# CS 305 Module Two Coding Assignment Template

## Run Dependency CheckA screenshot of a computer AI-generated content may be incorrect.

## Document Results

|  |  |  |
| --- | --- | --- |
| [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l2_7fd00bcd87e14b6ba66279282ef15efa30dd2492) | Hibernate's Bean Validation (JSR-380) reference implementation. | CVE-2025-35036, CVE-2023-1932, CVE-2020-10693 |
| [jackson-core-2.10.2.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l4_73d4322a6bda684f676a2b5fe918361c4e5c7cca) | Core Jackson processing abstractions (aka Streaming API), implementation for JSON | CVE-2025-52999(OSSINDEX), CVE-2025-49128(OSSINDEX) |
| [jackson-databind-2.10.2.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l5_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | General data-binding functionality for Jackson: works on the core streaming API | CVE-2020-25649, CVE-2020-36518, CVE-2021-46877, CVE-2022-42003, , CVE-2022-42004, CVE-2023-35116 |
| [log4j-api-2.12.1.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l10_a55e6d987f50a515c9260b0451b4fa217dc539cb) | The Apache Log4j API | CVE-2020-9488 |
| [logback-classic-1.2.3.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l12_7c4f3c474fb2c041d8028740440937705ebb473a) | logback-classic module | CVE-2023-6378, CVE-2021-42550 |
| [logback-core-1.2.3.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l13_864344400c3d4d92dfeb0a305dc87d953677c03c) | logback-core module | CVE-2023-6378, CVE-2021-42550, CVE-2024-12798, CVE-2024-12801 |
| [mongo-java-driver-2.4.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l14_f9bbd594f981d60f6a5b2d1ec3463b772355b64f) | Java Driver for MongoDB | CVE-2021-20328(OSSINDEX) |
| [snakeyaml-1.25.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l16_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) | YAML 1.1 parser and emitter for Java | [CVE-2022-1471](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1471), [CVE-2017-18640](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-18640) , [CVE-2022-25857](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-25857), [CVE-2022-38749](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38749), [CVE-2022-38751](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38751) , [CVE-2022-38752](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38752) , [CVE-2022-41854](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-41854), [CVE-2022-38750](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-38750) |
| [spring-aop-5.2.3.RELEASE.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l17_9cdd9a1dd636331767fffcc7fe49a7bb00e7b34b) | Spring AOP | [CVE-2022-22965](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965)  , [CVE-2024-22259](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22259), [CVE-2021-22118](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118), [CVE-2020-5421](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421), [CVE-2022-22950](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950), [CVE-2022-22971](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22971), [CVE-2023-20861](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861), [CVE-2023-20863](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863), [CVE-2022-22968](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968), [CVE-2022-22970](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22970) , [CVE-2021-22060](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060), [CVE-2021-22096](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096) |
| [spring-boot-2.2.4.RELEASE.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l18_225a4fd31156c254e3bb92adb42ee8c6de812714) | Spring Boot | [CVE-2023-20873](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20873), [CVE-2022-27772](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772), [CVE-2023-20883](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20883) |
| [spring-boot-starter-web-2.2.4.RELEASE.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l19_ec75d01d212b5229c16d872fb127744c0ed46ed8) | Starter for building web, including RESTful applications using Spring MVC. Uses Tomcat as the default embedded container | [CVE-2023-20873](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20873) , [CVE-2022-27772](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27772) , [CVE-2023-20883](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20883) |
| [spring-context-5.2.3.RELEASE.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l20_7750c95c96c7a1885c8b1b503ba915bc33ca579a) | Spring Context | [CVE-2022-22965](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965), [CVE-2024-22259](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22259), [CVE-2021-22118](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118), [CVE-2020-5421](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421), [CVE-2022-22950](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950), [CVE-2022-22971](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22971), [CVE-2023-20861](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861), [CVE-2023-20863](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863), [CVE-2022-22968](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968), [CVE-2022-22970](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22970), [CVE-2021-22060](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060), [CVE-2021-22096](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096), CVE-2025-22233 (OSSINDEX) |
| [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l21_3734223040040e8c3fecd5faa3ae8a1ed6da146b) | Spring Core | [CVE-2022-22965](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965), CVE-2025-41242 (OSSINDEX), [CVE-2024-22259](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22259) , [CVE-2021-22118](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118), [CVE-2020-5421](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421), [CVE-2022-22950](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950) , [CVE-2022-22971](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22971) , [CVE-2023-20861](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861), [CVE-2023-20863](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863), [CVE-2022-22968](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968), [CVE-2022-22970](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22970), [CVE-2021-22060](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060), [CVE-2021-22096](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096) |
| [spring-expression-5.2.3.RELEASE.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l22_d0c6bb10758805b2153c589686b8045554bfac2d) | Spring Expression Language (SpEL) | [CVE-2022-22965](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965) , [CVE-2024-22259](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22259) [CVE-2021-22118](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118)  [CVE-2020-5421](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421) [CVE-2022-22950](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950) [CVE-2022-22971](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22971) [CV[CVE-2023-20863](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863) E-2023-20861](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861) VE-2024-38808 (OSSINDEX) [CVE-2022-22968](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968) [CVE-2022-22970](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22970) [CVE-2021-22060](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060)  [CVE-2021-22096](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096) |
| [spring-web-5.2.3.RELEASE.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l23_dd386a02e40b915ab400a3bf9f586d2dc4c0852c) | Spring Web | [CVE-2016-1000027](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000027)  [CVE-2022-22965](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965)  CVE-2024-38809 (OSSINDEX, CVE-2024-22243 (OSSINDEX CVE-2024-22262 (OSSINDEX)  [CVE-2024-22259](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22259) [CVE-2021-22118](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118) CVE-2025-41234 (OSSINDEX) CVE-2024-38828 (OSSINDEX) [CVE-2020-5421](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421) [CVE-2022-22950](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950)  [CVE-2022-22971](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22971)  [CVE-2023-20861](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861)  [CVE-2023-20863](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863) [CVE-2022-22968](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968)  [CVE-2022-22970](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22970) [CVE-2021-22060](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060)  [CVE-2021-22096](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096) |
