****

# 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** | **01/19/22** | **Ronald Spires** |  |

## 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

Ronald S.

## 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?

Secure communications are important to protect the client and companies’ intellectual property and personal information. It is very important to ensure secure communication in the case of Artemis Financial as they are a financial company so unsecure communications could be disastrous. Global rain produces software for many different clients including international clients. Artemis financial might want to hire international employees in the future. There should be no governmental restrictions to take into account in this situation as there would be no third party use.

## 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.

Cryptography – this is applicable to the software because we will want to use cryptography to encrypt communications between the server and client.

Client/server – similar to why we need cryptography the client server is the communication that occurs between the client and the system server and completes the tasks desired. The client server also helps secure data so unauthorized users may not access it.

APIs – authorizes users without the need of a third party and Enables two or more applications to communicate with each other.

## 3. Manual Review

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

There appears to be an error of the variable “con” not being initialized properly in the docData class.

There does not appear to be any verification system in place.

The business names in the CRUDController class seem unsecure as they are passed as request variables.

## 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

The vulnerabilities found in the maven test mostly come from the services being out of date.

The recommendation moving forward is to update all the software and rerun tests.

## 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.

I did not notice any mention of HTTPS in the project code so that would be recommended to help secure sensitive information. Also, the request parameters for business name should be changed to headers. Also, all software should be updated to ensure that security can be appropriately updated and secure.