****

# 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** | **4/1/2022** | **Emma McCarter** |  |

## 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

Emma McCarter

## 1. Interpreting Client Needs

Artemis Financial values secure communications as a part of their company. They would like to take the next steps to protect their organization from external threats. Secure communications ensures that no data is lost or tampered with while being sent and received. The company could make international transactions if there is access. There are no government restrictions on secure communications. The government wants companies to have security to protect their data and privacy. External threats are very real and should be a top priority for all companies. External threats have a main goal of accessing information that is secure. As security becomes more complex, hackers become more knowledgeable, making external threats immanent now and in the immediate future.

## 2. Areas of Security

The areas of security that are applicable to the Artemis Financials software application are Input Validation, Client/Server, and Cryptography. Input validation is he first line of defense in a web application, it is a programming technique that limits what input a web application will legally accept. It defines what data is allowed and rejects the rest. Once proper validation is done, data can be processed and accessed by a validated user. Client/Server is crucial for keeping client information secure, and communication is key as well. Cryptography is the most important area of security for Artemis Financials as that is what keeps hackers out and what makes their data safe.

## 3. Manual Review

Addition vulnerabilities in the code are the APIs and Encapsulation. APIs are crucial for data to navigate from computer to computer and software to software. If there are flaws in the APIs, then the security is weak and that can be a huge loophole for hackers. Encapsulation bundle the data but it can be flawed if not done properly or if there are errors.

## 4. Static Testing

## 5. Mitigation Plan

The steps needed to remedy the identified security vulnerabilities for Artemis Financials are to modernize and evolve as advancements have. Functionality is key but so is privacy and security, so Artemis Financials will have to step up their security measures.