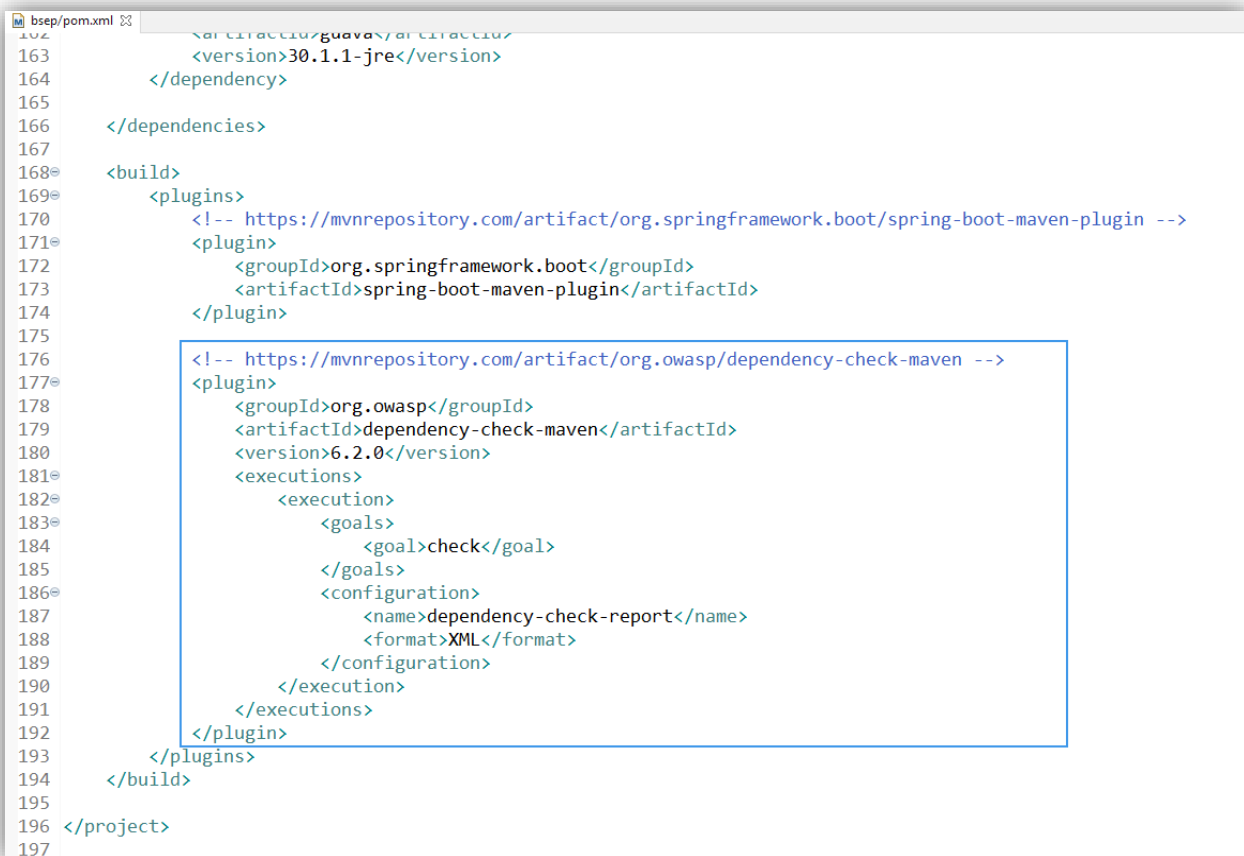


Dependency vulnerability check in a PKI

