# CS 305 Module Two Coding Assignment Template

## Run Dependency Check

A computer screen with many colorful text

Description automatically generated

HTML Report created in Eclipse

A screenshot of a web page

Description automatically generated

Scan information from dependency check report.

## Document Results

|  |  |  |
| --- | --- | --- |
| **Name** | **License** | **Description** |
| Classmate-1.5.1.jar | Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0.txt | Library for introspecting types with full generic information including resolving of field and method types. |
| Hibernate-validator-6.0.18.Final.jar | <http://www.apache.org/licenses/LICENSE-2.0.txt> | Hibernate's Bean Validation (JSR-380) reference implementation. |
| Jackson-core-2.10.2.jar | <http://www.apache.org/licenses/LICENSE-2.0.txt> | Core Jackson processing abstractions (aka Streaming API), implementation for JSON |
| Jackson-databind-2.10.2.jar | <http://www.apache.org/licenses/LICENSE-2.0.txt> | General data-binding functionality for Jackson: works on core streaming API |
| Jakarta.annotation-api-1.3.5.jar | EPL 2.0: http://www.eclipse.org/legal/epl-2.0  GPL2 w/ CPE: https://www.gnu.org/software/classpath/license.html | Jakarta Annotations API |
| Jakarta.validation-api-2.0.2.jar | Apache License 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt | Jakarta Bean Validation API |
| Jboss-logging-3.4.1.Final.jar | Apache License, version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt | The JBoss Logging Framework |
| Jul-to-slf4j-1.7.30.jar | N/A | JUL to SLF4J bridge |
| Log4j-api-2.12.1.jar | <https://www.apache.org/licenses/LICENSE-2.0.txt> | The Apache Log4j API |
| Log4j-to-slf4j-2.12.1.jar | <https://www.apache.org/licenses/LICENSE-2.0.txt> | The Apache Log4j binding between Log4j 2 API and SLF4J |
| Logback-classic-1.2.3.jar | [http://www.eclipse.org/legal/epl-v10.html, http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html](http://www.eclipse.org/legal/epl-v10.html,%20http:/www.gnu.org/licenses/old-licenses/lgpl-2.1.html) | logback-classic module |
| Logback-core-1.2.3.jar | [http://www.eclipse.org/legal/epl-v10.html, http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html](http://www.eclipse.org/legal/epl-v10.html,%20http:/www.gnu.org/licenses/old-licenses/lgpl-2.1.html) | logback-core module |
| Mongo-java-driver-2.4.jar | The Apache Software License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt | Java Driver for MongoDB |
| Slf4j-api-1.7.30.jar | N/A | The slf4j API |
| Snakaeyaml-1.25.jar | Apache License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt | YAML 1.1 parser and emitter for Java |
| Spring-boot-2.2.4.RELEASE.jar | Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0 | Spring Boot |
| Spring-boot-starter-web-2.2.4.RELEASE.jar | Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0 | Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container |
| Spring-core-5.2.3.RELEASE.jar | Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0 | Spring Core |
| Spring-expression-5.2.3.RELEASE.jar | Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0 | Spring Expression Language (SpEL) |
| Spring-web-5.2.3.RELEASE.jar | Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0 | Spring Web |
| Spring-webmvc-5.2.3.RELEASE.jar | Apache License, Version 2.0: https://www.apache.org/licenses/LICENSE-2.0 | Spring Web MVC |
| Tomcat-embed-core-9.0.30.jar | Apache License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt | Core Tomcat implementation |
| Tomcat-embed-el-9.0.30.jar | Apache License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt | Core Tomcat implementation |
| Tomcat-embed-websocket-9.0.30.jar | Apache License, Version 2.0: http://www.apache.org/licenses/LICENSE-2.0.txt | Core Tomcat implementation |

## Analyze Results

Looking at the snapshot information of the dependency report, there are a total of 24 unique dependencies found. The severity level there is 1 low, 2 medium, 3 High, and 9 critical for a total of 15 vulnerable dependencies. In the table below is the 15 vulnerable dependencies listed with potential solutions. It is important to filter false positives since vulnerabilities may be found that are not relevant to the current code base. Removing false positives allows us to prioritize higher severity level vulnerabilities rather than spending time on the flagged false vulnerabilities. Suppressing false postiives can be done by using the HTML report and copying the code given by the suppression link and pasting it into the xml file.

