# CS 305 Module Two Coding Assignment: Alexis Prazak

## Run Dependency Check

A screenshot of a computer

Description automatically generated

## Document Results

Current vulnerable dependicies:

* hibernate validator
* jackson databind
* log4j
* log back
* mongodb
* snakeyaml
* springboot
* tomcat

A screenshot of a computer

Description automatically generated

## Analyze Results

Based on the above vulnerabilities I recommend a handful of important steps. Upgrade the tomcat, snakyaml, and spring frameworks to more current versions. To prevent DDOS attacks and malicious inputs set limits for resources, especially for unprivileged users. Work to prevent the unserialization of untrusted data. Taking these steps will help prevent users from performing unwanted actions and injecting malicious content into the software.

Below is a summary of known vulnerabilities. Remember that this list is not exhaustive and does not predict new issues. False positives have been filtered out to prevent the team from focusing on vulnerabilities that may not exist.

* hibernate validator
  + 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
  + 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.
* log4j

|  |  |
| --- | --- |
|  | * + 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. Fixed in Apache Log4j 2.12.3 and 2.13.1 |

* log back
  + 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.
  + A serialization vulnerability in logback receiver component part of logback version 1.4.11 allows an attacker to mount a Denial-Of-Service attack by sending poisoned data.
* mongodb
  + Sending specially crafted commands to a MongoDB Server may result in artificial log entries being generated or for log entries to be split. This issue affects MongoDB Server v3.6 versions prior to 3.6.20; MongoDB Server v4.0 versions prior to 4.0.21 and MongoDB Server v4.2 versions prior to 4.2.10.
* snakeyaml
  + 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.
* springboot
  + 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.
  + In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.
  + 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
  + In Spring Framework versions 5.3.0 - 5.3.10, 5.2.0 - 5.2.17, and older unsupported versions, it is possible for a user to provide malicious input to cause the insertion of additional log entries.
  + 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
  + Generation of Error Message Containing Sensitive Information vulnerability in Apache Tomcat.This issue affects Apache Tomcat: from 8.5.7 through 8.5.63, from 9.0.0-M11 through 9.0.43. Users are recommended to upgrade to version 8.5.64 onwards or 9.0.44 onwards, which contain a fix for the issue.
  + The simplified implementation of blocking reads and writes introduced in Tomcat 10 and back-ported to Tomcat 9.0.47 onwards exposed a long standing (but extremely hard to trigger) concurrency bug in Apache Tomcat 10.1.0 to 10.1.0-M12, 10.0.0-M1 to 10.0.18, 9.0.0-M1 to 9.0.60 and 8.5.0 to 8.5.77 that could cause client connections to share an Http11Processor instance resulting in responses, or part responses, to be received by the wrong client.
  + Apache Tomcat 8.5.0 to 8.5.63, 9.0.0-M1 to 9.0.43 and 10.0.0-M1 to 10.0.2 did not properly validate incoming TLS packets. When Tomcat was configured to use NIO+OpenSSL or NIO2+OpenSSL for TLS, a specially crafted packet could be used to trigger an infinite loop resulting in a denial of service.

1. **Resources**

MITRE. (n.d.). *Common Weakness Enumeration*. CWE. https://cwe.mitre.org/index.html

Long, J. (n.d.). *How to Read the Reports*. How to read the reports – dependency-check-maven. http://jeremylong.github.io/DependencyCheck/general/thereport.html