****

# Artemis Financial Vulnerability Assessment Report

# Reynaldo Ortiz

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** | **11/9/2023** | **Reynaldo Ortiz** |  |

## 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

[Insert your name here.]

## Interpreting Client Needs

We need to establish what requirements the client is requesting to determine any potential attack and or threats that can be related to the type of program to establish any security requirements for the project. Several subjects need to be considered regarding how companies protect themselves against threats.

* How the company values its secure communication
* Any Federal and State requirements for secure data
* Is the company involved in any transaction other than local, for example, international transactions?
* Any new requirements that need to be considered
* The identification of any threats in the past, present, and future.

Due to the type of business the client conducts, it is safe and wise to consider that it is susceptible to data that will be tempting to any outsider. Artemis Financial deals with financial plans, including savings, retirement, investments, and insurance, making their client’s data highly secure. This data needs to be protected from any current and future threats. Therefore, they need not only to protect their client's information but the company’s information as well. Several recommendations can be implemented to prevent false access from external hackers, such as 2-way authentication.

## Areas of Security

We can use VAPFD to help identify all areas of security that could be relevant to the company’s program. However, we need to be clear and explain in detail to the client the reason we are taking this type of approach to protecting their data, and why it is important due to the sensitive data they save. This will include using any structured code that will prevent intruders from accessing their business database.

## Manual Review

Since there is a need to identify any vulnerability in the system or the code, it is recommended to be inspected for errors manually. This could mean that any request not being properly validated by the system allows outside intrusion since sensitive data will be shared within the program; the use of HTTPS is crucial, using any form of verification, explicitly using the 2-way authentication format.

## Static Testing

Run a Static Test on the company’s software application to identify all code security vulnerabilities. Ensure that the test report is recorded and verified. Include the following: The names of the known vulnerabilities, the description of the vulnerable code, and the recommended solution by the report.

## Mitigation Plan

After the results of the test have been identified and carefully reviewed, the next part will be establishing the steps to take to remedy the security vulnerability. this means that before all this happens, we need to ensure that all sensitive data from the company is secure from any outsider access.