| [spring-webmvc-5.2.3.RELEASE.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l24_745a62502023d2496b565b7fe102bb1ee229d6b7) | Spring Web MVC | [CVE-2022-22965](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22965)  CVE-2024-38816 (OSSINDEX) [CVE-2024-22259](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-22259)  [CVE-2021-22118](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22118)  [CVE-2020-5421](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-5421) [CVE-2022-22950](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22950) [CVE-2022-22971](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22971)  [CVE-2023-20861](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20861)  [CVE-2023-20863](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-20863)  [CVE-2022-22968](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22968)  [CVE-2022-22970](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22970)  [CVE-2021-22060](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22060)  [CVE-2021-22096](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22096) |
| [tomcat-embed-core-9.0.30.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l25_ad32909314fe2ba02cec036434c0addd19bcc580) | Core Tomcat implementation | [CVE-2020-1938](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1938)  [CVE-2024-50379](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-50379)  [CVE-2024-52316](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-52316)  [CVE-2024-56337](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-56337) [CVE-2025-24813](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-24813) [CVE-2025-31651](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-31651) [CVE-2025-49124](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-49124) [CVE-2020-11996](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11996) [CVE-2020-13934](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13934) [CVE-2020-13935](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13935) [CVE-2020-17527](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17527) [CVE-2021-25122](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25122) [CVE-2021-41079](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41079)  [CVE-2022-29885](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29885) [CVE-2022-42252](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42252)  [CVE-2023-44487](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-44487) [CVE-2023-46589](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-46589) [CVE-2024-24549](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-24549)  [CVE-2024-34750](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-34750) [CVE-2024-38286](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38286)  [CVE-2025-48988](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-48988)  [CVE-2025-48989](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-48989)  [CVE-2025-49125](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-49125)  [CVE-2025-52520](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-52520)  [CVE-2025-53506](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-53506) [CVE-2025-46701](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-46701) [CVE-2020-9484](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9484) [CVE-2021-25329](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25329)   [CVE-2021-30640](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30640) [CVE-2025-55668](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-55668) [CVE-2024-23672](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-23672) [CVE-2022-34305](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-34305)   [CVE-2023-41080](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-41080) [CVE-2021-24122](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24122) [CVE-2021-33037](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33037) [CVE-2023-42795](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-42795)  [CVE-2023-45648](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-45648) [CVE-2024-21733](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-21733) [CVE-2024-54677](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-54677) [CVE-2019-17569](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569)  [CVE-2020-1935](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1935) ...[CVE-2020-13943](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13943) [CVE-2023-28708](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-28708) [CVE-2021-43980](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43980) |
| [tomcat-embed-websocket-9.0.30.jar](file:///C:\Users\gag48\OneDrive\Desktop\Avryes%20School\Module%20two%20coding%20assign%20unzip\Module2.2\target\dependency-check-report.html#l27_33157f6bc5bfd03380ebb5ac476db0600a04168d) | Core Tomcat implementation | [CVE-2020-1938](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1938) [CVE-2024-50379](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-50379) [CVE-2024-52316](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-52316)  [CVE-2024-56337](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-56337) [CVE-2025-24813](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-24813) [CVE-2025-31651](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-31651)  [CVE-2025-49124](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-49124) [CVE-2020-8022](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8022) [CVE-2020-11996](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11996) [CVE-2020-13934](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13934) [CVE-2020-13935](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13935) [CVE-2020-17527](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17527) [CVE-2021-25122](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25122)  [CVE-2021-41079](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41079)  [CVE-2022-29885](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29885) [CVE-2022-42252](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-42252) [CVE-2023-44487](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-44487) [CVE-2023-46589](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-46589) [CVE-2024-24549](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-24549)  [CVE-2024-34750](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-34750)  [CVE-2024-38286](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-38286) [CVE-2025-48988](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-48988) [CVE-2025-48989](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-48989) [CVE-2025-49125](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-49125) [CVE-2025-52434](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-52434)  [CVE-2025-52520](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-52520)  [CVE-2025-53506](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-53506)  [CVE-2025-46701](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-46701) [CVE-2020-9484](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9484) [CVE-2021-25329](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25329)  [CVE-2021-30640](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30640) [CVE-2025-55668](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2025-55668) [CVE-2024-23672](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-23672) [CVE-2022-34305](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-34305)  [CVE-2023-41080](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-41080)  [CVE-2021-24122](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24122) [CVE-2021-33037](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33037)  [CVE-2023-42795](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-42795) [CVE-2023-45648](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-45648)  [CVE-2024-21733](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-21733) [CVE-2024-54677](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2024-54677) [CVE-2019-17569](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17569) [CVE-2020-1935](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1935)  [CVE-2020-13943](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13943) [CVE-2023-28708](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2023-28708) [CVE-2021-43980](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43980) |

