

# 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]** | **Arnold Limberg** | **Security Audit** |

## Client



Developer

Arnold Limberg

## Interpreting Client Needs

Artemis is a financial consulting firm that works with extremely private information, such as financial information about an individual. It is imperative to conduct a security audit of company operations and highlight the importance of secure connections in preventing the tampering or eavesdropping of customer data.

Key Considerations:

A. Ensuring the integrity of financial data and the confidentiality of clients requires secure communications. Data transmissions that are encrypted and use protocols like HTTPS, SSL, and TLS are essential.

B. Artemis, as a global company, manages transactions around the world, so it must adhere to secure transaction protocols and international security regulations, such as GDPR, for clients in Europe.

C. Adherence to legal statutes is vital, as they impact the methods of storing, processing, and transmitting data. Adhering to international standards and protocols with regards to international law for security and privacy must be a priority.

D.Global operations risk global attacks: malware, SQL injections, phishing, and other techniques could pose a threat. It's imperative to keep ahead of these problems since cybercriminals find the banking sector appealing.

E. Taking into account Artemis's goal to update, it is imperative to include safe cloud technologies, strong authentication protocols, and a reliance on safe open-source libraries. It is important to give priority to contemporary web application frameworks that promote security by design..

## Areas of Security

Design review: To find any possible weak areas in the application, a detailed analysis of its design is required. It is crucial to make sure that the architecture can provide safe, scalable solutions, given Artemis Financial's emphasis on modernization.

Validating input: Prior to processing is crucial for safeguarding against injection attacks such as SQL injection and cross-site scripting (XSS). Strict input validation procedures are essential, given the financial data that Artemis manages.

APIs: Artemis may use APIs for a variety of financial data processing functions, so secure API interactions are essential. It is crucial to make sure APIs are safe against illegal access and data leakage.

Cryptography: Strong encryption procedures for data at rest and in transit are a must given Artemis's requirement for secure conversations and transactions.

Client/Server Communication: It is essential that client apps and servers communicate securely. This entails successfully authenticating and authorizing users, in addition to encrypting data in transit.

Code Error and Exception Handling: Handling errors and exceptions correctly helps stop confidential data from leaking and offers a clear debugging path without jeopardizing security.

Secure Coding Practices and Code Quality: Following secure coding guidelines can drastically lower vulnerabilities. This entails incorporating security into the development process, doing frequent code reviews, and utilizing well-established frameworks.

## Manual Review

GreetingController.java: Vulnerability to SpEL Injection

Method: greeting; File: GreetingController.java

The procedure parses and evaluates expressions straight from user input (name argument) using SpEL. Because of this, there is a danger of SpEL injection, which might enable an attacker to create input that would run arbitrary expressions in the context of the program.

Vulnerability: Array Index Out of Bounds

GreetingController.java is the file.

Method: number

This method accesses items of a statically created array using a user-supplied index (the id path variable) without first validating the index. If the index is outside the bounds of the array, this may result in an ArrayIndexOutOfBoundsException, which could lead to a denial of service or enable unwanted behavior.

Lack of Error Handling: This applies to all files, but it is particularly important to perform thorough error handling for cases when exceptions such as ArrayIndexOutOfBoundsException can be thrown (GreetingController.java). In order to prevent sensitive information about the application's internal operations or file structure from being revealed, custom error handlers should catch exceptions and provide generic error messages.

## Static Testing

## **Summary**

Display: [Showing Vulnerable Dependencies (click to show all)](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Dependency** | **Vulnerability IDs** | **Package** | **Highest Severity** | **CVE Count** | **Confidence** | **Evidence Count** |
| [hibernate-validator-6.0.18.Final.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l2_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=9.0.10) | MEDIUM | 1 | Highest | 32 |
| [jackson-databind-2.10.2.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l4_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) cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | [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=9.0.10) | HIGH | 6 | Highest | 39 |
| [log4j-api-2.12.1.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l9_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=9.0.10) | LOW | 1 | Highest | 42 |
| [logback-core-1.2.3.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l11_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=9.0.10) | HIGH | 2 | Highest | 31 |
| [mongo-java-driver-2.4.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l12_f9bbd594f981d60f6a5b2d1ec3463b772355b64f) | [cpe:2.3:a:mongodb:java\_driver:2.4:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Amongodb&cpe_product=cpe%3A%2F%3Amongodb%3Ajava_driver&cpe_version=cpe%3A%2F%3Amongodb%3Ajava_driver%3A2.4) | [pkg:maven/org.mongodb/mongo-java-driver@2.4](https://ossindex.sonatype.org/component/pkg:maven/org.mongodb/mongo-java-driver@2.4?utm_source=dependency-check&utm_medium=integration&utm_content=9.0.10) | MEDIUM | 1 | Highest | 20 |
| [snakeyaml-1.25.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l14_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) | [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=9.0.10) | CRITICAL | 8 | Highest | 44 |
| [spring-boot-2.2.4.RELEASE.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l15_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=9.0.10) | CRITICAL | 3 | Highest | 39 |
| [spring-boot-starter-web-2.2.4.RELEASE.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l16_ec75d01d212b5229c16d872fb127744c0ed46ed8) | [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) [cpe:2.3:a:web\_project:web: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%3Aweb_project&cpe_product=cpe%3A%2F%3Aweb_project%3Aweb&cpe_version=cpe%3A%2F%3Aweb_project%3Aweb%3A2.2.4) | [pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=9.0.10) | CRITICAL | 3 | Highest | 35 |
| [spring-core-5.2.3.RELEASE.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l17_3734223040040e8c3fecd5faa3ae8a1ed6da146b) | [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) [cpe:2.3:a:vmware: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%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3) | [pkg:maven/org.springframework/spring-core@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-core@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=9.0.10) | CRITICAL\* | 11 | Highest | 36 |
| [spring-web-5.2.3.RELEASE.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l18_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) [cpe:2.3:a:vmware: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%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3) [cpe:2.3:a:web\_project:web: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%3Aweb_project&cpe_product=cpe%3A%2F%3Aweb_project%3Aweb&cpe_version=cpe%3A%2F%3Aweb_project%3Aweb%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=9.0.10) | CRITICAL\* | 13 | Highest | 34 |
| [spring-webmvc-5.2.3.RELEASE.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l19_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) [cpe:2.3:a:vmware: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%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3) [cpe:2.3:a:web\_project:web: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%3Aweb_project&cpe_product=cpe%3A%2F%3Aweb_project%3Aweb&cpe_version=cpe%3A%2F%3Aweb_project%3Aweb%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=9.0.10) | CRITICAL\* | 11 | Highest | 36 |
| [tomcat-embed-core-9.0.30.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l20_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=9.0.10) | CRITICAL\* | 26 | Highest | 30 |
| [tomcat-embed-websocket-9.0.30.jar](file:///C:/Program%20Files/ONLYOFFICE/DesktopEditors/editors/web-apps/apps/documenteditor/main/index.html?_dc=0&lang=en-US&frameEditorId=placeholder&isForm=false&parentOrigin=file://&fileType=docx#l22_33157f6bc5bfd03380ebb5ac476db0600a04168d) | [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-websocket@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=9.0.10) | CRITICAL\* | 27 | Highest | 30 |

