****

# 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** | **11/10/23** | **Evan Scarborough** |  |

## 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

Evan Scarborough

## Interpreting Client Needs

Secure communications are critical for Artemis Financial’s operations because they deal with sensitive client data such as savings and retirement account information. This information is highly valuable to criminals and other bad actors, and Artemis Financial’s business depends heavily upon their ability to protect and secure this data. Due to the nature of this information, Artemis Financial must also maintain compliance with certain governmental regulations; failure to do so may affect their ability to do business in the United States.

As such, the platform built for the company should be very well-secured. Relevant government regulations relating to the processing and storage of sensitive customer information must be adhered to. In addition to meeting client requirements, proactive measures should be taken to guarantee the security of the delivered application.

## Areas of Security

Relevant areas of security include:

* APIs: Current infrastructure in place at Artemis Financial uses RESTful APIs. The security of these APIs and the callers and endpoints associated with them is paramount.
* Cryptography: Government regulations stipulate that data containing certain types of sensitive information must be encrypted. These regulations must be regarded as a minimum for ensuring the security of the application.
* Client/Server: The application will need a backend to store data and a frontend to request and display it, thus a secure client/server architecture, using authorization/authentication for the former and database encryption for the latter, satisfies requirements.
* Code Error: Error handling should be graceful and display messages to the user that do not betray unnecessary information about the internal workings of the application – this is information that could, in the worst case, lead to sensitive user data being compromised.

## Manual Review

* Account info can be shown without any authentication or authorization of the user (customer.java)
* Deposits to accounts can be made without any information being collected (besides the deposit amount) or validated (customer.java)
* Stack traces are directly printed in the currently implemented error handling, providing an easy way for bad actors to discover details about the application’s internal structure (DocData.java)
* There is no authentication scheme for users.
* User information is not encrypted.

## Static Testing

cpe:2.3:a:apache:log4j : Improper validation of certificate – Requires Apache update.

cpe:2.3:a:apache:tomcat : Did not correctly parse the HTTP transfer-encoding request header – Update Apache Tomcat.

cpe:2.3:a:bouncycastle:the\_bouncy\_castle\_crypto\_package\_for\_java : Vulnerability to code injection – Update BouncyCastle.

cpe:2.3:a:springsource:spring\_framework:5.2.3:release : RFD defense vulnerability – Update Spring.

cpe:2.3:a:redhat:hibernate\_validator:6.0.18 : Hibernate Validator flaw – Update Hibernate Validator.

## Mitigation Plan

Action list:

1. Update all dependencies for the current Artemis Financial application.
2. Implement a user authentication/authorization scheme using a username and password.
3. Implement encryption for storage and transmission of sensitive user data.
4. Securely make API requests.