****

# Artemis Financial Vulnerability Assessment Report

Table of Contents

[Document Revision History 3](#_Toc32574607)

[Client 3](#_Toc32574608)

[Instructions 3](#_Toc32574609)

[Developer 4](#_Toc32574610)

[1. Interpreting Client Needs 4](#_Toc32574611)

[2. Areas of Security 4](#_Toc32574612)

[3. Manual Review 4](#_Toc32574613)

[4. Static Testing 4](#_Toc32574614)

[5. Mitigation Plan 4](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **[Date]** | **[Your name]** |  |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In the report, identify your findings of security vulnerabilities and provide recommendations for the next steps to remedy the issues you have found.

* Respond to the five steps outlined below and include your findings.
* Respond using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
* Refer to the Project One Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Will McLaughlin

## Interpreting Client Needs

1. What is the value of secure communications to the company?
2. Does the company make any international transactions?
3. Are there governmental restrictions about secure communications to consider?
4. What external threats might be present now and in the immediate future?
5. What are the modernization requirements that you must consider? For example:
   1. The role of open-source libraries
   2. Evolving web application technologies

Artemis Financial is a firm which uses internal and external priority, important information to deal with their clients, which makes secure communication an absolute priority for Artemis Financial. As Artemis is a financial firm, transactions should be international and domestic in nature. There are no laws on secure communications between others, while there are some in receiving government communications, but secure communications should be an absolute priority nonetheless, as a leaking of use communications can result in hefty fines from the government. External threats that face Artemis now, and in the immediate future may include things like data leaks, hacks, and security breakdowns/ bugs that lead to vulnerabilities in communications. Artemis handles biometrics, account information, and SSN’s, so the requirements that need to be considered are things like constant updates in their libraries, and security, as well as secure servers and outside cloud storage usage from big and secure companies. Two factor authentication, biometric authentication, as well as secure password enforcement and encryption must be used to ensure security.

## Areas of Security

Potential vulnerabilities in Artemis:

Input Validation – Input string validation must be used to stop SQL injections or potential bugs in the code that allow other injections, or incorrect input that grants admin access.

Cryptography – Cryptography is a necessary component of security in things like transfers, especially internationally. Data needs to be secured through encryption to comply to international and national regulations.

Code Error – Code error handling is a must in the Artemis system, as it is used to prevent bad input and input validation, as well as prevent admin attempts that are malicious.

API – API will be used as it is needed to generate responses for the users on the Artemis site. I recommend using multiple third-party security API handlers to ensure that the data accessed and used to respond to users is correct, and not internally accessible from the outside through malicious parties.

Code Quality – The code quality of the site and security features is one of the most important parts to ensure security. Running extensive tests on the code to determine issues and what is necessary to address these issues is necessary. This will prevent possible data leaks, and allow security by preventing users from taking data they are not authorized to.

## Manual Review

In the DocData class, the method read\_document is vulnerable to SQL injections, as it accepts key and value for parameters. The code does not have any restrictions or parameters on the input before it uses them.

In the DocData class the code does not get secure database connection through DriverManager.getConnection, using things like SSL to communicate.

The DocData class also does not contain any error handling.

No API is used throughout the program, as the POST method is used which allows for exploits.

There is no data encryption through the code, which is necessary.

In the POM.XML file, there is no Apache Validator, which ensures there is no input validation.

## Static Testing

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| [bcprov-jdk15on-1.46.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l2_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) | [cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Abouncycastle&cpe_product=cpe%3A%2F%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api&cpe_version=cpe%3A%2F%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api%3A1.46) | [pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46](https://ossindex.sonatype.org/component/pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | HIGH | 17 | Highest | 37 |
| [spring-boot-2.2.4.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l3_225a4fd31156c254e3bb92adb42ee8c6de812714) | [cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_boot&cpe_version=cpe%3A%2F%3Avmware%3Aspring_boot%3A2.2.4) | [pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | CRITICAL | 3 | Highest | 32 |
| [logback-core-1.2.3.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l4_864344400c3d4d92dfeb0a305dc87d953677c03c) | [cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aqos&cpe_product=cpe%3A%2F%3Aqos%3Alogback&cpe_version=cpe%3A%2F%3Aqos%3Alogback%3A1.2.3) | [pkg:maven/ch.qos.logback/logback-core@1.2.3](https://ossindex.sonatype.org/component/pkg:maven/ch.qos.logback/logback-core@1.2.3?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | MEDIUM | 1 | Highest | 32 |
| [log4j-api-2.12.1.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l5_a55e6d987f50a515c9260b0451b4fa217dc539cb) | [cpe:2.3:a:apache:log4j:2.12.1:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Alog4j&cpe_version=cpe%3A%2F%3Aapache%3Alog4j%3A2.12.1) | [pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1](https://ossindex.sonatype.org/component/pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | CRITICAL | 5 | Highest | 46 |
| [snakeyaml-1.25.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l8_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) | [cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Asnakeyaml_project&cpe_product=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml&cpe_version=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml%3A1.25) [cpe:2.3:a:yaml\_project:yaml:1.25:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Ayaml_project&cpe_product=cpe%3A%2F%3Ayaml_project%3Ayaml&cpe_version=cpe%3A%2F%3Ayaml_project%3Ayaml%3A1.25) | [pkg:maven/org.yaml/snakeyaml@1.25](https://ossindex.sonatype.org/component/pkg:maven/org.yaml/snakeyaml@1.25?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | CRITICAL | 10 | Highest | 28 |
| [jackson-databind-2.10.2.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l9_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | [cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Afasterxml&cpe_product=cpe%3A%2F%3Afasterxml%3Ajackson-databind&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson-databind%3A2.10.2) | [pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | HIGH | 6 | Highest | 39 |
| [tomcat-embed-core-9.0.30.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l13_ad32909314fe2ba02cec036434c0addd19bcc580) | [cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Atomcat&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A9.0.30) [cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_tomcat&cpe_product=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat&cpe_version=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat%3A9.0.30) | [pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | CRITICAL | 25 | Highest | 39 |
| [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l16_7fd00bcd87e14b6ba66279282ef15efa30dd2492) | [cpe:2.3:a:redhat:hibernate\_validator:6.0.18:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aredhat&cpe_product=cpe%3A%2F%3Aredhat%3Ahibernate_validator&cpe_version=cpe%3A%2F%3Aredhat%3Ahibernate_validator%3A6.0.18) | [pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final](https://ossindex.sonatype.org/component/pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | MEDIUM | 1 | Highest | 36 |
| [spring-web-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l19_dd386a02e40b915ab400a3bf9f586d2dc4c0852c) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) | [pkg:maven/org.springframework/spring-web@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-web@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | HIGH | 4 | Highest | 28 |
| [spring-beans-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l20_0250c8c641433dc06b1b44e4563fa08a2fbf8954) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) | [pkg:maven/org.springframework/spring-beans@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-beans@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | HIGH | 1 | Highest | 28 |
| [spring-webmvc-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l21_745a62502023d2496b565b7fe102bb1ee229d6b7) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) | [pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | MEDIUM | 1 | Highest | 30 |
| [spring-context-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l22_7750c95c96c7a1885c8b1b503ba915bc33ca579a) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) | [pkg:maven/org.springframework/spring-context@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-context@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | MEDIUM | 1 | Highest | 28 |
| [spring-expression-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l23_d0c6bb10758805b2153c589686b8045554bfac2d) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) | [pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=5.3.0) | MEDIUM | 3 | Highest | 30 |

