Victi.ms

Jenkins Plugin User Guide

Victi.ms Jenkins Plugin User Guide
Edition 1.0

This Jenkins-CI 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.

1. Introduction **1**

2. Implementation **2**

3. Usage **3**

3.1. Obtaining Victims Plugin HPI 3
3.2. Installation 3
3.3. Adding Victims Action 3
3.4. Configuration Options 3
3.5. Building Your Project 4

A. Revision History **5**

Introduction

Victims-plugin-jenkins is a Jenkins-CI plugin which provides a post build action to Jenkins. 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.

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 passed to the plugin via a setting on the project configuration page. A single jar can be scanned or if a directory is provided then the plugin will recursively scan for all .jar files within it.

The plugin will utilise the caching capabilities of victims-lib-java to make repeated builds more efficient. It also has a concurrent implementation to make large builds with many dependencies quicker.

Usage

For the purposes of this guide we assume you have Jenkins-CI installed.

3.1. Obtaining Victims Plugin HPI

Currently the Victims plugin can only be obtained by compiling from *source*[1]. The project is built using Maven with the following command:

```
mvn install
```

3.2. Installation

The plugin can be installed through Jenkins' plugin manager (http://yourhost/jenkins/pluginManager/).

3.3. Adding Victims Action

To add the victims post build scan action go into the configuation page for your project. From there the post build action can be added and configured.

3.4. 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.

options: 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.

[1] https://github.com/victims/victims-plugin-jenkins

options: 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.

options: 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"

Build Directory or File

The output directory of your build or the file produced. If a directory is supplied the plugin will recursively scan the directory for .jar files.

Verbose File Scanning

If set the log will list all files scanned and whether they are cached or not.

default: false

3.5. Building Your Project

Once the configuration has been saved the victims plugin will run the next time the project is built.

The plugin will run after the project is built. If the plugin isn't configured to fail the build will still succeed with vulnerabilities. To find out the results of the scan check the build log.

Appendix A. Revision History

Revision 1-0 Fri Aug 16 2013 Isaac Anderson

First version created