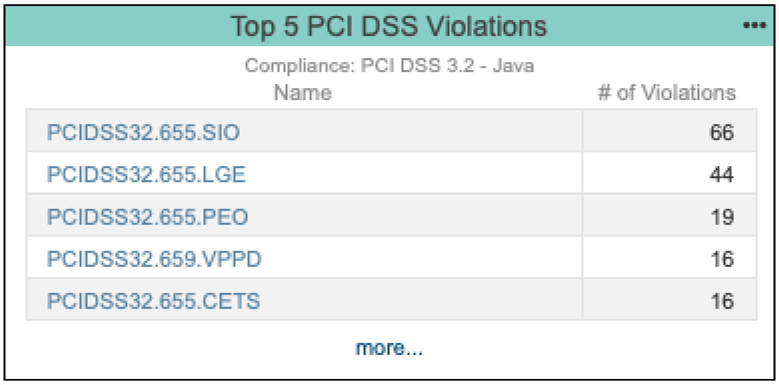
Top 5 PCI DSS Categories

Compliance: PCI DSS 3.2 - Java

Name	# of Violations
6.5.5 Improper error handling	158
6.5.9 Cross-site request forgery (CSRF)	27
6.5.1 Injection flaws	15
6.5.8 Improper access control	9
6.5.4 Insecure communications	2

Rules - Top 5 Table

The dashboard includes an instance of the native Rules - Top 5 Table widget configured for PCI DSS. It shows the five Parasoft rules mapped to PCI DSS categories with the most violations. See Rules - Top 5 Table for details about the widget.