\* indicates the dependency has a known exploited vulnerability

Key Vulnerabilities and Recommendations

**A. Spring Framework Related Vulnerabilities (CRITICAL)**

Affected Components: spring-boot-2.2.4.RELEASE.jar, spring-boot-starter-web-2.2.4.RELEASE.jar, spring-core-5.2.3.RELEASE.jar, spring-web-5.2.3.RELEASE.jar, spring-webmvc-5.2.3.RELEASE.jar

Implications: These vulnerabilities can lead to remote code execution, unauthorized access, and information disclosure.

Recommendation: Upgrade Spring Boot and Spring Framework dependencies to the latest versions that have addressed these vulnerabilities. Ensure thorough testing to confirm compatibility and functionality.

**B. Apache Tomcat Vulnerabilities (CRITICAL)**

Affected Components: tomcat-embed-core-9.0.30.jar, tomcat-embed-websocket-9.0.30.jar

Implications: Vulnerabilities in Tomcat can lead to remote code execution, denial of service, and information disclosure.

Recommendation: Upgrade to the latest version of Tomcat that has patched these vulnerabilities. Review Tomcat configuration settings to ensure they are secure and follow best practices.

**C. Jackson Databind Vulnerability (HIGH)**

Affected Component: jackson-databind-2.10.2.jar

Implications: Deserialization of untrusted data can lead to remote code execution.

Recommendation: Update to the latest secure version of Jackson Databind. Implement safe usage patterns to avoid deserialization of untrusted data.

**D. Logback-core Vulnerability (HIGH)**

Affected Component: logback-core-1.2.3.jar

Implications: Potential remote code execution via malicious log patterns or log data.

Recommendation: Upgrade to a version of Logback that addresses these issues. Review logging configuration for potential exposure.

**E. SnakeYAML Vulnerability (CRITICAL)**

Affected Component: snakeyaml-1.25.jar

Implications: Can lead to code execution through crafted YAML inputs.

Recommendation: Upgrade SnakeYAML to a secure version. Validate and sanitize YAML input when possible.

## Mitigation Plan

The following mitigation plan identifies critical vulnerabilities found through manual review and static testing and implements strategic activities to fully resolve each problem in order to secure the Artemis Financial online application.

GreetingController.java may have vulnerabilities related to Array Index Out of Bounds and SpEL injection, according to the manual review. The plan employs strict input validation and sanitation procedures, especially in dynamic expression evaluation contexts like SpEL, to prevent the evaluation of untrusted user inputs. Furthermore, putting in place checks to make sure user-supplied indices are within allowable boundaries would reduce the possibility of array index out-of-bounds exceptions, improving the stability and security of the program.

The static analysis found serious flaws in a number of dependencies, such as Apache Tomcat, Spring Framework components, Jackson Databind, Logback-core, and SnakeYAML. These dependencies need to be updated right away and carefully. Taking into account the most recent security advisories and recommendations, it is imperative to update these dependencies to their most secure versions.

An essential part of the mitigation plan is to improve error handling even more to stop end users from learning about critical application internals. The program can prevent unintended information leaks that could assist attackers by offering thorough logging for internal use and generic error messages for client-facing issues.

A company culture of secure coding practices, along with continuous monitoring of dependency vulnerabilities, is paramount. Integrating tools like OWASP Dependency-Check into the CI/CD pipeline aids in sure development.

**References**

*CVE - Search CVE list*. (n.d.). <https://cve.mitre.org/cve/search_cve_list.html>

*dependency-check-maven – Usage*. (n.d.). https://jeremylong.github.io/DependencyCheck/dependency-check-maven/index.html