### Southern New Hampshire University

2-2 Coding Assignment: Static Testing

David Vega

### Dr. Vivian Lyon

### CS-305 – Software Security

01/15/2023

# CS 305 Module Two Coding Assignment Template

## Run Dependency Check

Graphical user interface, text, application, email

Description automatically generated

## Document Results

Graphical user interface, text, application

Description automatically generated



(Project: Module2.2, 2023)

## Analyze Results

It is important to note that suppressing false positives will help to alleviate some of the tedious work of having to sift through an applications vulnerabilities. False positives create unnecessary work and suppressing them will allow you to focus on true vulnerabilities (Common Vulnerabilities and Exposure "CVE", 2023).

### spring-boot-2.2.4.RELEASE.jar

### The method within the spring-boot versions <2.2.11 that creates a working directory for embedded web servers is impacted. This directory stores files such as config files, and class files. If an attacker were to have permissions to write in this directory, they could compromise the application by assigning themselves elevated permissions (Common Vulnerabilities and Exposure "CVE", 2023).

**logback-core-1.2.3.jar**

This exploit would allow attackers with permmissions to inject code from LDAP servers. LDAP servers will typically store user credentials (Common Vulnerabilities and Exposure "CVE", 2023).

**log4j-api-2.12.1.jar**

This log file is basically a journal of activities for the application. This particular exploit would allow an attacker to inject malicious code using a JNDI Lookup pattern to extract data (Common Vulnerabilities and Exposure "CVE", 2023).

**snakeyaml-1.25.jar**

The exploit would allow user input that could potentially overwhelm the parser causing a DoS (“Denial of Service”) attack (Common Vulnerabilities and Exposure "CVE", 2023).

**jackson-databind-2.10.2.jar**

The exploit is meant to process deeply nested objects and array values to impact the Jackson data processor. This data processor is used to parse java code and return JSON (Common Vulnerabilities and Exposure "CVE", 2023).

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

During an upgrade to HTTP/2, the HTTP/1 protocol was never released. This exploit can use that to cause unnecessary consumption of resources resulting in a denial of service (Common Vulnerabilities and Exposure "CVE", 2023).

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

This exploit would essentially allow the attacker to inject malicious code into a constraint violation message by using EL expressions. When the constraint violation message is evaluated, it would cause the passed in code to be executed before the message was returned. Rather than concatenating variables with strings for these types of messages, string interpolation would be advised as it will mitigate arbitrary code from executing in a string literal (Common Vulnerabilities and Exposure "CVE", 2023).

**spring-web-5.2.3.RELEASE.jar**

**spring-beans-5.2.3.RELEASE.jar**

**spring-webmvc-5.2.3.RELEASE.jar**

**spring-context-5.2.3.RELEASE.jar**

**spring-expression-5.2.3.RELEASE.jar**

These exploits depends on a particular situation where the application is running from the web server Tomcat as a WAR deployment. The WAR file contains any and all files related to the web application (i.e. – html files, css, etc.) (Common Vulnerabilities and Exposure "CVE", 2023).

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

This exploit allows the attacker to use a Man in the Middle attack to intercept transmission between a client and KMS server. The client computer is able to perform client-side field level encryption within a version of mongodb. The KMS (Key management service) is used to create and control cryptographic keys used to protect your data (Common Vulnerabilities and Exposure "CVE", 2023).

# References

(2023, January 15). Retrieved from Common Vulnerabilities and Exposure "CVE": https://cve.mitre.org/cve/search\_cve\_list.html

*Project: Module2.2.* (2023, January 15). Retrieved from Dependency Check: file:///Users/davidvega/eclipse-workspace/Module2.1/target/dependency-check-report.html#l17\_dd386a02e40b915ab400a3bf9f586d2dc4c0852c