Spring Boot application

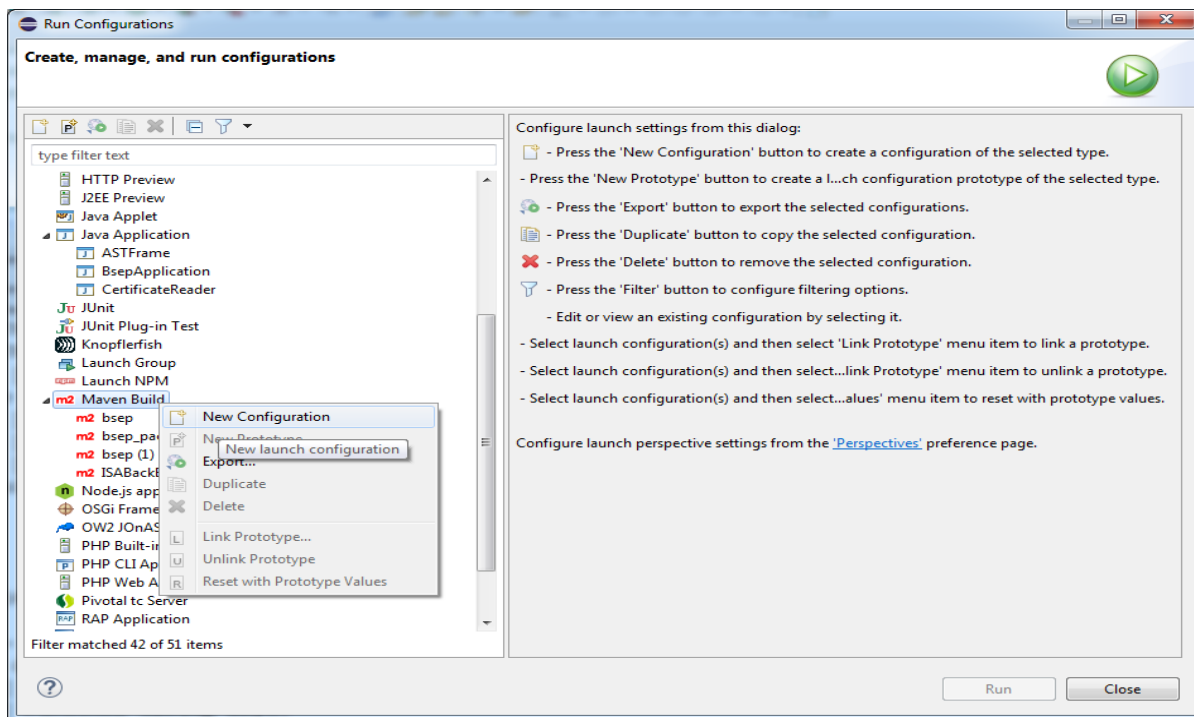
Steps for running a dependency check test

