# CS 305 Module Two Coding Assignment

Jason Kremhelmer

Southern New Hampshire University

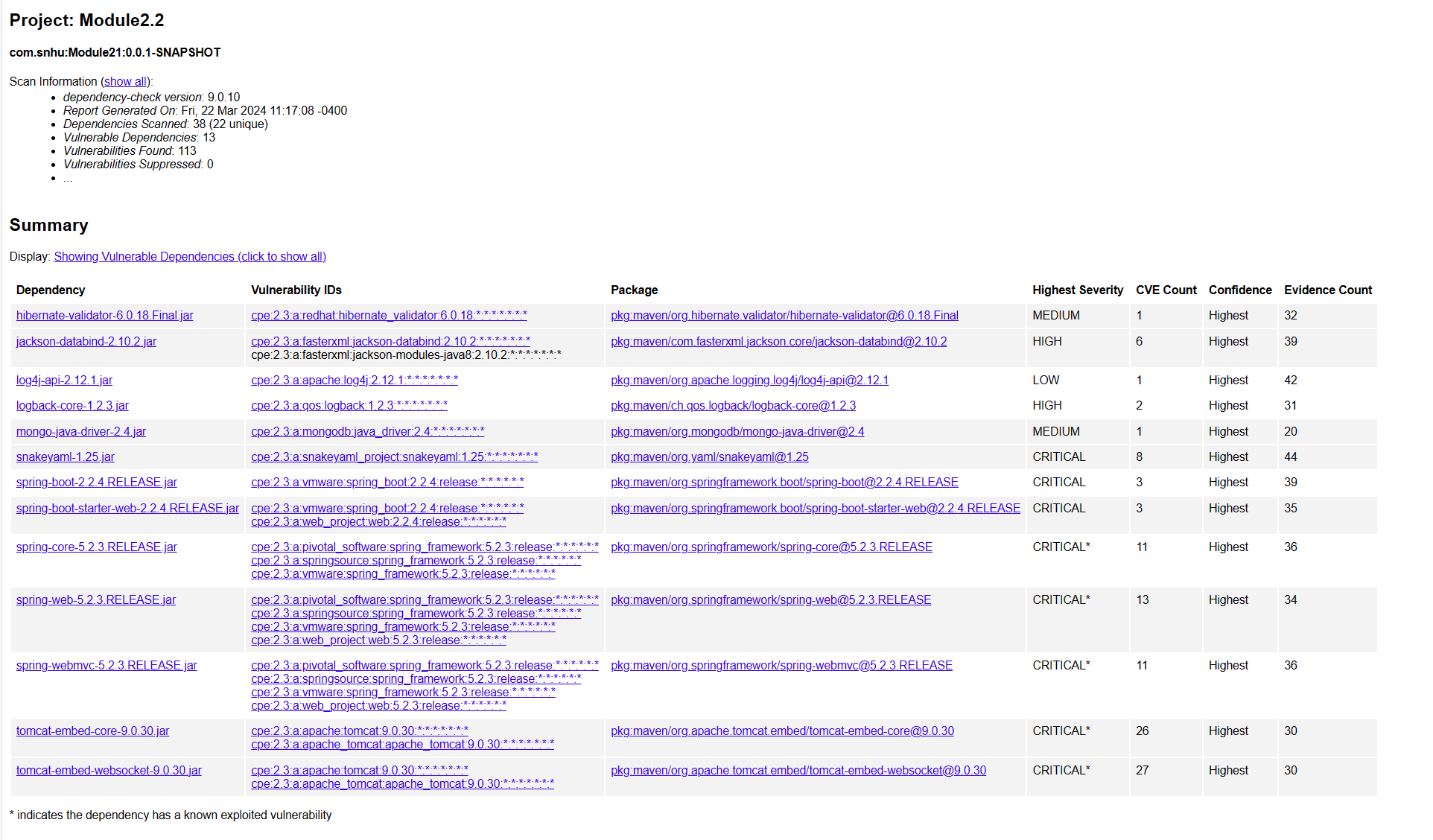
CS 305: Software Security

Dr. Sarah North

## 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



## Document Results

Results from dependency check:

Scan Information ([show less](file:///C:\Users\jkrem\OneDrive\Desktop\Jason%20School\CS305\Module%202\Module2.2\target\dependency-check-report.html)):

* *dependency-check version*: 9.0.10
* *Report Generated On*: Fri, 22 Mar 2024 11:17:08 -0400
* *Dependencies Scanned*: 38 (22 unique)
* *Vulnerable Dependencies*: 13
* *Vulnerabilities Found*: 113
* *Vulnerabilities Suppressed*: 0
* *NVD API Last Checked*: 2024-03-22T11:14:24-04
* *NVD API Last Modified*: 2024-03-22T14:15:10Z

Document Results o 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 o jackson-databind-2.10.2.jar](http://www.apache.org/licenses/LICENSE-2.0.txt%20o%20jackson-databind-2.10.2.jar%20)

Description: General data-binding functionality for Jackson: works on core streaming API License: [http://www.apache.org/licenses/LICENSE-2.0.txt o log4j-api-2.12.1.jar](http://www.apache.org/licenses/LICENSE-2.0.txt%20o%20log4j-api-2.12.1.jar%20)

Description: The Apache Log4j API License: [https://www.apache.org/licenses/LICENSE-2.0.txt o snakeyaml-1.25.jar](https://www.apache.org/licenses/LICENSE-2.0.txt%20o%20snakeyaml-1.25.jar%20)

Description: YAML 1.1 parser and emitter for Java License: Apache License, Version 2.0: [http://www.apache.org/licenses/LICENSE2.0.txt o spring-aop-5.2.3.RELEASE.jar](http://www.apache.org/licenses/LICENSE2.0.txt%20o%20spring-aop-5.2.3.RELEASE.jar%20)

Description: Spring AOP License: Apache License, Version 2.0: [https://www.apache.org/licenses/LICENSE2.0 spring-core-5.2.3.RELEASE.jar](https://www.apache.org/licenses/LICENSE2.0%20spring-core-5.2.3.RELEASE.jar%20)

Description: Spring Core License: Apache License, Version 2.0: [https://www.apache.org/licenses/LICENSE2.0 o tomcat-embed-core-9.0.30.jar](https://www.apache.org/licenses/LICENSE2.0%20o%20tomcat-embed-core-9.0.30.jar%20)

Description: Core Tomcat implementation License: Apache License, Version 2.0: [http://www.apache.org/licenses/LICENSE2.0.txt o tomcat-embed-websocket-9.0.30.jar](http://www.apache.org/licenses/LICENSE2.0.txt%20o%20tomcat-embed-websocket-9.0.30.jar%20)

Description: Core Tomcat implementation License: Apache License, Version 2.0: <http://www.apache.org/licenses/LICENSE2.0.txt>

## 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 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.

**jackson-databind-2.10.2.jar**

Summary: A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion 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-themiddle attack which could leak any log messages sent through that appender.

**snakeyaml-1.25.jar**

Summary: The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564.

**spring-aop-5.2.3.RELEASE.jar**

Summary: In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

**spring-core-5.2.3.RELEASE.jar**

Summary: In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0- 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.

**tomcat-embed-core-9.0.30.jar**

Summary: The fix for bug 63362 present in Apache Tomcat 10.1.0-M1 to 10.1.0-M5, 10.0.0-M1 to 10.0.11, 9.0.40 to 9.0.53 and 8.5.60 to 8.5.71 introduced a memory leak. The object introduced to collect metrics for HTTP upgrade connections was not released for WebSocket connections once the connection was closed. This created a memory leak that, over time, could lead to a denial of service via an OutOfMemoryError.

**tomcat-embed-websocket-9.0.30.jar**

Summary: The fix for bug 63362 present in Apache Tomcat 10.1.0-M1 to 10.1.0-M5, 10.0.0-M1 to 10.0.11, 9.0.40 to 9.0.53 and 8.5.60 to 8.5.71 introduced a memory leak. The object introduced to collect metrics for HTTP upgrade connections was not released for WebSocket connections once the connection was closed. This created a memory leak that, over time, could lead to a denial of service via an OutOfMemoryError.