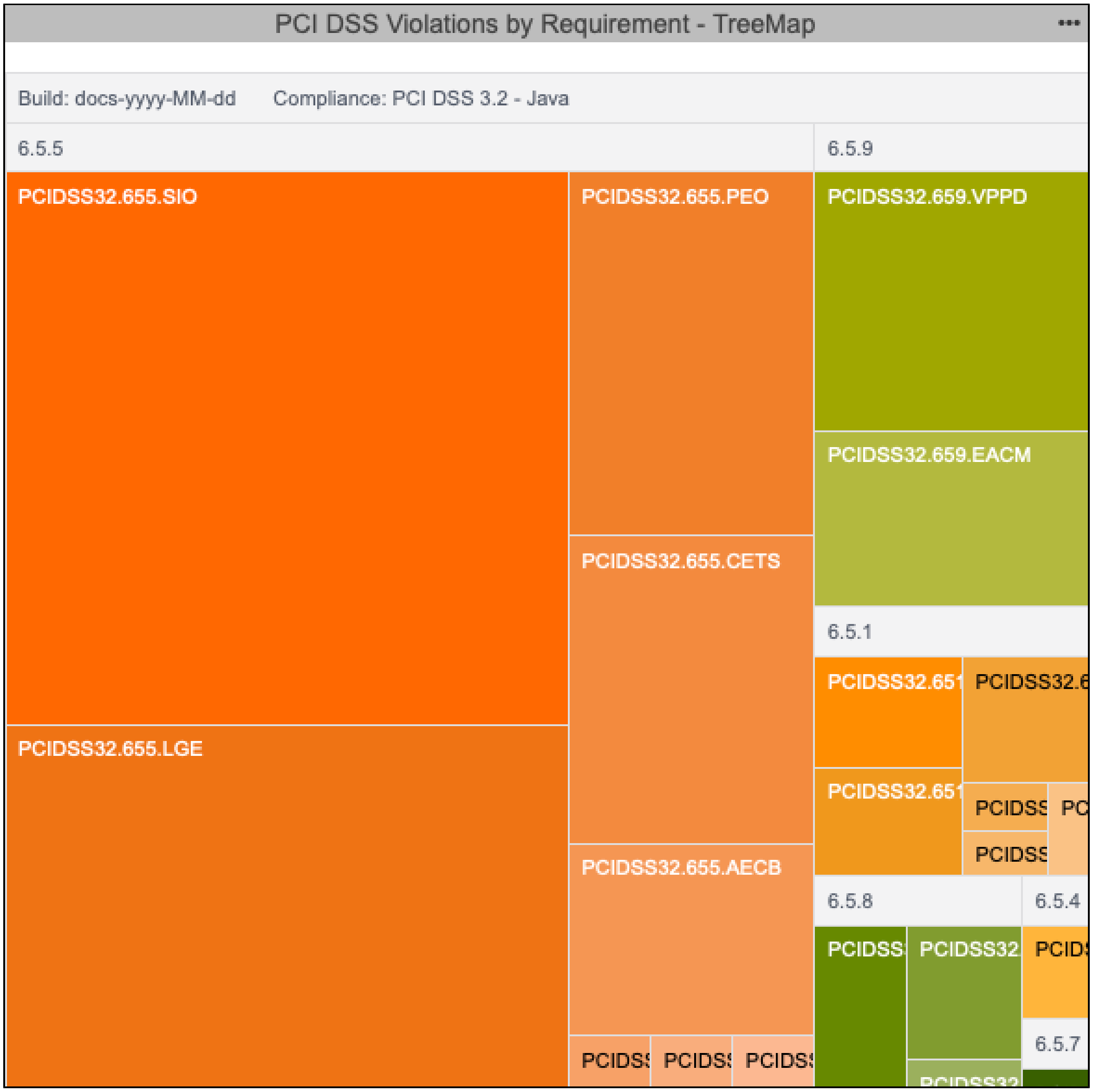
Top 5 PCI DSS Violations

Compliance: PCI DSS 3.2 - Java

Name	# of Violations
PCIDSS32.655.SIO	66
PCIDSS32.655.LGE	44
PCIDSS32.655.PEO	19
PCIDSS32.659.VPPD	16
PCIDSS32.655.CETS	16

Violations by Requirement - Treemap

This widget shows the violations grouped by PCI DSS requirement in a tree map. Each tile is assigned a color and represents a requirement from the guidelines. See Configuring Security Compliance Pack Widgets for details on how to configure this widget.

