# CS 305 Module Two Coding Assignment

## Run Dependency Check

A screenshot of a computer

Description automatically generated

## Document Results

* hibernate-validator-6.0.18.Final.jar - Hibernate's Bean Validation (JSR-380) reference implementation.
* jackson-databind-2.10.2.jar - General data-binding functionality for Jackson: works on core streaming API
* log4j-api-2.12.1.jar - The Apache Log4j API
* logback-core-1.2.3.jar - logback-core module
* mongo-java-driver-2.4.jar - Java Driver for MongoDB
* snakeyaml-1.25.jar - YAML 1.1 parser and emitter for Java
* spring-boot-2.2.4.RELEASE.jar - Spring Boot
* spring-boot-starter-web-2.2.4.RELEASE.jar - Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container
* spring-core-5.2.3.RELEASE.jar - Spring Core
* spring-web-5.2.3.RELEASE.jar - Spring Web
* spring-webmvc-5.2.3.RELEASE.jar - Spring Web MVC
* tomcat-embed-core-9.0.30.jar - Core Tomcat implementation
* tomcat-embed-websocket-9.0.30.jar - Core Tomcat implementation

## Analyze Results

False positives should be filtered out of a dependency-check tool as this helps to hide areas of smaller concern. This helps to highlight the dependencies more proon to higher risk vulnerabilities but should be noted that it might be beneficial to still check the area that posted a false positive just to make sure there still are no vulnerabilities later.

* **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 they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages. Update to latest version.
* **jackson-databind-2.10.2.jar**
  + Summary: jackson-databind 2.10.x through 2.12.x before 2.12.6 and 2.13.x before 2.13.1 allows attackers to cause a denial of service (2 GB transient heap usage per read) in uncommon situations involving JsonNode JDK serialization. Update to latest version.
* **log4j-api-2.12.1.jar**
  + Summary: Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.
* **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. Update to latest version.
* **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. Update to latest version.
* **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: In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache. Update to latest version.
* **spring-boot-starter-web-2.2.4.RELEASE.jar**
  + Summary: In Spring Boot versions 3.0.0 - 3.0.6, 2.7.0 - 2.7.11, 2.6.0 - 2.6.14, 2.5.0 - 2.5.14 and older unsupported versions, there is potential for a denial-of-service (DoS) attack if Spring MVC is used together with a reverse proxy cache. Update to latest version.
* **spring-core-5.2.3.RELEASE.jar**
  + Summary: In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition. Update to latest version.
* **spring-web-5.2.3.RELEASE.jar**
  + Summary: In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.
* **spring-webmvc-5.2.3.RELEASE.jar**
  + Summary: In spring framework versions prior to 5.2.24 release+ ,5.3.27+ and 6.0.8+ , it is possible for a user to provide a specially crafted SpEL expression that may cause a denial-of-service (DoS) condition.
* **tomcat-embed-core-9.0.30.jar**
  + Summary: Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issue.
* **tomcat-embed-websocket-9.0.30.jar**
  + Summary: Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issue.