# 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.jar

**Description**: Java Driver for MongoDB

**License**: The Apache Software License, Version 2.0: <http://www.apache.org/licenses/LICENSE-2.0.txt>

* 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 Boot

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

* spring-boot-starter-web-2.2.4.RELEASE.jar

**Description**: Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container.

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

## Analyze Results

* **hibernate-validator-6.0.18.Final.jar**

**Summary**: A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if theywere valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls thatdevelopers may have put in place when handling user-controlled data in error messages.

* **jackson-databind-2.10.2.jar**

**Summary**: A flaw was found in FasterXML Jackson Databind, where it did not have entityexpansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity

* **log4j-api-2.12.1.jar**

**Summary**: Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.

* **logback-core-1.2.3.jar**

**Summary**: In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.

* **mongo-java-driver-2.4.jar**

**Summary**: Specific versions of the Java driver that support client-side field level encryption (CSFLE) fail to perform correct host name verification on the KMS server’s certificate. This vulnerability in combination with a privileged network position active MITM attack could result in interception of traffic between the Java driver and the KMS service rendering Field Level Encryption ineffective. This issue was discovered during internal testing and affects all versions of the Java driver that support CSFLE. The Java async, Scala, and reactive streams drivers are not impacted. This vulnerability does not impact driver traffic payloads with CSFLE-supported key services originating from applications residing inside the AWS, GCP, and Azure network fabrics due to compensating controls in these environments. This issue does not impact driver workloads that don’t use Field Level Encryption.

* **snakeyaml-1.25.jar**

**Summary**: SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. We recommend using SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. We recommend upgrading to version 2.0 and beyond.

* **spring-boot-2.2.4.RELEASE.jar**

**Summary**: \*\* UNSUPPORTED WHEN ASSIGNED \*\* spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer.

* **spring-boot-starter-web-2.2.4.RELEASE.jar**

**Summary**: \*\* UNSUPPORTED WHEN ASSIGNED \*\* spring-boot versions prior to version v2.2.11.RELEASE was vulnerable to temporary directory hijacking. This vulnerability impacted the org.springframework.boot.web.server.AbstractConfigurableWebServerFactory.createTempDir method. NOTE: This vulnerability only affects products and/or versions that are no longer supported by the maintainer.