Victi.ms

Eclipse Plugin User Guide

Victi.ms Eclipse Plugin User Guide
Edition 1.0

This Eclipse plugin provides the functionality to scan a Java projects dependencies against a database of publicly known vulnerabilities. The canonical version of the database is hosted at http://victi.ms and is maintained by Red Hat security teams.

Introduction

Victims-Plugin-Eclipse is an Eclipse plugin which can be utilised from within the Eclipse IDE. The plugin provides the functionality to scan a Java projects dependencies against a database of publicly known vulnerabilities. The canonical version of the database is hosted at https://victi.ms and is maintained by Red Hat Security teams. It also allows for other vulnerability databases to be compared against utilising the victims java library. The methods of comparing java libraries to vulnerabilities is by fingerprinting of class and jar files or matching jar manifest file information against records in the database. The plugin also optionally lets you configure a different database for vulnerability sources.

Implementation

Utilising the Victims Java library the program creates a local copy of the database which is then synchronised automatically/daily or not at all based on settings defined when executing the task. Please note that the first execution of the task will take some time as it synchronises the whole Victims database. The files to scan are fetched from Eclipse via the projects dependencies that you are executing it against. Currently, the plugin will scan all dependencies linked to a project. Due to the way Eclipse handles the core java libraries, these will also be scanned. In future versions this functionality will be provided as an option. The plugin utilises caching so consecutive scans will be efficient and has a concurrent implementation so large projects shouldn't be a problem.

Installation

We don't have a deployed jar for this plugin yet but will be hosting one soon. In the meantime you can clone the project and build it yourself. The source code contains two projects, Victims-p2-repo, and Victims-Plugin-Eclipse. Victims-p2-repo is used for automatic resolving of third party non-OSGi dependencies and hosting a p2 compliant repository. It is required that you build this project first before building Victims-Plugin-Eclipse.

To perform the build and run the webserver:

```
cd victims-plugin-eclipse/victims-p2-repo/
mvn p2:site
mvn jetty:run
```

You should then be able to build the Eclipse plugin using:

```
mvn clean install
```

Usage

To use the Eclipse plugin simply install the plugin using an update site and then right click on your project (Only java is supported at the moment) and hit Victims Scan. The default options should be satisfactory for now. Please note that although there are options for fingerprint and metadata they do not have any effect as the scan is not performed as part of the build.

4.1. Configuration Options

baseUrl

The URL of the victims web service used to synchronize the local database.

default: "https://victims"

entryPoint

The entrypoint of the victims webservice to synchronize against.

default: "/service"

metadata

The severity of exception to be thrown when a dependency is encountered that matches the known vulnerable database based on metadata. Fatal indicates the build should fail, warning indicates a warning should be issued but the build should proceed.

allowed: warning, fatal, disabled
default: warning

fingerprint

The severity of exception to be thrown when a dependency is encountered that matches the known vulnerable database based on a fingerprint. Fatal indicates the build should fail, warning indicates a warning should be issued but the build should proceed.

allowed: warning, fatal, disabled
default: fatal

updates

Allows the configuration of the synchronization mechanism. In automatic mode new entries in the victims database are pulled from the victims-web instance during each build. In daily mode new entries are pulled from the victims-web instance only once per day. The synchronization mechanism may be disabled and processed manually for closed build environments.

allowed: auto, offline, daily
default: auto

jdbcDriver

The jdbc driver to use for the local victims database. By default victims uses an embedded H2 database.

default: org.h2.Driver

jdbcUrl

The jdbc connection URL to for the local victims database.

default: .victims (embedded h2 instance)

jdbcUser

The username to use for the jdbc connection.

default: "victims"

jdbcPass

The password to use for the jdbc connection.

default: "victims"

Appendix A. Revision History

Revision 1-0 Fri Aug 16 2013 Isaac Anderson

First version created