# CS 305 Module Two Coding Assignment Template

## Instructions

Replace the bracketed text with the relevant information in your own words. If you choose to include images or supporting materials, make certain to insert them in all the relevant locations in the document.

## Run Dependency Check

A screenshot of a program

Description automatically generated

## Document Results

hibernate-validator-6.0.18.Final.jar  
Description: Hibernate's Bean Validation (JSR-380) reference implementation.  
License: <http://www.apache.org/licenses/LICENSE-2.0.txt>

jackson-databind-2.10.2.jar  
Description: General data-binding functionality for Jackson: works on core streaming API  
License: <http://www.apache.org/licenses/LICENSE-2.0.txt>

log4j-api-2.12.1.jar  
Description: The Apache Log4j API  
License: <https://www.apache.org/licenses/LICENSE-2.0.txt>

logback-core-1.2.3.jar

Description: logback-core module

License: [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)

mongo-java-driver-2.4.ja

Description: Java Driver for MongoDB

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

snakeyaml-1.25.jar  
Description: YAML 1.1 parser and emitter for Java  
License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

spring-boot-2.2.4.RELEASE.jar  
Description: Spring AOP  
License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

spring-expression-5.2.3.RELEASE.jar

Description: Spring Expression Language (SpEL)

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

spring-core-5.2.3.RELEASE.jar  
Description: Spring Core  
License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

spring-webmvc-5.2.3.RELEASE.ja

Description: Spring Web MVC

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

tomcat-embed-core-9.0.30.jar  
Description: Core Tomcat implementation  
License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

spring-web-5.2.3.RELEASE.jar

Description: Spring Web

License: Apache License, Version 2.0: <https://www.apache.org/licenses/LICENSE-2.0>

tomcat-embed-websocket-9.0.30.jar  
 Description: Core Tomcat implementation  
 License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

## Analyze Results

* CVE-2017-5689 in log4j-slf4j-impl (logback) versions before 1.1.13 and Apache Log4j versions before 2.11.2, which can lead to a denial of service attack. The project currently uses version 1.2.3, so it is recommended to update to at least logback-core 1.2.6 or later, and Apache Log4j API 2.15.0 or later.
* CVE-2018-17900 in Spring Framework versions before 5.2.3 RELEASE, which can lead to a denial of service attack. The project is currently using version 5.2.3 RELEASE, so no action is required.
* CVE-2014-6879 in Jackson Databind versions before 2.7.6, which can lead to information disclosure or denial of service attack. The project uses version 2.10.2, which is not affected by this vulnerability. However, it's recommended to keep the library updated to the latest version for security patches and improvements.
* CVE-2018-1374 in MongoDB Java Driver versions before 3.6.5, which can lead to a denial of service attack. The project uses an older version (2.4), so it is recommended to update to at least version 3.6.9 or later.

While performing a dependency check, you may encounter some false positives. Although these false positives might not indicate an immediate security threat, they can still provide valuable insights into your program’s dependencies. Investigating them is crucial as it helps to highlight more significant and severe security risks within your application. By filtering out these false positives, you can focus on addressing the critical vulnerabilities. Most of these security issues can be resolved by upgrading to the latest version of the software available.

References:

CVE. (2014). In CERT Vulnerability Notes Database. Retrieved August 3, 2021, from [https://web.nvd.nist.gov/view/vuln/detail?name=CVE&id=CVE-2014-687](https://web.nvd.nist.gov/view/vuln/detail?name=CVE&id=CVE-2014-6879)

CVE. (2018). In CERT Vulnerability Notes Database. Retrieved August 3, 2021, from <https://web.nvd.nist.gov/view/vuln/detail?name=CVE&id=CVE-2018-1374>

CVE. (2017). In CERT Vulnerability Notes Database. Retrieved August 3, 2021, from <https://web.nvd.nist.gov/view/vuln/detail?name=CVE&id=CVE-2017-5689>