CS 305 Integrating the Maven Dependency-Check Plug-In Tutorial

This course uses Maven, which is a package manager. You can choose to run the dependency check as a standalone application or as part of a Maven project. This tutorial shows you how to run a dependency check as a Maven project. Follow these steps to integrate the dependency-check plug-in.

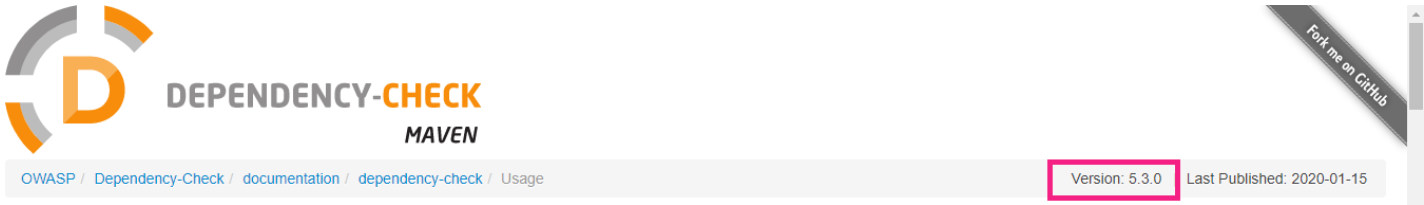
1. Go to OWASP Dependency-Check Maven. Refer to the example provided on the webpage and as shown below:

Example 1:

Create the dependency-check-report.html in the target directory.

```
<project>
    ...
    <build>
        ...
        <plugins>
            ...
            <plugin>
              <groupId>org.owasp</groupId>
              <artifactId>dependency-check-maven</artifactId>
              <version>5.3.0</version>
              <executions>
                  <execution>
                      <goals>
                          <goal>check</goal>
                      </goals>
                  </execution>
              </executions>
            </plugin>
            ...
        </plugins>
        ...
    </build>
    ...
</project>
```

2. Identify the current version number of the dependency check. You will need this information for Step 3.



3. Next, upload the Maven project you would like to complete a static test for in Eclipse.

    a. Open the pom.xml file to add the dependency-check plug-in.

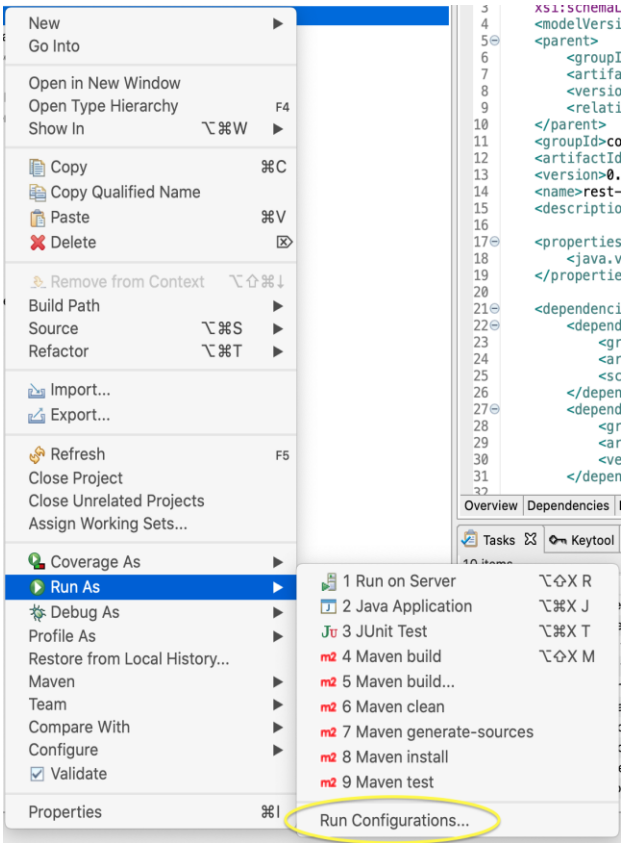
b. Copy the following lines of code and paste the code into the pom.xml file. Be sure the version number is current based on your findings in step 2.

```
            <plug-in>
                <groupId>org.owasp</groupId>
                <artifactId>dependency-check-maven</artifactId>
                <version>5.3.0</version>
                <executions>
                    <execution>
                        <goals>
                            <goal>check</goal>
                        </goals>
                    </execution>
                </executions>
              </plug-in>
```

