****

# 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** | **9/14/2023** | **Joshua Hunter** |  |

## 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

Joshua Hunter

## Interpreting Client Needs

a.) What is the value of secure communications to the company?

b.) Does the company make any international transactions?

c.) Are there governmental restrictions about secure communications to consider?

d.) What external threats might be present now and in the immediate future?

e.) What are the modernization requirements that you must consider? For example:

I.) The role of open-source libraries

II). Evolving web application technologies

Since this company is dealing with finances, investments, savings, retirement, and insurance. The value of secure communications is extremely important to keep people’s money safe. The company does make international transactions I would assume given that they’re coming to global rain, and if it is global, it is everywhere. Governments worldwide impose various restrictions on secure communications; however, the specific rules and their stringency vary from country to country. Some external threats may be people trying to get their data or steal information from their clients. In addition to open-source libraries and evolving web technologies, several other factors should be considered when modernizing, these factors can include things like cloud security, user awareness, and many other factors.

## Areas of Security

API’s – this controls the information that is accessible to outside sources.

Code Quality – controls quality of code and secureness of code.

Input Validation – used to validate an account owners information to make sure it’s them.

Code Error – This will show where there’s issues in the code that need improvement and to be fixed.

Cryptography – This would make everything encrypted to ensure safety and information protection.

## Manual Review

While manual reviewing I came across several issues, there is cryptographic issues meaning the application is vulnerable to timing attacks, there is an issue where people can bypass sanitation, I don’t see that it has HTTPS there’s something that can leak any log messages, this application is vulnerable to Denial of service attacks, and a plethora of other things upon manually reviewing this information.

## Static Testing

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Mitigation Plan

After reviewing manually and seeing the results from the static testing I believe the company needs an entire overhaul. All their systems need to be updated, everything needs to be verified from the ground up, there needs to be a constant check of code quality and user awareness. There needs to be more encryption, more ways to protect client’s information. I believe the best fix would be to start from scratch with a different team all together and really put some thought into the quality of work they’re putting out.