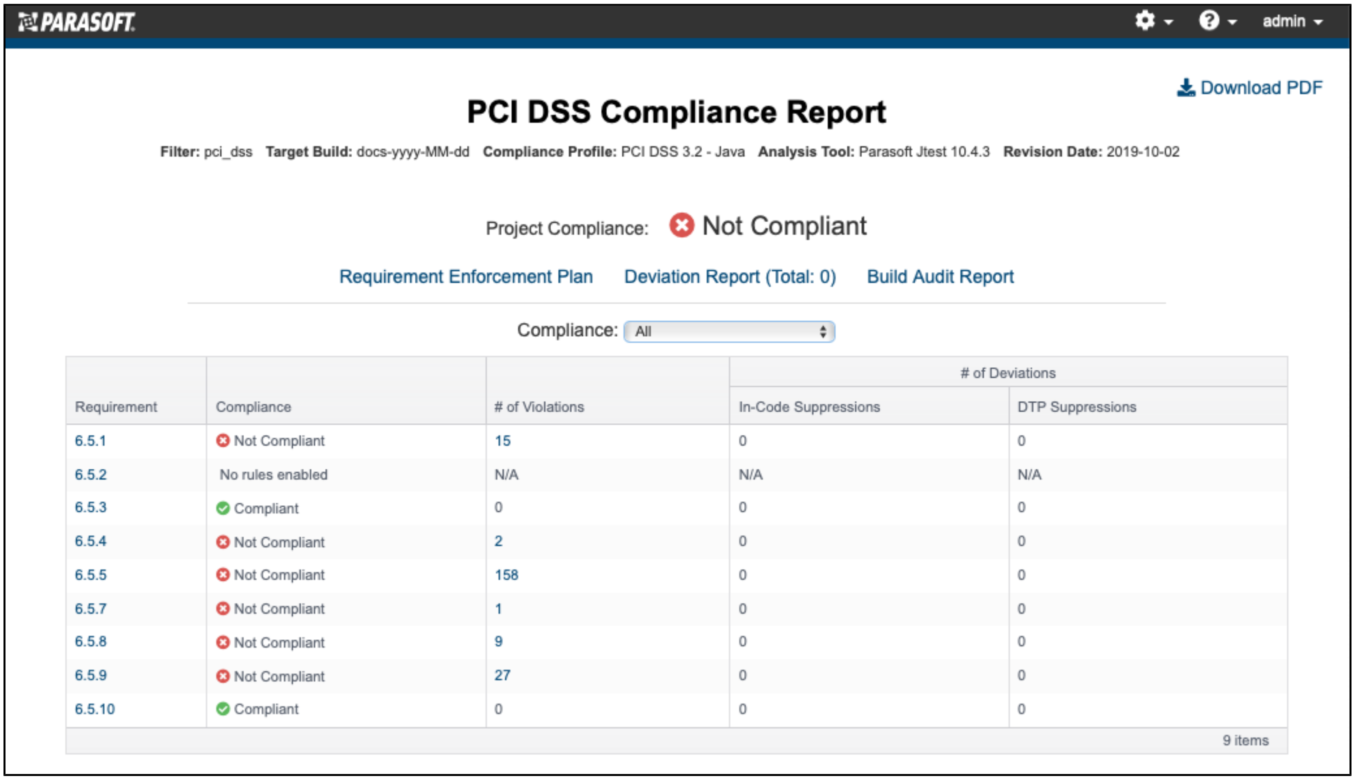


PCI DSS Violations by Requirement - TreeMap

Build: docs-yyyy-MM-dd Compliance: PCI DSS 3.2 - Java

Viewing the PCI DSS Compliance Report

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



PCI DSS Compliance Report

Filter: pci_dss **Target Build:** docs-yyyy-MM-dd **Compliance Profile:** PCI DSS 3.2 - Java **Analysis Tool:** Parasoft Jtest 10.4.3 **Revision Date:** 2019-10-02

Project Compliance: ✖ Not Compliant

Requirement Enforcement Plan   Deviation Report (Total: 0)   Build Audit Report

Compliance: All

			# of Deviations	
Requirement	Compliance	# of Violations	In-Code Suppressions	DTP Suppressions
6.5.1	✖ Not Compliant	15	0	0
6.5.2	No rules enabled	N/A	N/A	N/A
6.5.3	✓ Compliant	0	0	0
6.5.4	✖ Not Compliant	2	0	0
6.5.5	✖ Not Compliant	158	0	0
6.5.7	✖ Not Compliant	1	0	0
6.5.8	✖ Not Compliant	9	0	0
6.5.9	✖ Not Compliant	27	0	0
6.5.10	✓ Compliant	0	0	0