## Analyze Results

Above are recorded all the dependencies and the codes that link the dependencies to their issues. The issues can be summarized by going down the list as follows.

Hibernate Validators before 6.2.0 – 7.0.0 may allow users to input something they are not supposed to, allowing hackers to be able also insert bad things to access sensitive data. To fix, you could update the Hibernate Validators.

Jackson-core could throw a stack overflow error if an input file is too deeply nested in versions before 2.15.0. To fix, users should avoid parsing the input file.

Flaws were found in FasterXML Jackson databind. It didn’t have entity expansion, with attacks occurring in the XML external entity, and data integrity could be breached. It can also allow denial of service. This could be caused due to improper restriction of XML External entity reference.

Improper validation of the certificate with a host mismatch in the Apache Log4j SMTP appender. This could all be a man-in-the-middle attack with leaks of logs. This was fixed in a later update.

A serialization vulnerability in the logback receiver part of logback v. 1.4.11. Allows for attacker to mount a denial of service attack by sending poisoned data. Destruction of untrusted data could fix poisoned data.

Improper certificate validation, which can cause the Java driver to fail the encryption of the host name verification on the KMS server certificate.

SnakeYaml's constructor class does not restrict the types that can be instantiated during deserialization. This could lead to a remote attack. Use this when parsing untrusted content.

Spring MVC. Webflux applications running on JDK 9+ are vulnerable to remote code execution via data vindication. Fix by updating.

Spring Boot version is out of date, update it.

Apache Tomcat treats Jserv protocol connections having higher trust. Fixed by applying updates.

So, after breaking down all the dependencies, we can note that most issues can be fixed by updating all plugins, such as Hibernate Validators, Jackson core, Spring, and Apache. Once these plugins are up to date, any existing known weaknesses can be patched. Some issues are programmer-based based where inputting improper applications, leaving holes without covering the previous code, or improper validation allows for hackers to steal information from users and customers. It is important to look into the dependencies to make sure that all information is secure and allows for privacy from user logs to information. Other hacking can be done by not properly checking untrusted information, which in turn can allow a hacker to infiltrate the code, which can be fixed by using known sources and making sure that the application or plug-in is safe to use. Overall, by being careful, up to date, and thorough, the programmer can keep their code relatively safe. False positives should be filtered because they show something that does not need to be fixed within the code. This happens when there are no rule violations, but it still proceeds to print one. This causes the programmer to take more time trying to fix non-existent problems. The same goes the other way with false negatives, being worse than the false positive, this is because a missed mistake can cause larger issues down the line, and possible information loss.

**Citations**

Bellairs, R. (n.d.). *What Is A False Positive? How to Identify False Postives and False Negatives*. Perforce Software. https://www.perforce.com/blog/qac/what-are-false-positives-and-false-negatives

‌

*dependency-check – How To Read The Reports*. (n.d.). Jeremylong.github.io. <https://jeremylong.github.io/DependencyCheck/general/thereport.html>

**‌**