# CS 305 Module Two Coding Assignment Template

Alex Surprenant

## Run Dependency Check

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Document Results

1. hibernate-validator-6.0.18.Final.jar
   * Description: Hibernate's Bean Validation (JSR-380) reference implementation.
2. jackson-databind-2.10.2.jar
   * Description: General data-binding functionality for Jackson: works on core streaming API
3. log4j-api-2.12.1.jar
   * Description: The Apache Log4j API
4. logback-core-1.2.3.jar
   * Description: logback-core module
5. mongo-java-driver-2.4.jar
   * Description: Java Driver for MongoDB
6. snakeyaml-1.25.jar
   * Description: YAML 1.1 parser and emitter for Java
7. spring-boot-2.2.4.RELEASE.jar
   * Description: Spring Boot
8. 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

1. spring-core-5.2.3.RELEASE.jar
   * Description: Spring Core
2. spring-expression-5.2.3.RELEASE.jar
   * Description: Spring Expression Language (SpEL)
3. spring-web-5.2.3.RELEASE.jar
   * Description: Spring Web
4. spring-webmvc-5.2.3.RELEASE.jar
   * Description: Spring Web MVC
5. tomcat-embed-core-9.0.30.jar
   * Description: Core Tomcat implementation
6. tomcat-embed-websocket-9.0.30.jar
   * Description: Core Tomcat implementation

## Analyze Results

1. A flaw was found that could allow a user to bypass a class by omitting a less than character and allows invalid expressions to be evaluated.
2. Flaw found in FasterXML Jackson Databind that allows vulnerability to externam entity attacks, possibly affecting data integrity
3. Improper validation of certificate, which could allow interception from a man-in-the-middle attack.
4. Vulnerability in logback receiver component which could allow an attacker to mount a denial-of-service attack.
5. Specific versions of the Java driver have a vulnerability that can allow intercepted traffic to bypass encryption.
6. SnakeYaml’s Constructor class does not restrict types which can be instantiated during deserialization. An attacker can gain remote access.
7. Older versions of springboot can be susceptible to security bypass.
8. Older versions of springboot can be susceptible to security bypass.
9. A spring MVC or WebFlux app running on Java Development Kit 9+ may be vulnerable to remote code execution.
10. A spring MVC or WebFlux app running on Java Development Kit 9+ may be vulnerable to remote code execution.
11. Pivital Spring Framework versions up to 5.3.16 can potentially be susceptible to remote code execution.
12. A spring MVC or WebFlux app running on Java Development Kit 9+ may be vulnerable to remote code execution.
13. Apache Tomcat can be exploited for remote code execution if made accessible to untrusted users.
14. Apache Tomcat can be exploited for remote code execution if made accessible to untrusted users.