****

# 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** | **09/22/2022** | **Quincy Hodge** |  |

## 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

Quincy Hodge

## Interpreting Client Needs

The value of secure communications for Artemis Financial hinges upon the fact that their institution primarily manages an individual’s sensitive data and financial goals. Secure communications are important to Artemis Financial because if there were to be a data breach due to the lack of security, the organization would loss customer trust, and that leads to a loss of revenue. After reviewing the information and code provided, there is no specific mention of international transactions, but it would be best to error on the side of caution and assume there are international transactions until, the answer can be ascertained. Yes, there are government restrictions about secure communications to consider, one of the locations these restrictions can be found is [www.ffiec.gov](http://www.ffiec.gov), here they have guidance on electronic financial services and consumer compliance. Some of the cyber threats that may be present now or in the immediate future for Artemis Financial are unencrypted data, malware, third party services that are not secure, data manipulation and spoofing threats. Modernization requirements are integral to the continued success of Artemis Financial, one of the first modernizations that should take place is how users access their data, the organization should make sure they are using multifactor authentication, this makes illegal entry into the secure communications more difficult for a hacker. Scalability of the environment should also be considered when modernizing the application, this ensure that as the Artemis Financial continues to grow and expand the environment will be able to grow and expand with the company.

## Areas of Security

1. API – API security is needed because there will be a RESTful web API used in the is software for this organization. API security is important due to the connections with interior and exterior services and data. If the API were to be hacked there is a high probability of a data breach and leak.
2. Cryptography – Cryptography is a foundation of a modern security system. Cryptography is used to protect privacy and data, and because there will be APIs used, cryptography will be important to keep all the information secure.
3. Client/Server – The client/server interaction is part of the front-line defense of the application, when it comes to user identification and authentication, if this is left unsecured the rest of the app has little chance of being secure. For secure communications it is important to make sure the correct HTTP requests are made and constructed in a secure manner.

## Manual Review

1. Input validation is not leveraged in the application, which leaves a gap for hackers to attack.
2. There could be a vulnerability in the CRUDController.java file because there are objects exposed. Even though there is CRUD, there do not seem to be any Post, Get, Update, or Delete functions along with there not being any HTTPS functions to secure the interactions.

## Static Testing

1. Dependency: bcprov-jdk15on-1.46.jar
2. Description: The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms. This jar contains JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.7.
3. Recommendation: There was no recommendation provided
4. Dependency: hibernate-validator-6.0.18.Final.jar
5. Description: Hibernate's Bean Validation (JSR-380) reference implementation.
6. Recommendation: Update fixed issue
7. Dependency: jackson-core-2.10.2.jar
8. Description: Core Jackson processing abstractions (aka Streaming API), implementation for JSON
9. Recommendation: Update fixed issue
10. Dependency: jackson-databind-2.10.2.jar
11. Description: General data-binding functionality for Jackson: works on core streaming API
12. Recommendation: Update fixed issue
13. Dependency: log4j-api-2.12.1.jar
14. Description: 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
15. Recommendation: Upgrade to version 2.14.2 will resolve this issue
16. Dependency: snakeyaml-1.25.jar
17. Description: YAML 1.1 parser and emitter for Java
18. Recommendation: Update fixed issue
19. Dependency: spring-boot-2.2.4.RELEASE.jar
20. Description: Spring Boot
21. Recommendation: Update fixed issue
22. Dependency: spring-core-5.2.3.RELEASE.jar
23. Description: Spring Core
24. Recommendation: Update fixed issue
25. Dependency: spring-web-5.2.3.RELEASE.jar
26. Description: Spring Web
27. Recommendation: Update fixed issue
28. Dependency: tomcat-embed-core-9.0.30.jar
29. Description: Core Tomcat implementation
30. Recommendation: Update released to fix issue
31. Dependency: tomcat-embed-websocket-9.0.30.jar
32. Description: Core Tomcat implementation
33. Recommendation: Update fixed issue

## Mitigation Plan

Most of the issues have been fixed updates that have taken place. There are a few other issues that have updates available, that have not been update and that would fix those issues. For the CRUDcontroller, it would be best to add secure https calls and get, post, delete and updates to add security to the API calls.