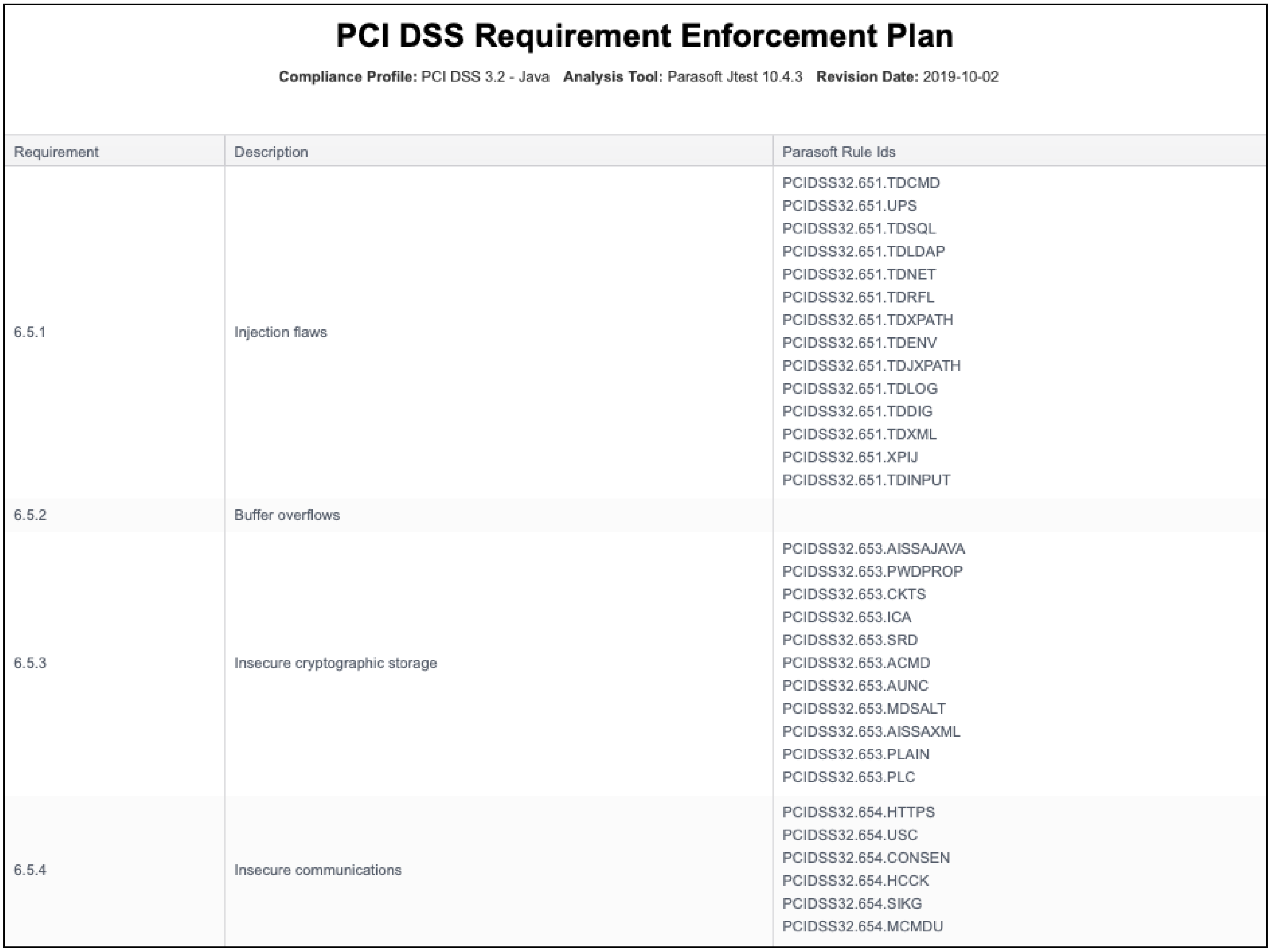
9 items

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 Requirement column to open the Requirement Enforcement Plan. The link goes directly to the specific requirement so that you can review the Parasoft code analysis rule or rules detecting the weaknesses.
- Open one of the sub-reports (Requirement Enforcement 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.

Requirement Enforcement Plan

The Requirement Enforcement Plan shows which static analysis rules are used to enforce the PCI DSS requirements. It is intended to describe how you are enforcing each requirement. 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.



PCI DSS Requirement Enforcement Plan

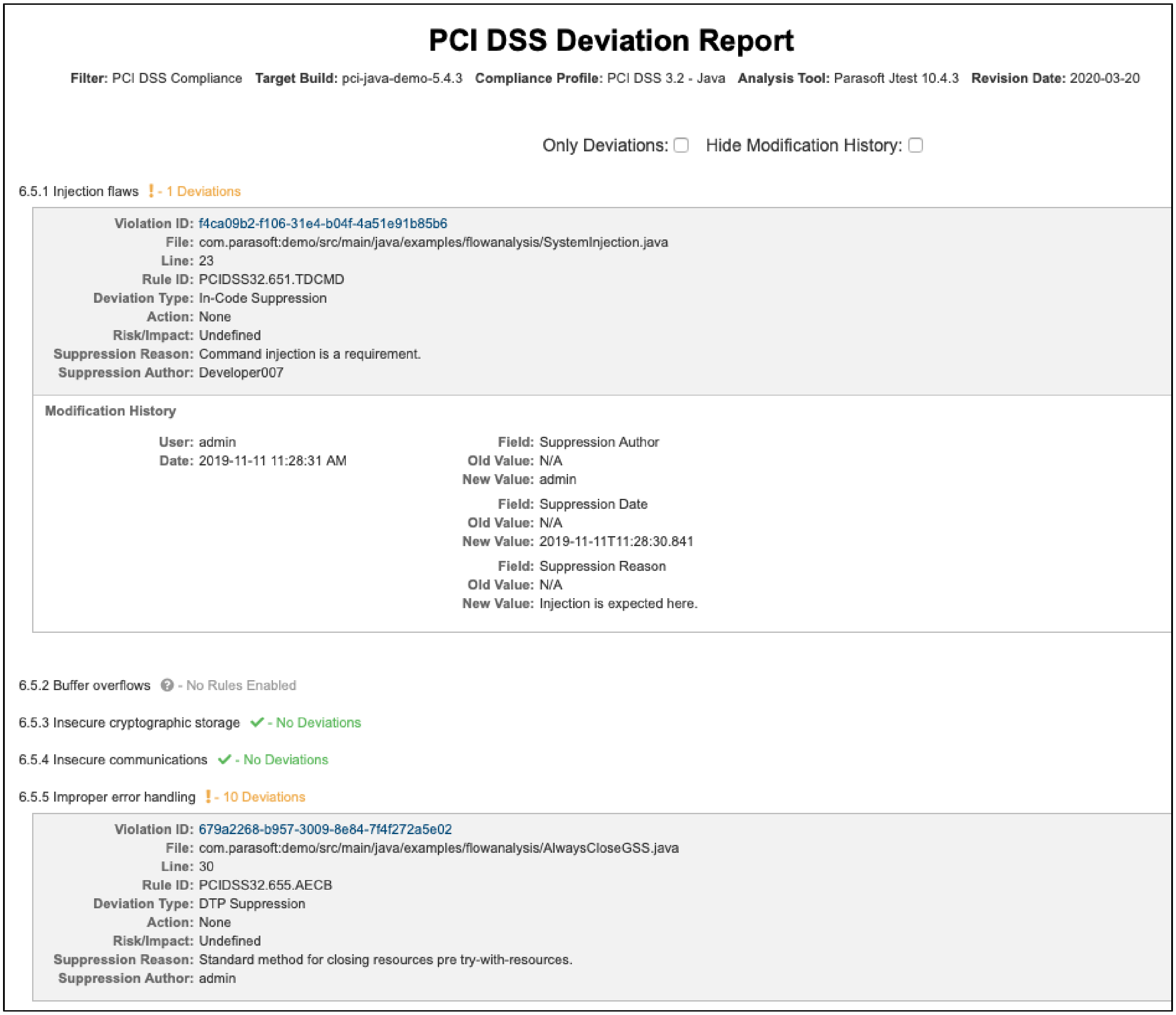
Compliance Profile: PCI DSS 3.2 - Java **Analysis Tool:** Parasoft Jtest 10.4.3 **Revision Date:** 2019-10-02

