****

# 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** | **[Date]** | **[Your name]** |  |

## 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

Alvin Negron

## Interpreting Client Needs

The company needs their communication to be very secure since they want all their communication to be confidential and be safe from hackers. The company works with companies all over the world, so they will have a lot of international transactions. We will also need to consider any governmental restrictions when it comes to secure communications. Having a secure program from external threats will always be a top priority, either now or in the future. When thinking about modernization requirements and having a secure program, we should stray away from open-source libraries since these sources can be reused and are open to be used by anyone. We should investigate more secure and close web technologies.

## Areas of Security

There are some areas of security that we need to consider when completing the program.

* Input Validation – We need to check input validation so that whenever a customer is login into their account to communicate with the company, they can’t be hacked by someone else.
* API’s – Since we are using a RESTful, we need to verify that when an API is created that there is no unexpected access to the system.
* Cryptography – We should secure that proper cryptography is used to protect the customers data and ours.
* Client/Server – Every company that is directly connected to their clients should have some form of client/server security so that proper certificates are being used.
* Code Error – Any kind of program or code needs to be checked for any errors, we need to check that everything is working exactly how we want it to.
* Encapsulation – If any data is being accessed from our system, we need to make sure that it is being accessed correctly and not messing up our database.

## Manual Review

Our pom.xml file has an outdated version, we need to upgrade to the latest version.

## Static Testing

[Insert text.]

## Mitigation Plan

Upgrade the outdated version into the latest version present.