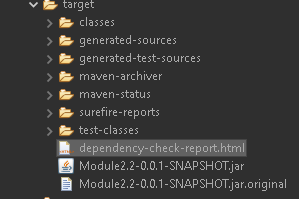
# CS 305 Module Two Coding Assignment

## Run Dependency Check



A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Document Results

Below are the dependencies identified during the dependency check, along with their vulnerability details:  
  
1. hibernate-validator-6.0.18.Final.jar  
 - Vulnerability ID: cpe:2.3:a:redhat:hibernate\_validator:6.0.18:\*:\*:\*:\*:\*:\*:\*  
 - Severity: MEDIUM  
 - CVE Count: 1  
 - Confidence: Highest  
 - Evidence Count: 32  
  
2. jackson-databind-2.10.2.jar  
 - Vulnerability ID: cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\*  
 - Severity: HIGH  
 - CVE Count: 6  
 - Confidence: Highest  
 - Evidence Count: 39  
  
3. log4j-api-2.12.1.jar  
 - Vulnerability ID: cpe:2.3:a:apache:log4j:2.12.1:\*:\*:\*:\*:\*:\*:\*  
 - Severity: LOW  
 - CVE Count: 1  
 - Confidence: Highest  
 - Evidence Count: 42  
  
4. logback-core-1.2.3.jar  
 - Vulnerability ID: cpe:2.3:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\*  
 - Severity: HIGH  
 - CVE Count: 2  
 - Confidence: Highest  
 - Evidence Count: 31  
  
5. mongo-java-driver-2.4.jar  
 - Vulnerability ID: cpe:2.3:a:mongodb:java\_driver:2.4:\*:\*:\*:\*:\*:\*:\*  
 - Severity: MEDIUM  
 - CVE Count: 1  
 - Confidence: Highest  
 - Evidence Count: 20  
  
6. snakeyaml-1.25.jar  
 - Vulnerability ID: cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 8  
 - Confidence: Highest  
 - Evidence Count: 44  
  
7. spring-boot-2.2.4.RELEASE.jar  
 - Vulnerability ID: cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 3  
 - Confidence: Highest  
 - Evidence Count: 39  
  
8. spring-boot-starter-web-2.2.4.RELEASE.jar  
 - Vulnerability ID: cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 3  
 - Confidence: Highest  
 - Evidence Count: 35  
  
9. spring-core-5.2.3.RELEASE.jar  
 - Vulnerability ID: cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 11  
 - Confidence: Highest  
 - Evidence Count: 36  
  
10. spring-expression-5.2.3.RELEASE.jar  
 - Vulnerability ID: cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 12  
 - Confidence: Highest  
 - Evidence Count: 36  
  
11. spring-web-5.2.3.RELEASE.jar  
 - Vulnerability ID: cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 15  
 - Confidence: Highest  
 - Evidence Count: 34  
  
12. spring-webmvc-5.2.3.RELEASE.jar  
 - Vulnerability ID: cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 11  
 - Confidence: Highest  
 - Evidence Count: 36  
  
13. tomcat-embed-core-9.0.30.jar  
 - Vulnerability ID: cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 26  
 - Confidence: Highest  
 - Evidence Count: 30  
  
14. tomcat-embed-websocket-9.0.30.jar  
 - Vulnerability ID: cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*  
 - Severity: CRITICAL  
 - CVE Count: 27  
 - Confidence: Highest  
 - Evidence Count: 30

Spring Boot Version 2.2.4.RELEASE (Critical Vulnerabilities)

A screen shot of a computer code

Description automatically generated

Vulnerabilities: Critical vulnerabilities in spring-boot-starter-web-2.2.4.RELEASE.jar.

MongoDB Java Driver Version 2.4 (Medium Vulnerabilities)

A screen shot of a computer

Description automatically generated

Vulnerabilities: Medium severity in mongo-java-driver-2.4.jar.

## Analyze Results

The best solutions for addressing dependencies in the code base are:

**Upgrade Spring Boot and Related Dependencies**:

* The version of Spring Boot (2.2.4.RELEASE) used in the project has major security problems. It should be upgraded to a newer version, like 2.5.x or higher. This will fix issues with spring-boot-starter-web, spring-core, and other related issues.

**MongoDB Java Driver**:

* The MongoDB Java driver version 2.4 has medium-level security risks. This also needs to be updated to a newer version

**Tomcat Embedded Dependencies**:

* The tomcat-embed-core and tomcat-embed-websocket at version 9.0.30 have serious security issues. These need to be updated.

**Filter False Positives**:

* When we run the OWASP Dependency Check, not all errors/issues flagged by the tool are real threats. Some may be "false positives" a.k.a issues that don’t actually affect the project. Filtering these out helps us focus on the real problems.

### Summary:

* Regularly updating your code with updated andsecure versions of libraries and filtering out false positives are important steps in keeping your code safe. Using trusted resources like CVE and NVD can help you stay on top of security issues.