Requirement	Description	Parasoft Rule Ids
6.5.1	Injection flaws	PCIDSS32.651.TDCMD PCIDSS32.651.UPS PCIDSS32.651.TDSQL PCIDSS32.651.TDLDAP PCIDSS32.651.TDNET PCIDSS32.651.TDRFL PCIDSS32.651.TDXPATH PCIDSS32.651.TDENV PCIDSS32.651.TDJXPATH PCIDSS32.651.TDLOG PCIDSS32.651.TDDIG PCIDSS32.651.TDXML PCIDSS32.651.XPIJ PCIDSS32.651.TDINPUT
6.5.2	Buffer overflows	
6.5.3	Insecure cryptographic storage	PCIDSS32.653.AISSAJAVA PCIDSS32.653.PWDPROP PCIDSS32.653.CKTS PCIDSS32.653.ICA PCIDSS32.653.SRD PCIDSS32.653.ACMD PCIDSS32.653.AUNC PCIDSS32.653.MDSALT PCIDSS32.653.AISSAXML PCIDSS32.653.PLAIN PCIDSS32.653.PLC
6.5.4	Insecure communications	PCIDSS32.654.HTTPS PCIDSS32.654.USC PCIDSS32.654.CONSEN PCIDSS32.654.HCCK PCIDSS32.654.SIKG PCIDSS32.654.MCMDU

Deviations Report

Your code can contain violations and still be PCI DSS-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.

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



PCI DSS Deviation Report

Filter: PCI DSS Compliance **Target Build:** pci-java-demo-5.4.3 **Compliance Profile:** PCI DSS 3.2 - Java **Analysis Tool:** Parasoft Jtest 10.4.3 **Revision Date:** 2020-03-20

Only Deviations: □ Hide Modification History: □

6.5.1 Injection flaws ! - 1 Deviations

Violation ID: f4ca09b2-f106-31e4-b04f-4a51e91b85b6
File: com.parasoft:demo/src/main/java/examples/flowanalysis/SystemInjection.java
Line: 23
Rule ID: PCIDSS32.651.TDCMD
Deviation Type: In-Code Suppression
Action: None
Risk/Impact: Undefined
Suppression Reason: Command injection is a requirement.
Suppression Author: Developer007

Modification History

User: admin
Date: 2019-11-11 11:28:31 AM

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

Field: Suppression Date
Old Value: N/A
New Value: 2019-11-11T11:28:30.841

Field: Suppression Reason
Old Value: N/A
New Value: Injection is expected here.

