****

# 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** | **11/13/2022** | **Gregory Greene** | **Initial Report** |

## 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

Gregory Greene

## Interpreting Client Needs

As a financial institution Artemis Financial should value security and privacy above all else. Artemis Financial will store client personal data as well as financial data which is a common target for cyber-attacks. Secure communications are a high priority, as well as adherence to governmental regulations and any international laws that may need to be considered. As a financial institution the external threats that will remain constant are attacks seeking personal or a company’s financial information. Two quick implementations to be made are Two Factor authentication to support secure logins, and communication must happen through HTTPS to help protect client data.

## Areas of Security

The areas of security to be focused on are Code Errors, APIs, Input Validation, and Secure Coding. APIs are used through the systems RESTful API which works with input validation as the input must be validated and secure. Secure coding and Code errors are important when creating data systems or structures, as well as when reviewing bugs. Any bugs or errors encountered should be handled through a secure server.

## Manual Review

From the code the following errors were found:

* Input requests are not being validated (security problem)
* Service is not using HTTPS to protect sensitive information
* No authentication for verification (Implement 2FA)
* CRUDController class is sending business name as a request parameter (security problem)

## Static Testing

Graphical user interface, text, application, Teams

Description automatically generated

## Mitigation Plan

After reviewing the dependency check I feel the biggest impact to current and potential future errors can be made through implementing 2FA and HTTPS. Additionally, all dependencies need to be updated continuously to the current version, many dependencies were not up to date leaving security flaws unpatched. 2FA being implemented will allow for additional security for the user’s and make outside access difficult to obtain. HTTPS implementation will allow for secure communication and protect user/client information.