The 15 Vulnerable Dependencies

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Severity** | **CVE ID** | **Risk/Solution** |
| Hibernate-validator-6.0.18.Final.jar | Medium | [**CVE-2020-10693**](https://nvd.nist.gov/vuln/detail/CVE-2020-10693) | Bug found in message interpolation processor allowing hackers to bypass input sanitation. Solution: Update to current version. |
| Jackson-databind-2.10.2.jar | High | [**CVE-2023-35116**](https://nvd.nist.gov/vuln/detail/CVE-2023-35116) | Allows attackers to cause a DoS attack that use crylic dependencies. Solution: Input validation and sterilize data. |
| Log4j-api-2.12.1.jar | Low | [**CVE-2021-44832**](https://nvd.nist.gov/vuln/detail/CVE-2021-44832) | Vulnerable to remote code execution (RCE). Solution: Limit JNDI data source names to java protocol. |
| Logback-classic-1.2.3.jar | High | [**CVE-2023-6378**](https://nvd.nist.gov/vuln/detail/CVE-2023-6378) | Serialization vulnerability allows attackers to send DoS attack. Solution: Implement deserialization security. |
| Logback-core-1.2.3.jar | High | [**CVE-2023-6378**](https://nvd.nist.gov/vuln/detail/CVE-2023-6378) | Serialization vulnerability allows attackers to send DoS attack. Solution: Implement deserialization security. |
| Mongo-java-driver-2.4.jar | Medium | N/A |  |
| Snakeyami-1.25.jar | Critical | [**CVE-2022-1471**](https://nvd.nist.gov/vuln/detail/CVE-2022-1471) | Deserializing can allow attckers to RCE attacks. Solution: Use SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. |
| Spring-boot-2.2.4.RELEASE.jar | Critical | [**CVE-2023-20883**](https://nvd.nist.gov/vuln/detail/CVE-2023-20883) | Allows DoS attack if Spring MVC is used with a reverse proxy cache. Solution: Upgrade to current version. |
| Spring-boot-starter-web-2.2.4.RELEASE.jar | Critical | [**CVE-2023-20863**](https://nvd.nist.gov/vuln/detail/CVE-2023-20863) | SpEL expression may cause DoS. Solution: Upgrade to most recent version. |
| Spring-core-5.2.3.RELEASE.jar | Critical | [**CVE-2023-20863**](https://nvd.nist.gov/vuln/detail/CVE-2023-20863) | SpEL expression may cause DoS. Solution: Upgrade to most recent version. |
| Spring-expression-5.2.3.RELEASE.jar | Critical | [**CVE-2023-20863**](https://nvd.nist.gov/vuln/detail/CVE-2023-20863) | SpEL expression may cause DoS. Solution: Upgrade to most recent version. |
| Spring-web-5.2.3.RELEASE.jar | Critical | [**CVE-2023-20863**](https://nvd.nist.gov/vuln/detail/CVE-2023-20863) | SpEL expression may cause DoS. Solution: Upgrade to most recent version. |
| Spring-webmvc-5.2.3.RELEASE.jar | Critical | [**CVE-2023-20863**](https://nvd.nist.gov/vuln/detail/CVE-2023-20863) | SpEL expression may cause DoS. Solution: Upgrade to most recent version. |
| Tomcat-embed-core-9.0.30.jar | Critical | [**CVE-2024-21733**](https://nvd.nist.gov/vuln/detail/CVE-2024-21733) | Error message containing sensitive information. Solution: Upgrade to version 8.5.64 onwards or 9.0.44 onwards |
| Tomcat-embed-websocket-9.0.30.jar | Critical | [**CVE-2024-21733**](https://nvd.nist.gov/vuln/detail/CVE-2024-21733) | Error message containing sensitive information. Solution: Upgrade to version 8.5.64 onwards or 9.0.44 onwards |