6.5.2 Buffer overflows ? - No Rules Enabled

6.5.3 Insecure cryptographic storage ✓ - No Deviations

6.5.4 Insecure communications ✓ - No Deviations

6.5.5 Improper error handling ! - 10 Deviations

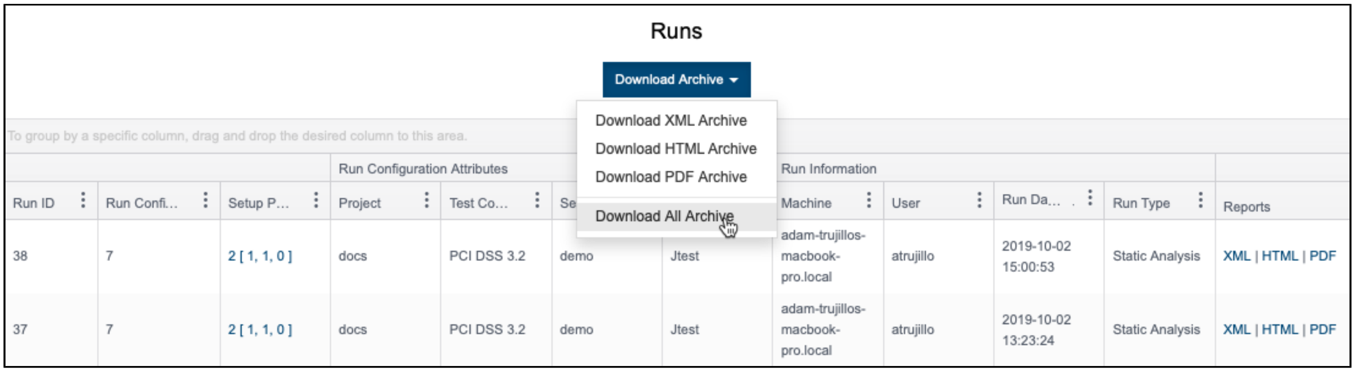
Violation ID: 679a2268-b957-3009-8e84-7f4f272a5e02
File: com.parasoft:demo/src/main/java/examples/flowanalysis/AlwaysCloseGSS.java
Line: 30
Rule ID: PCIDSS32.655.AECB
Deviation Type: DTP Suppression
Action: None
Risk/Impact: Undefined
Suppression Reason: Standard method for closing resources pre try-with-resources.
Suppression Author: admin

The Deviations Report shows all requirement IDs and headers, but requirements that have been suppressed will show additional information. You can perform the following actions:

- Enable the **Only Deviations** option to only show deviations
- Enable the **Hide Modification History** option to exclude the modification history for 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 PCI DSS during a regulatory audit.