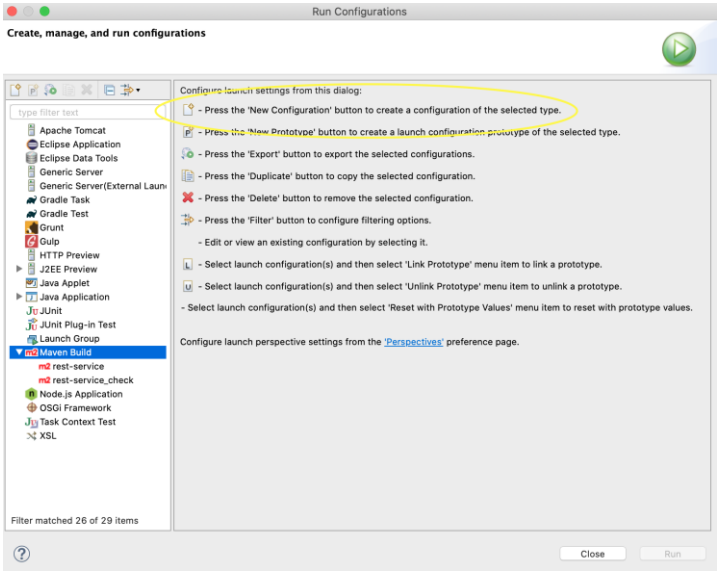
*Please note: To use the dependency-check plug-in, you will need to complete these steps for **each** code base or software application.*

4. When you compile your code, Eclipse will run the Maven plug-in. Run the pom.xml file to ensure that the plug-in is running effectively.

   a. On the menu bar, click **Run**, **Run As**, and **Run Configurations.**

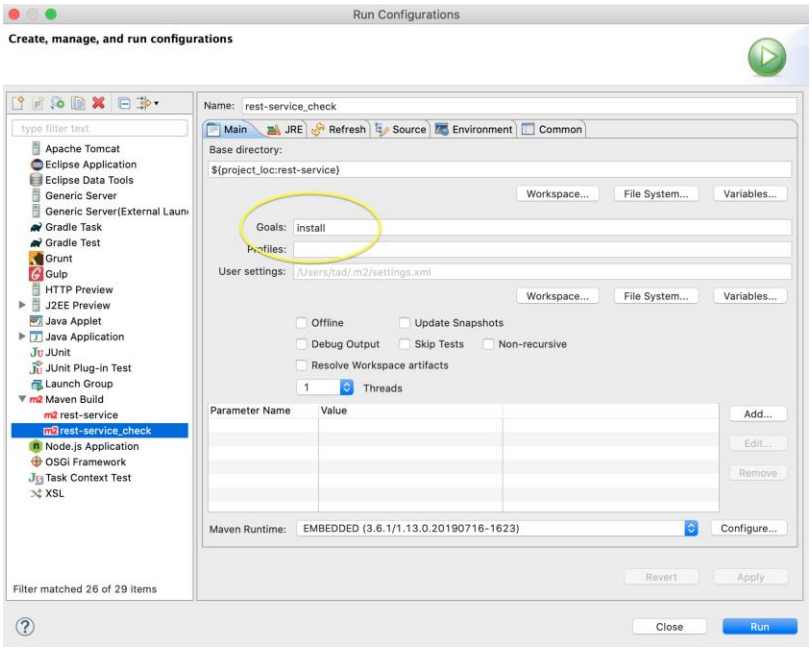


b. In the Run Configurations window in Eclipse, double-click on **Maven Build**.

