****

# 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** | **11/9/2022** | **Alexander Garcia** |  |

## 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

Alexander Garcia

## Interpreting Client Needs

The client is asking us to evaluate any possible breaches in security or areas where there are threats. Security is very important to this client as they are dealing with the finances of their own clients and are also having their systems accessible online. It does not appear to specify in the prompt whether or not the company is operating in USA only or is worldwide, however since they do investment and insurance, I am going to assume they are specialized to USA. Many of the services they offer are regulated by government, such as investing and insurance. Many types of attacks can be present for this kind of organization including DOS attacks, data leaks, or remote code execution. It is very important for this type of software to be actively maintained and actively try to find any security breaches or points of weakness, especially as technology improves and brute force attacks become more relevant as hardware becomes more potent.

## Areas of Security

With such a big project you would expect lots of areas for security concern. Input validation will always be a concern with any project that takes in user inputs as prompts and will therefore be a security concern here. Although having an API that is secure is important to any system working online, however, it was addressed in the prompt that the client is using REST which is already a secure API, so I do not think there is a security concern there for this project. Encryption will definitely be a high concern for this project as the company will be handling a large amount of personal data that could cause large amount of harm if it was exposed. Cryptography will need to be implemented not only for client data stored by the company but also any data being transferred to and from the servers to the client-side website. This also plays into having secure client server interactions, which will be needed for this project, however for this kind of project it will likely host the entire application on the server so there won’t need to be a security concern regarding distributed a system. Secure error handling will also need to be implemented and handled as this project is possibly going to be working within many of the different systems the client is involved in, such as investing and retirement. Having secure code practices and patterns will be very important in this kind of project so that there isn’t any exploitable code.

## Manual Review

Upon initial review of the code a few major problems jump out at me. Firstly, it appears that the is no use of any encryption or decryption when getting the user data from the SQL program that is holding it. The next biggest thing I noticed is that there does not appear to be any input verification when reaching out to the SQL server or anywhere else, which can lead to injection attacks where the contents of the data table can be accessed and stolen. The last big issue I noticed was that although for data retrieval there was exception handling, exception handling was lacking from any other functions, which can lead to many problems including any small error coming up completely bringing down the application. Some other small problems I noticed include a lack of proper code documentation for many parts of the code base. Although there were some comments much of the project was lacking proper documentation. Another small problem for security can arise from the customer class having the account balance not be private which leaves it open to being set directly rather than having to be set by a function.

## Static Testing

Graphical user interface, application

Description automatically generated

Some of the major vulnerabilities found in the dependencies include: vulnerability to hijacking, allowing arbitrary code to be executed from LDAP servers, vulnerable to remote code execution, vulnerability to DOS attacks, allowing smuggling attacks. Some of the lesser vulnerabilities include allowing invalid expressions to be used, using old versions that are not supported, having options in the dependencies which can break if set incorrectly. For the majority of these a possible solution can be to not use the functionality which has the vulnerabilities and using other functions to accomplish those tasks. For some of the simpler things it can be solved by updating the dependencies and making sure to keep up to date.

## Mitigation Plan

Firstly, the code base needs a face lift to include fixes to many of the vulnerabilities needed. I would suggest that someone go through and add TODO’s and FIXME’s where necessary to address the previously mentioned vulnerabilities. The next step should be to update all dependencies to current versions and rerun the dependency tests. At which point any vulnerabilities remaining will need to be addressed with the solution that best fits this project.