****

# 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** | **[5-19-2023]** | **[Ethan Menchaca]** | **The purpose of this document is to identify potential security threats to Artemis Financial and to propose counters to these threats.** |

## 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

[Ethan Menchaca]

## Interpreting Client Needs

1. What is the value of secure communications to the company?
   * + Seeing that Artemis financial deals with very private and very sensitive data such as financial information and other personal data, it is paramount that the company focuses on developing secure communication. Without secure communication, the information entrusted to Artemis financial could be susceptible to hackers, which would result in a compromise which would be detrimental to their clientele. Since the premise of the business is to customize financial plans based on an individual’s specific needs, it is safe to assume that the client and the company will be in constant communication, and if this communication is not protected every piece of information shared during an exchange could be snagged by malicious hackers.
2. Does the company make any international transactions?
   * + Yes. Upon opening the XAResource.class in lines 33-37 an explanation to DTP(distributed transaction processing) is given:

The XA interface defines the contract between a Resource Manager

\* and a Transaction Manager in a distributed transaction processing

\* (DTP) environment. A JDBC driver or a JMS provider implements

\* this interface to support the association between a global transaction

\* and a database or message service connection.

This implies that global transactions will be made.

1. Are there governmental restrictions about secure communications to consider?
   * + In the United States of America, federal laws are notoriously bad at protecting its citizens private data online, whilst the government concurrently has some of the most invasive surveillance laws in the entire world. Excluding the government, there is one act which stands out which addresses the misuse of data collection and addresses the need for secure communications. The Federal Trade Commission act regulates unfair or deceptive commercial practices. The FTC is the primary federal regulator in the privacy area and brings enforcement actions against companies. This includes failing to comply with posted privacy policies and failing to adequately protect personal information. For Artemis Financial, this would be important to note, especially if the company is promising a secure platform for users to work with.
2. What external threats might be present now and in the immediate future?
   * + There are many external threats present now and which will continue to be present. Below is a list of common attacks and how they are implemented:
     + SQL injection-it is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. When an SQL injection is successful, it allows an attacker to get access to information they wouldn’t previously have been able to have access to.
     + Social engineering- This is a very common attack, and it doesn’t involve coding in any form. The main goal of social engineering is to convince a trusted user who has access to Artemis Financial as an admin or other authoritative position to give up valuable information to a malicious hacker, by means of manipulation and deceit. Often times, the hacker will pose as an authority figure or a trustworthy person and convince the trusted user to give them access. The specific attack which one poses as someone they are not is called a phishing attack, and is very common.

## Areas of Security

* + - Input Validation- Any time a program requires input, it is important to implement some form of input validation. In line 12 of the CRUDcontroller class, it allows input to be passed into a string parameter.
    - API- This aspect of security is a given, considering that the application will be run in a web environment. Any time differing applications or programs interact with one another, an API is essential to ensuring safe communication between the two. Controlling which data can be accepted into the program is an essential part of the API, and an essential part of Artemis security.
    - Cryptography- As stated earlier, the potential for Artemis security to do business overseas makes cryptography essential, and since Artemis financial will be in constant contact with their clients is all the more reason for it.
    - Secure coding- Ensuring that code doesn’t have any bugs is key to making a secure application.

## Manual Review

[Upon my review of the application code base, I identified some spots which presented vulnerabilities. They are as follows. In the greeting controller class, there is input which is passed through as a string, but no sort of input validation exists for this input. ]

## Static Testing

[]

## Mitigation Plan

[Insert text.]