****

# Artemis Financial Vulnerability Assessment Report

Table of Contents

Artemis Financial Vulnerability Assessment Report 1

Document Revision History 3

Client 3

Instructions 3

Developer 4

1. Interpreting Client Needs 4
2. Areas of Security 4
3. Manual Review 5
4. Static Testing 5
5. Mitigation Plan 5

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **Jan 23rd 2023** | **Jordan Carver** |  |

## 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

Jordan Carver

## Interpreting Client Needs

* What is the value of secure communications to the company?

The value in secure communications is to ensure confidence with the businesses customers. With secure communication we can assure customers that their privacy is important.

* Does the company make any international transactions?

Artemis Financial’s does in fact make international transactions that deals with various stocks and international clients.

* Are there governmental restrictions about secure communications to consider?

I believe governmental restrictions always need to be considered in the equation of dealing with any form of communication or information being sent back and forth. It is important to always consider these restrictions because when dealing with private data, or digital money transfers we must ensure it is secure and safe.

* What external threats might be present now and in the immediate future?

Current and future threats are present all around us. These include new hacking technologies and new ways to manipulate a system or a system user to hack into valuable information to either steal or to cause damage with. Another quickly growing external threat would be a rise in viruses such as phishing scams.

* What are the modernization requirements that you must consider?

To modernize the company the requirement states that the business must be fully web based. This would actually allow the company to increase security by adding additional layers of security and functionality to the program. Thus further protecting valuable customer transactions and client data from being stolen.

## Areas of Security

The main areas of security that apply to this particular business analysis would include API, Cryptography, Client/Server, and Secure Coding. We have to ensure every aspect of the application is secured and that the relationship between two or more application is end to end protected with API. With Cryptography we are ensuring any data that is transmitted through the internet can be accessed and stay secured. Without encryption it could compromise a persons personal information or a leak of valuable business data. One valuable resource here is a commitment scheme in which two businesses or two parties would interact with a series of computational securities are used to trust and secure data between the parties. Client/Server is the communication relationship between the client and servers that are utilized on web applications. These systems will contain security features that ensure data is secure physically through hardware and networks across a business or an organization. And lastly with Secure Coding we would use this to apply to ensure coding is clean, organized and secure. Secure coding is more of an exercise used to check vulnerabilities that are accidentally placed within the code or application like bugs and errors for example. Essentially Secure Coding is the proof reading of software development. It is a process in which a developer will proof check their work and correct errors found within it.

## Manual Review

Manually reviewing the vulnerability assessment process flow diagram and code. I was able to locate two possible design flaws with. One located within the data access and the other located within the direct object. The first one located in the DocData.java folder. The main flaw here is that the root user and password could easily be guessed which would lead to compromised accounts and a data leak. While with the second flaw located in the CRUDCcontroller.java file. The flaw here is that objects could be vulnerable to code injections.

## Static Testing

After running the static test on the Artemis Financials software we can see there are many vulnerabilities within the code that would need to be properly addressed and the issues corrected.

Tomcat embed core 9.0.30 CVE 2019 17569

Core Tomcat can potentially cause a high consumption of memory that could theoretically crash the Artemis system. The most effective way to fight this would be to use the update version of the system to overcome flaws and vulnerabilities.

Bouncy Castle, CVE 2015-6644

The bouncy castle would allow malicious software to access secured date stored within a database. The best approach to correct this vulnerability would be to consistently update the system and all software as often as possible to the newest version available. This prevents known vulnerabilities from being used against the system.

Apache Log4j SMTP appender, CVE 2020-9488

This would cause for log messages to be revealed with no way of keeping them secure. To overcome the vulnerability I would recommend incorporating a verification feature built within the software and keeping software updated to its newest version.

## Mitigation Plan

After analyzing the results from my manual and static tests there are a few security vulnerabilities that would need to be addressed with the Artemis Financials software. The first being the data access of the username and password. Ensuring a strong combination of a username and password is one of the fundamental steps in ensuring accounts stay secured from accounts getting hacked. Proper code reviewing is another critical step in securing the Artemis software. For this developers would need to integrate best code practices and ensure all steps are taken seriously to reduce possible code errors and to have proper authentication when needed. Updating the Apache server would be another critical move to make as old versions of software and servers may contain known vulnerabilities and be more prone to attack from hackers. Proper certification is also very important for both a client and server perspectives. By the TLS certificate mutual checking we are trying to avoid any potential attack or vulnerability of client requests of the API.