****

# 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** | **10 November 2023** | **Austin Adams** |  |

## 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

Austin Adams

## Interpreting Client Needs

Since Artemis is a financial service company they would be a very valuable target meaning security should be an extremely high priority for them. This emphasis on security will help to protect their reputation, assets and privacy of their clients. Since a financial firm can transfer funds between two different nations they must make sure that they comply with all of the different standards and laws present within all nations that they are operating in. Government regulations such as the Electronic Communications Privacy Act means that the government is able to subpoena different forms of digital communications like email and direct messages.

## Areas of Security

Input validation is very much needed to help regulate the user inputs to prevent any unwanted issues arising from an incorrect input. This should be used in conjunction with encapsulation in order to make sure that sensitive data is protected and that any malicious users aren’t able to modify or gain access to any data structures and cause unwanted changes. Since all data flows ought to be encrypted, cryptography should also be taken into account. It is recommended that all databases and data transport use RSA-2048 strength. Because laws about cryptography differ by operating country, it is important to verify the nature and capabilities of encryption.

## Manual Review

It was discovered during the static testing that the POM.xml needs to be upgraded to a more recent Maven release. Certain CVEs will go unnoticed if outdated static cases are used. There are some setters and getters available in the code, an example being the Greeting class that are going unused by other classes such as the GreetingController. The myDateTime class has a few poorly coded methods which are incomplete. The DocData class also has username and passwords unencrypted making them easily readable. These should be encrypted even for testing purposes.

## Static Testing

|  |  |  |  |
| --- | --- | --- | --- |
| Dependency | Vulnerability Code | Description | Mitigation |
| [bcprov-jdk15on-1.46.jar](file:///C:\Users\BTH\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\rest-service\target\dependency-check-report.html#l1_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) | cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.46:  cpe:2.3:a:bouncycastle:bouncy\_castle\_crypto\_package:1.46  cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytographyapi:1.46  cpe:2.3:a:bouncycastle:the\_bouncy\_castle\_crypto\_package\_for\_java:1.46 | The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms | Upgrade Bouncy castle to version 1.60 or higher |
| tomcat-embed-websocket-9.0.30.jar | cpe:2.3:a:apache:tomcat:9.0.30  cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30 | Core Tomcat implementation | Update Tomcat to the newest version |
| tomcat-embed-core-9.0.30.jar | cpe:2.3:a:apache:tomcat:9.0.30  cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30 | Core Tomcat implementation | Upgrade to newest Tomcat version |
| spring-core-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release  cpe:2.3:a:springsource:spring\_framework:5.2.3:release  cpe:2.3:a:vmware:spring\_framework:5.2.3:release  cpe:2.3:a:vmware:springsource\_spring\_framework:5.2.3:release | Spring Core | Upgrade to the latest version of Spring |
| spring-aop-5.2.3.RELEASE.jar | cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release  cpe:2.3:a:springsource:spring\_framework:5.2.3:release  cpe:2.3:a:vmware:spring\_framework:5.2.3:release | Spring AOP | Upgrade to the latest version of Spring |
| spring-boot-2.2.4.RELEASE.jar | cpe:2.3:a:vmware:spring\_boot:2.2.4:release | Spring Boot | Only affects unsupported versions. Upgrade. |
| snakeyaml-1.25.jar | cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25 | YAML 1.1 parser and emitter for Java | Allows entity expansion. Upgrade. |
| jackson-databind-2.10.2.jar | cpe:2.3:a:fasterxml:jackson-databind:2.10.2  cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2 | General data-binding functionality for Jackson: works on core streaming API | Data integrity concerns. Upgrade to latest release. |
| logback-core-1.2.3.jar | cpe:2.3:a:qos:logback:1.2.3 | logback-core module | Arbitrary code execution. Upgrade to the latest version |
| hibernate-validator-6.0.18.Final.jar | cpe:2.3:a:redhat:hibernate\_validator:6.0.18 | Hibernate's Bean Validation (JSR-380) reference implementation | Input validation bypass issue. Upgrade to the latest version. |

## Mitigation Plan

The first thing that needs to be done is updating all of the libraries and recompiling the code. After that is completed input validation and error messages need to be incorporated and then tested to make sure they are functioning as desired. All changes made to the code should be followed with a code review in case the developer overlooked anything that could possibly be seen as a risk or security threat.