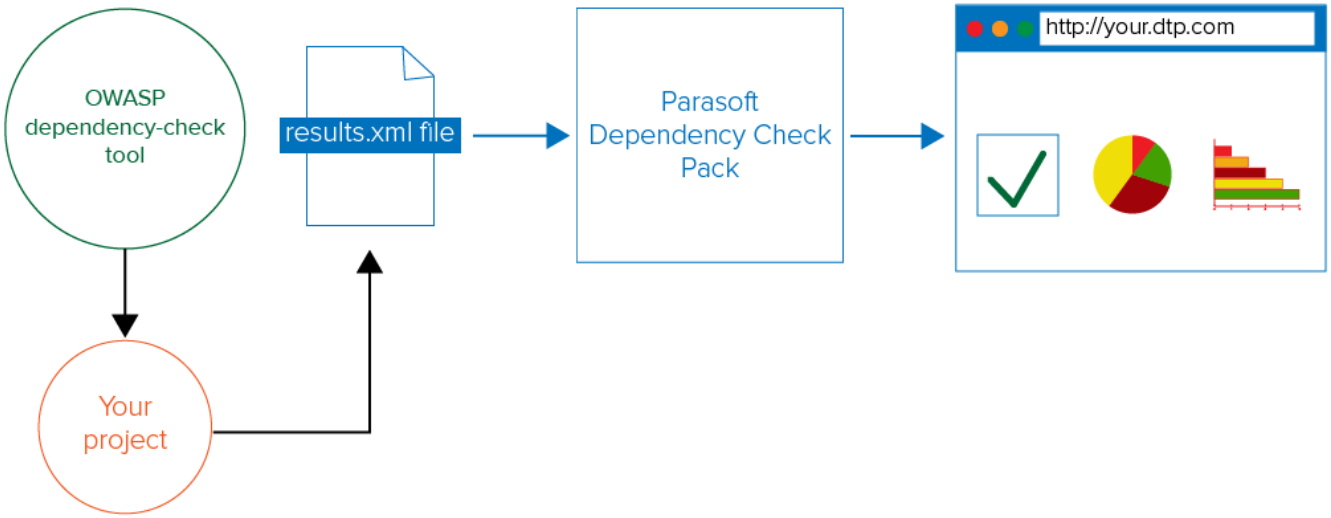
OWASP Dependency Check Pack

In this section:

Introduction

OWASP dependency-check is an open source tool that scans Java and .NET projects and identifies the use of known vulnerable components. Parasoft OWASP Dependency Check Pack reads the results the OWASP dependency-check tool and reports vulnerabilities to Parasoft DTP in a standardized format. This enables DTP to present the data in widgets and to provide remediation paths for addressing the vulnerabilities.

Vulnerabilities are reported in DTP as violations of the OWASP Top 10 2013 entry: A9 Using Components with Known Vulnerabilities guideline. Merging the OWASP Dependency Check Pack data with code analysis results from Parasoft Jtest or dotTEST enables the full implementation of your OWASP security compliance initiative.



Requirements

Oracle Java Runtime 8 or higher

- X-Server access (Linux only). The `DISPLAY` variable must be set and access control must be disabled for the `xhost` command (run `xtest +`). This is required to ensure that overview images in HTML reports display correctly.
- OWASP dependency-check results in XML format. See the OWASP dependency-check documentation for details.
- A valid license for Parasoft Test 10.4 added to your DTP License Server.

Deployment

The OWASP Dependency Check Pack is shipped with the Parasoft Security Bundle.

1. Extract the contents of the security-bundle-<version>.zip file, which contains the dependency-check-<version>.zip and security-compliance-pack-<version>.zip files.
2. Extract the dependency-check-pack-<version>.zip file distribution to the desired location. Some extractor tools, such as the default Windows and MacOS extractors, will create a directory for the dependency check pack files. We recommend creating an installation home directory if your tool does not automatically create a directory to hold the extracted files.
3. Follow the instructions for installing Security Compliance Pack into your DTP environment. This step is not required to run the OWASP Dependency Check Pack, but it is required for viewing results in DTP.

OWASP dependency-check Rule Documentation

For DTP to display the OWASP dependency-check rule documentation, the rules shipped with the OWASP Dependency Check Pack must be copied to the DTP rules directory.

Copy the contents of the <DEPENDENCY_CHECK_INSTALL>/rulesdoc/dependencycheck/ directory to the <DTP_INSTALL>/tomcat/webapps/grs/rulesdoc/ directory.

After copying the rules, documentation associated with OWASP dependency-check violations will be available in DTP interfaces, such as the Documentation tab of the Violations Explorer.

Connecting to DTP

The OWASP Dependency Check Pack is a separate tool and must connect to DTP to acquire a license and to send results to your DTP project. Specify the following settings in the *settings.properties* file located in the installation directory:

dtp.server

Specifies the host name of the DTP server.

dtp.port

Specifies the DTP port number. Default is `8443`.

dtp.user

Specifies the user name for DTP authentication.

dtp.password

Specifies the user password for DTP authentication. You can encode your DTP password by running the dependency.sh or .bat with the `-encodepass` parameter. For example:

```
./dependencycheck.sh -encodepass=<mypassword>
```

dtp.project

Specifies the name of the existing DTP project that you want to link to.

build.id

Specifies the build that the data should be associated with. For accurate results, the build ID should match the build ID configured in your static analysis tool

Usage

If you have not already done so, execute OWASP dependency-check. The results should be output to an XML file.

Open a command prompt and navigate to the OWASP Dependency Check Pack installation directory.

Execute the .BAT or .SH script with specifying the OWASP dependency-check results using the `-results.file` parameter, e.g.:

```
./dependencycheck.sh -results.file="/Users/admin/Desktop/dependency_check.xml"
```

The `-results.file` is the only required parameter, but you can pass the following optional parameters:

-parasoft.local.storage.dir

This settings specifies the location for generated log files. The recommended location is `${project.base.dir}/.dependencycheck`.

For example:

```
-parasoft.local.storage.dir=.dependencycheck
```

-settings

By default, the OWASP Dependency Check Pack will reference the settings.properties file in the installation directory, but you can use this setting to point to alternate configuration files. Example:

```
-settings=C:\my-team-configs\my-settings.properties
```

Viewing Results

After executing the OWASP Dependency Check Pack, results are output in two ways:

- As local Parasoft HTML reports. The local HTML report (and XML data that feeds the report) are saved to the <INSTALL>/reports directory after execution.
- Sent to DTP and presented in widgets, reports, and other visualizations. Vulnerabilities are reported in DTP as violations of the OWASP Top 10 2013 entry: A9 Using Components with Known Vulnerabilities guideline. See OWASP Compliance for details on viewing violations in DTP.