****

# 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** | **03/15/2023** | **Anthony Mink** |  |

## 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

Anthony Mink

## Interpreting Client Needs

**What is the value of secure communications to the company?**

Secure communications are essential to the business because they safeguard sensitive data and information against unwanted access. It also preserves the confidentiality, integrity, and availability of the company’s data.

**Does the company make any international transactions?**

They do not mention specifically in the scenario if they make any international transactions, but I assume that a financial company would, to grow their business. In this case General data protection regulation and Payment card industry data security standard would take affect in their business.

**Are there governmental restrictions about secure communications to consider?**

Depending on the location of the company governmental limits may exist such as, encryption legislation or surveillance regulations.

**What external threats might be present now and in the immediate future?**

Cyber attacks against the company may exist now or in the future. To give a few examples phishing, network intrusions, ransomware, and malware injections.

**What are the modernization requirements that you must consider?**

The usage of open-source libraries may bring new vulnerabilities. Also, developing web application technologies, may make it necessary to update security measures.

## Areas of Security

*Input Validation:* All inputs into the web application that will processed in the code need to be validated to prevent cyberattacks such as, DDoS, and malware injection.

*API’s*: Since the company is using a RESTful API web application it is imperative that these transactions are handle carefully. This would require authentication from users and well as proper coding practices of the API format.

*Cryptography:* There will be financial information involved so the information being sent from the client and server needs to be encrypted.

*Code Error*: The code of the web application needs to be checked and maintained for security breaches from outside sources, especially because we are using an API.

## Manual Review

I could not figure out how to get this all downloaded and use the right apps.

## Static Testing

I could not figure out how to get this all downloaded and use the right apps.

## Mitigation Plan

I could not figure out how to get this all downloaded and use the right apps.

IF there is a video tutorial instead of the word document that is 8 versions behind in updates that would really help.

Sorry for turning this project in late I really just could not figure it out.