1. Add the next part of the code in a pom XML file

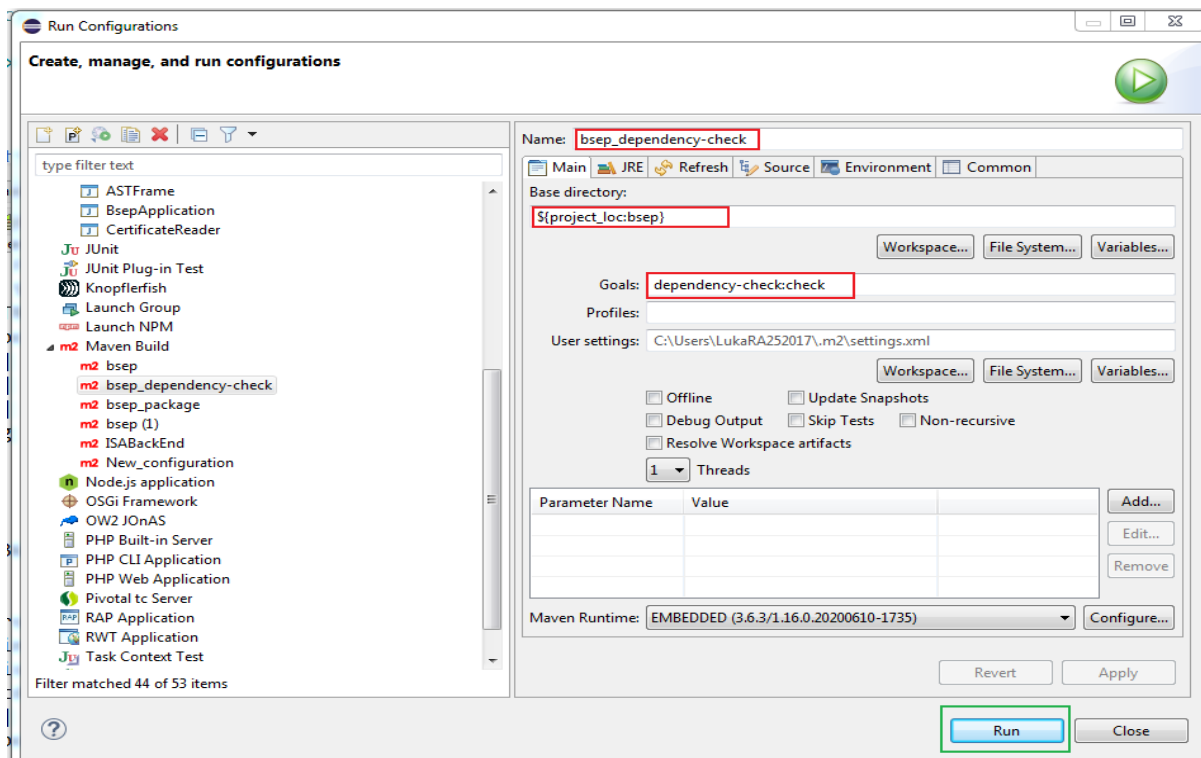


```
163     <artifactId>guava</artifactId>
164     <version>30.1.1-jre</version>
165     </dependency>
166 </dependencies>
167
168 <build>
169     <plugins>
170         <!-- https://mvnrepository.com/artifact/org.springframework.boot/spring-boot-maven-plugin -->
171         <plugin>
172             <groupId>org.springframework.boot</groupId>
173             <artifactId>spring-boot-maven-plugin</artifactId>
174         </plugin>
175
176         <!-- https://mvnrepository.com/artifact/org.owasp/dependency-check-maven -->
177         <plugin>
178             <groupId>org.owasp</groupId>
179             <artifactId>dependency-check-maven</artifactId>
180             <version>6.2.0</version>
181             <executions>
182                 <execution>
183                     <goals>
184                         <goal>check</goal>
185                     </goals>
186                     <configuration>
187                         <name>dependency-check-report</name>
188                         <format>XML</format>
189                     </configuration>
190                 </execution>
191             </executions>
192         </plugin>
193     </plugins>
194 </build>
195
196 </project>
197
```

2. Then right-click on the pom.xml file, after which you will find the Run as option, and then hold the mouse cursor over it, a drop-down menu will open. After clicking the Run Configurations option, a modal dialog will be displayed (see image below). Then right-click on Maven Build and select new configuration.

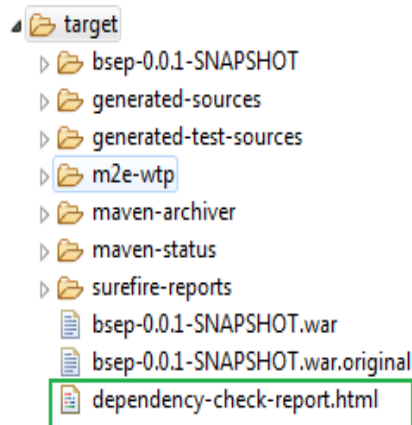


3. Finally, fill in the input fields as shown in the photo and run the dependency check test



Dependency-check report

When the report is generated, you will be able to find it in the target folder.