[bcprov-jdk15on-1.46.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l2_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) : This vulnerability allows the use of ECB mode, which an unsafe mode, which has been removed. Security fixes recommend upgrading Maven.

[spring-boot-2.2.4.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l3_225a4fd31156c254e3bb92adb42ee8c6de812714): This vulnerability allows for DoS or denial of service attacks in Spring Boot versions 3 – 3.0.6, 2.7.0 – 2.7.11, 2.60 – 2.6.14, 2.5.0 – 2.5.14 and older. Security fixes recommend updating to current Spring version.

[logback-core-1.2.3.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l4_864344400c3d4d92dfeb0a305dc87d953677c03c): This vulnerability allows for an attacker with required privileges to edit configuration files to create malicious configuration, which would allow the execution of arbitrary code in logback version 1.2.7 and earlier. Security fixes recommend updating to current Apache version.

[log4j-api-2.12.1.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l5_a55e6d987f50a515c9260b0451b4fa217dc539cb): This vulnerability allows for improper validation of certificate with a host mismatch in Apache Log4j SMTP appender. This vulnerability could allow for an SMPTS connection to be intercepted by a man in the middle attack, which could possibly leak log messages. Security fixes recommend upgrading to version 2.13.2 or higher.

[snakeyaml-1.25.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l8_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421): This vulnerability is exploited through SnakeYaml’s constructor class, which does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution. Security fixes recommend using SnakeYal’s SafeConstructor when parsing, and upgrading to version 2.0 or greater.

[jackson-databind-2.10.2.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l9_0528de95f198afafbcfb0c09d2e43b6e0ea663ec): This vulnerability through Jackson-databind 2.15.2 allows attackers to cause a DoS attack through a crafted object that uses cyclical dependencies. Security fixes include upgrading, however, the vendor has a perspective that this report is invalid, as the ability of constructing a cyclic data structure and serializing it cannot be done by an external attacker.

[tomcat-embed-core-9.0.30.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l13_ad32909314fe2ba02cec036434c0addd19bcc580): Apache Tomcat 10.0.0-M1 to 10.0.6, 9.0.0.M1 to 9.0.46 and 8.5.0 to 8.5.66 did not correctly parse the HTTP transfer-encoding request header in some circumstances leading to the possibility to request smuggling when used with a reverse proxy. Security fixes include upgrading to Apache Tomcat 10.0.6 or greater.

[hibernate-validator-6.0.18.Final.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l16_7fd00bcd87e14b6ba66279282ef15efa30dd2492): This vulnerability includes a bug found in version 6.1.2Final, where the bug in message interpolation processor enable invalid EL expressions to be evaluated as if they were valid. The flaw allows attackers to bypass input sanitation. Security fixes include upgrading to version 6.0.20 or higher.

[spring-web-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l19_dd386a02e40b915ab400a3bf9f586d2dc4c0852c): 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 CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter. Security fixes include upgrading to current version.

This last vulnerability encompasses [spring-beans-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l20_0250c8c641433dc06b1b44e4563fa08a2fbf8954) , [spring-webmvc-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l21_745a62502023d2496b565b7fe102bb1ee229d6b7), [spring-context-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l22_7750c95c96c7a1885c8b1b503ba915bc33ca579a), and [spring-expression-5.2.3.RELEASE.jar](file:///C:\Users\willm\OneDrive\Desktop\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l23_d0c6bb10758805b2153c589686b8045554bfac2d)

## Mitigation Plan

To mitigate the vulnerabilities found through the Maven testing, upgrading to the current versions of their own unique software’s will fix most of the issues in the tests. The one different solution is the SnakeYaml vulnerability, which will have to be fixed by changing the version and restricting its aliases for security.