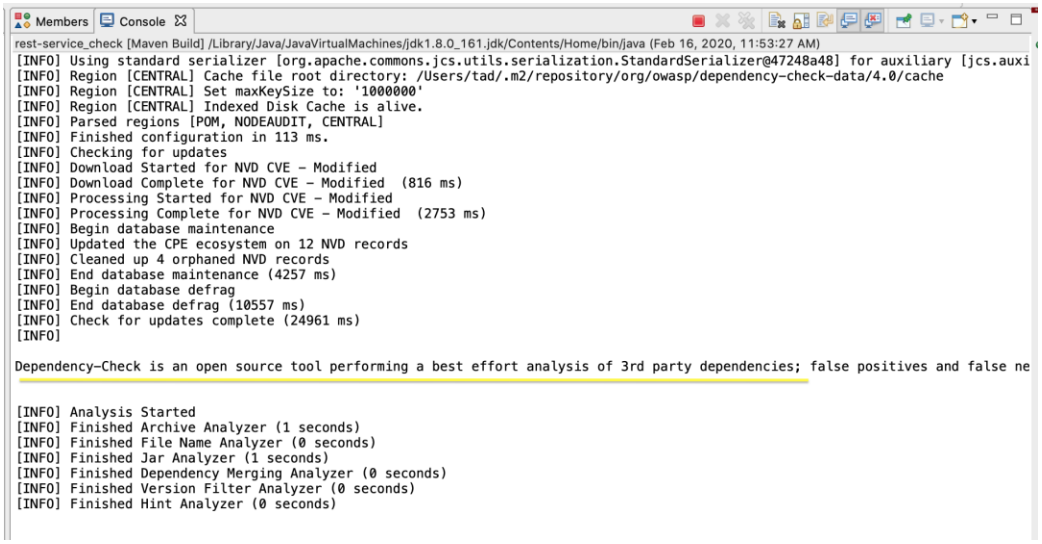


i. Choose the Base directory if it is not already present by clicking **Workspace**, then select the appropriate directory.

c. Set goals to “install” then click **Run**.



d. Be sure to observe the **Console** for dependency-check execution. The first time you do this, it will require more time to download the Common Vulnerabilities and Exposures (CVE) from the National Vulnerabilities Database (NVD).



e. When the Run is complete, check under the **Target director** of the project to see the report: **dependency-check-report.html**.

   i. A sample report is available: Dependency-Check Report. The output report should look similar to the example below.

Project: DependencyCheck

Scan Information (show all):

- *dependency-check version*: 1.4.4-SNAPSHOT
- *Report Generated On*: Oct 9, 2016 at 07:04:35 EDT
- *Dependencies Scanned*: 306 (289 unique)
- *Vulnerable Dependencies*: 36
- *Vulnerabilities Found*: 289
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
ghostscript/configure.ac	cpe:/a:ghostscript:ghostscript:8.62		High	5	HIGHEST	4
axis-1.4.jar	cpe:/a:apache:axis:1.4	axis:axis:1.4	Medium	2	HIGHEST	17
axis2-kernel-1.4.1.jar	cpe:/a:apache:axis2:1.4.1	org.apache.axis2:axis2-kernel:1.4.1	High	6	HIGHEST	16
ffmpeg\ffmpeg_version.cmake	cpe:/a:ffmpeg:ffmpeg:55.18.102		High	3	LOW	3
cmake\OpenCVDetectPython.cmake	cpe:/a:python:python:-		High	11	LOW	1
commons-fileupload-1.2.1.jar	cpe:/a:apache:commons_fileupload:1.2.1	commons-fileupload:commons-fileupload:1.2.1	High	3	HIGHEST	23
commons-httpclient-3.1.jar	cpe:/a:apache:commons-httpclient:3.1 cpe:/a:apache:httpclient:3.1	commons-httpclient:commons-httpclient:3.1	Medium	2	LOW	20