Runs

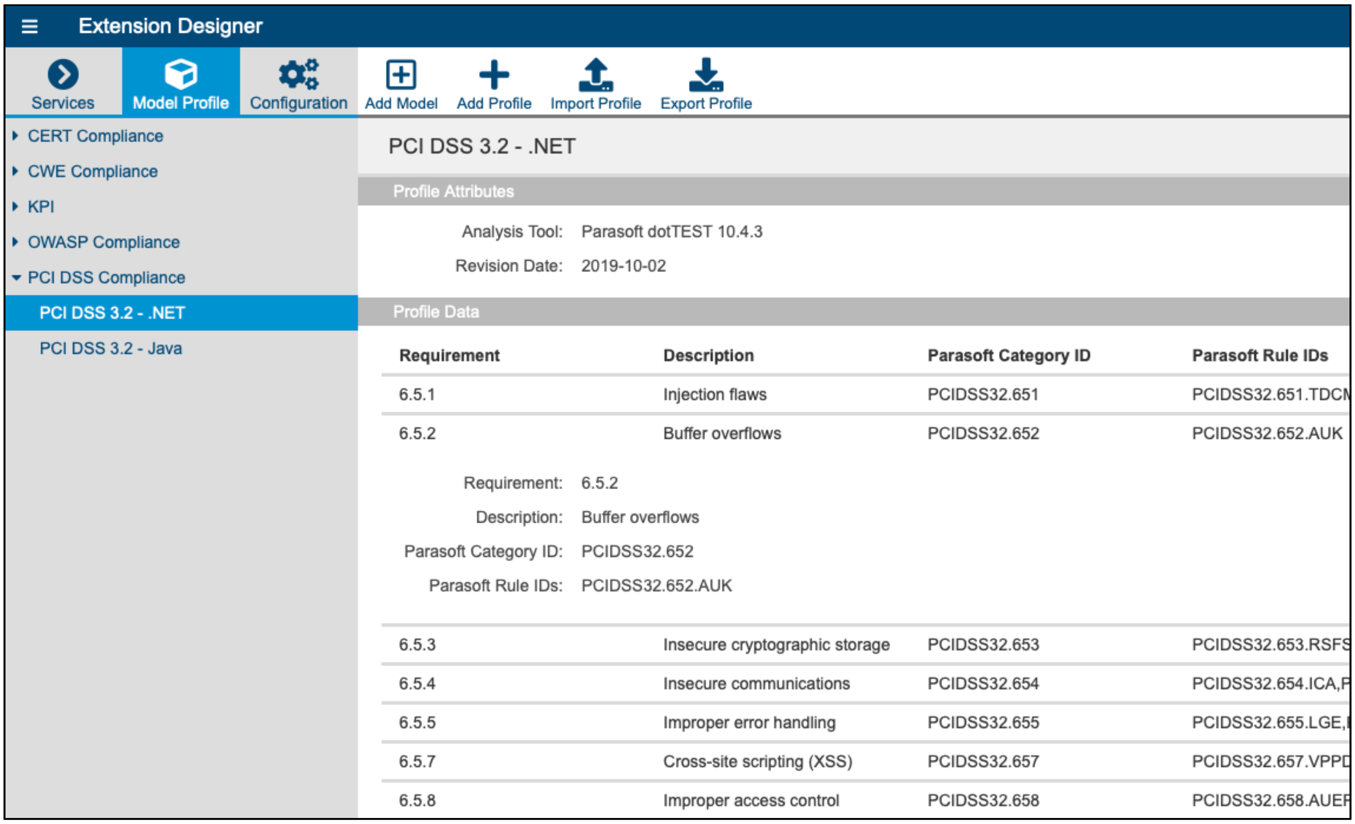
			Run Configuration Attributes				Run Information				
Run ID	Run Confi...	Setup P...	Project	Test Co...	Se		Machine	User	Run Da...	Run Type	Reports
38	7	2 [1, 1, 0]	docs	PCI DSS 3.2	demo	Jtest	adam-trujillos-macbook-pro.local	atrujillo	2019-10-02 15:00:53	Static Analysis	XML | HTML | PDF
37	7	2 [1, 1, 0]	docs	PCI DSS 3.2	demo	Jtest	adam-trujillos-macbook-pro.local	atrujillo	2019-10-02 13:23:24	Static Analysis	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 PCI DSS Compliance artifact ships with a default model and profile for code analysis results from Parasoft dotTEST and Jtest. Each profile contains categorization information for mapping Parasoft rules to PCI DSS requirements.



PCI DSS 3.2 - .NET

Profile Attributes

Analysis Tool: Parasoft dotTEST 10.4.3

Revision Date: 2019-10-02

Profile Data

Requirement	Description	Parasoft Category ID	Parasoft Rule IDs
6.5.1	Injection flaws	PCIDSS32.651	PCIDSS32.651.TDCM
6.5.2	Buffer overflows	PCIDSS32.652	PCIDSS32.652.AUK

Requirement: 6.5.2
Description: Buffer overflows
Parasoft Category ID: PCIDSS32.652
Parasoft Rule IDs: PCIDSS32.652.AUK

Requirement	Description	Parasoft Category ID	Parasoft Rule IDs
6.5.3	Insecure cryptographic storage	PCIDSS32.653	PCIDSS32.653.RSFS
6.5.4	Insecure communications	PCIDSS32.654	PCIDSS32.654.ICA,F
6.5.5	Improper error handling	PCIDSS32.655	PCIDSS32.655.LGE,I
6.5.7	Cross-site scripting (XSS)	PCIDSS32.657	PCIDSS32.657.VPPD
6.5.8	Improper access control	PCIDSS32.658	PCIDSS32.658.AUEF

The profile includes information necessary for generating compliance reports, as well as displaying data in the widgets shipped with the PCI DSS 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 Requirement Enforcement 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 PCI DSS artifact.