Example of the first dependency-check report summary

Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
bcprov-jdk15on-1.57.jar	cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle:1.57:*:*:*:*:* cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.57:*:*:*:*:*	pkg:maven/org.bouncycastle/bcprov-jdk15on@1.57	CRITICAL	4	Low	47
bcprov-jdk16-1.45.jar	cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-cryptography-api:1.45:*:*:*:*:*	pkg:maven/org.bouncycastle/bcprov-jdk16@1.45	Unknown	16	Highest	27
httpclient-4.3.6.jar	cpe:2.3:a:apache:httpclient:4.3.6:*:*:*:*:*	pkg:maven/org.apache.httpcomponents/httpclient@4.3.6	MEDIUM	1	Highest	34
maven-core-2.0.9.jar	cpe:2.3:a:apache:maven:2.0.9:*:*:*:*:*	pkg:maven/org.apache.maven/maven-core@2.0.9	CRITICAL	1	Highest	25
plexus-utils-2.0.5.jar	cpe:2.3:a:plexus-utils:project:plexus-utils:2.0.5:*:*:*:*:*	pkg:maven/org.codehaus.plexus/plexus-utils@2.0.5	Unknown	3	Highest	29

Consideration of the vulnerability of the plexus-utils dependency 2.0.5

For example, for this dependence, the dependency-check report shows us that there is a possibility of performing XML Injections.

```
References:
  • OSSINDEX - Directory traversal in org.codehaus.plexus.util.Expand

Vulnerable Software & Versions (OSSINDEX):
  • cpe:2.3:a:org.codehaus.plexus:plexus-utils:2.0.5:*:*:*:*:*

Possible XML Injection (OSSINDEX) suppress

> `org.codehaus.plexus.util.xml.XmlWriterUtil#writeComment(XmlWriter, String, int, int, int)` does not check if the comment includes a "-->" sequence. This means that text contained in the
command string could be interpreted as XML, possibly leading to XML injection issues, depending on how this method is being called.
>
> -- [github.com](https://github.com/codehaus-plexus/plexus-utils/issues/3)

Unscored:
  • Severity: Unknown

References:
  • OSSINDEX - Possible XML Injection

Vulnerable Software & Versions (OSSINDEX):
  • cpe:2.3:a:org.codehaus.plexus:plexus-utils:2.0.5:*:*:*:*:*
```

We are suggested to replace this version of dependency with a new one.

After the version was updated, the vulnerability disappeared and we made the PKI system more secure.

Below, we present the specific dependencies that have affected security in terms of vulnerability.

Updated dependencies

No.	GroupId	ArtifactId	Old version	New version
1.	org.bouncycastle	bcpkix-jdk15on	1.57	1.68
2.	org.apache.httpcomponents	httpclient	4.3.6	4.5.13
3.	io.jsonwebtoken	jjwt	0.6.0	0.9.1

Added dependencies

No.	GroupId	ArtifactId	Version
1.	org.apache.maven	maven-core	3.8.1
2.	commons-io	commons-io	2.9.0
3.	com.google.guava	guava	30.1.1-jre
4.	org.codehaus.plexus	plexus-utils	3.3.0

Removed dependencies

No.	GroupId	ArtifactId	Version
1.	org.bouncycastle	bcprov-jdk16	1.46

Conclusion

Based on the generated "dependency-check" report, we found that certain dependencies have vulnerabilities. We followed the advice, we upgraded the older versions of the addition with the newer ones. We have achieved satisfactory results, and by adding the still missing recommended dependencies, we have made our PKI application have a high degree of security.



DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS-IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

[Sponsor](#)

Project: bsep

bsep:bsep:0.0.1-SNAPSHOT

Scan Information ([show all](#)):

- *dependency-check version*: 6.2.0
- *Report Generated On*: Tue, 1 Jun 2021 15:15:27 +0200
- *Dependencies Scanned*: 124 (90 unique)
- *Vulnerable Dependencies*: 0
- *Vulnerabilities Found*: 0
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
------------	-------------------	---------	------------------	-----------	------------	----------------