****

# 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** | **1/31/2021** | **Marcus Bullock** |  |

## 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

Marcus Bullock

## 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 will make sure that not only is the client information secure, but the businesses as well. Unsecure communications could end up being a very hefty lawsuit. It does not look like they partake in any international transactions. However, it could be a possibility seeing as they are a financial company. Working in financial there are quite a few government restrictions that will need to be considered. Mostly client information, and how encryption is being handled. External threats will always be present as anyone would want to break into a financial site to gather social’s and customer information. Let alone any information regarding money. One of the biggest things I can think of is storing client information in the cloud.

## 2. Areas of Security

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

One of the two biggest processes I can see on the diagram would by cryptography and api’s. There needs to be secure api interactions to make sure none of the client information may be getting picked up by unwanting eyes. Cryptography will also be needed as there will be a lot of sensitive information the client will be providing that will need to be encrypted. Namely their social security.

## 3. Manual Review

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

From looking at the code, it looks like there really isn’t any encryption at all. There are also a few warnings on DocData with the connection.

## 4. Static Testing

Run a dependency check on Artemis Financials’ 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

From running my dependency report there are two critical dependencies. Tomcat-embed-core-9.0.30.jar and tomcat-embed-websocket-9.0.30.jar. For the first tomcat dependency it appears that the biggest issue is with invalid transfer-encoding headers. This could lead to a http request smuggling if tomcat is located behind a reverse proxy. Here is a reference  <https://security.netapp.com/advisory/ntap-20200327-0005/> . It appears the same for the secondary tom-cat dependency as both will also have a possibility of triggering high CPU usage.

## 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 Financials’ software application.

It looks like though both tom-cat dependencies may have some serious issues, along with having a high vulnerability rate of hackers being able to access information. Most of these issues are actually resolved by using an updated version of tom-cat. It should alleviate these issues and vulnerabilities. Staying up to date on each update and verifying regression should make the software application secure.