****

# CS 305 Project One

**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** | **01-18-2022** | **Jamiya Ennis** |  |

## Client



## Instructions

Deliver this completed vulnerability assessment report, identifying your findings of security vulnerabilities and articulating recommendations for next steps to remedy the issues you have found.

Respond to the five steps outlined below and include your findings. Replace the bracketed text on all pages with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

## Developer

Jamiya Ennis

## 1. Interpreting Client Needs

Determine your client’s needs and potential threats and attacks associated with their application and software security requirements. Consider the following regarding how companies protect against external threats based on the scenario information:

* What is the value of secure communications to the company?
* Are there any international transactions that the company produces?
* Are there governmental restrictions about secure communications to consider?
* What external threats might be present now and in the immediate future?
* What are the “modernization” requirements that must be considered, such as the role of open source libraries and evolving web application technologies?

Because the organization provides financial services to its customers, the information they manage might include sensitive information about them. Customer confidence increases the value of secure communication to a corporation. Secure communications have an impact on more than just emails; they also have an impact on patron privacy. The organization appears to have the ability to conduct international transactions and offer communications, thus this should be considered when considering the possible dangers and safeguards that should be taken. The company will very certainly be required to obey existing government laws in the country where it is situated, as well as make adaptations for customers in order to comply with any local ordinances that may be in place. External threats include hackers using phishing tactics amongst other things in order to obtain patrons sensitive information. Making the organization totally web-based and providing more security are among the modernization criteria. To add further levels of security and functionality to their application, the corporation can use an open-source library. Unauthorized access to the web application or servers in general become possible as a result of modernization needs.

## 2. Areas of Security

Referring to the Vulnerability Assessment Process Flow Diagram, identify which areas of security are applicable to Artemis Financial’s software application. Justify your reasoning for why each area is relevant to the software application.

When it comes to security systems, Artemis Financial has a lot of room for improvement. APIs, cryptography, client/server, and secure coding are the key elements of security. The API must be secure so that when users use the system, the commands they submit over the API are not stopped or changed, potentially resulting in a security breach. When there is a lack of sufficient encryption during a transmission, the integrity and confidentiality of sensitive information might be jeopardized. Artemis Financial's secure code has to be improved because it provides the cornerstone for the company's commercial goals. When it comes to security issues, having everything controlled and guarded is a key responsibility.

## 3. Manual Review

Continue working through the Vulnerability Assessment Process Flow Diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

I don't see a validation technique used, this could lead to security risks infiltrating the system. The requests are not verified when they are sent out through the system's software. It is also lacking the use of HTTPS as a secure communication protocol.

## 4. Static Testing

Run a dependency check on Artemis Financial’s software application to identify all security vulnerabilities in the code. Record the output from dependency check report. Include the following:

1. The names or vulnerability codes of the known vulnerabilities
2. A brief description and recommended solutions provided by the dependency check report
3. Attribution (if any) that documents how this vulnerability has been identified or documented previously

Update the version to the latest on available. CVE-2013-1624 CVE-2016-6644 CVE-2015-7940 CVE-2016-100338 CVE-2016-100339 CVE-2016-100341 CVE-2016-100342 CVE-2016-100343 CVE-2016-100344 CVE-2016-100345 CVE-2016-100346 CVE-2016-100352 CVE-2017-13098 CVE-2018-1000613

## 5. Mitigation Plan

After interpreting your results from the manual review and static testing, identify the steps to remedy the identified security vulnerabilities for Artemis Financial’s software application.

Ensuring that clients and customers have a strong mix of characters including numbers, letters, symbols while also including lowercase and uppercase letters to guarantee that their credentials aren't guessed and accessed by hackers. To include secure programming practices, the code must be reviewed and updated. The code's quality should be upgraded in order to provide appropriate authentication and error detection.