****

# 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** | **05/25/21** | **Naomi Ruffalo** |  |

## Client



## Developer

Naomi Ruffalo

## 1. Interpreting Client Needs

Communication throughout application development is key to a successful application. The developers must communication throughout the creation of the application with the scrum master and the testers. Specially, communicating about security. Security is crucial specially for a company such as Artemis Financials where people entrust their life savings.

Artemis Financial does conduct transactions globally as mentioned in the description. Security is extremely important when dealing with transactions that are not in person. Any one can be an imposter to steal another person’s income. To ensure security, adding facial recognition and fingerprint identification to the system will be extremely helpful. This way we can verify who the customer is every time they sign into the account through the application.

One governmental restriction about secure communications that should be considered is the Federal Information Security Modernization Act of 2014. This act requires a report on all the information security changes and developments added to the code in the applications.

Some external threats that might be present now and in the immediate future is cyber attacks and fraud. With financial applications fraud happens very often. To help for this like I mentioned above, adding facial recognition and fingerprint validation will reduce the likelihood of fraud attempts. For cyber-attacks, the developers should add longer password and username requirements. Making it harder for cyber users to hack.

Some modernization requirements that should be considered are putting the customers needs first and making the overall design simpler. To create the customers needs first, a question-and-answer section, where the customer can find the answer to most of their problems. For the design, more icons can be created to make it easier for the customers to understand.

**Sources**

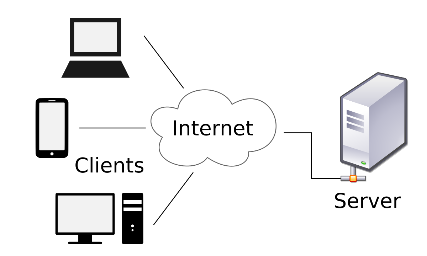
CISA.gov. Retrieved from: <https://www.cisa.gov/federal-information-security-modernization-act>

Cooper, Leon. Retrieved from: <https://www.strategy-business.com/article/10-Principles-for-Modernizing-Your-Companys-Technology?gko=6ff05>

## 2. Areas of Security

**Input** validation should be required for every application development process. This way we can entail all the necessary and correct code in the software application.

**APIs** process should also be incorporated. This application requires the use of external operating systems since it will be used globally.



**Client/Server** relationship is extremely important because multiple clients will be accessing their account information from several platforms. Client/Server should be excellent for this matter with simple connection to the internet and the server.

**Code Error** should also be taken into consideration when developing a software application because if there is code error, the application will not be able to run. It should be reviewed constantly.

Encapsulation is the final step of the process and it is particularly important. This is when the software application for Artemis Financials because during it, we create the code into one unit instead of having the code separate.

**Sources**

Vulnerability Assessment Process Flow Diagram. Retrieved from: <https://learn.snhu.edu/content/enforced/751242-CS-305-X5833-OL-TRAD-UG.21EW5/course_documents/CS%20305%20Vulnerability%20Assessment%20Process%20Flow%20Diagram.pdf?_&d2lSessionVal=LSz3WKYhMFaSrjQd4BXjL670H&ou=751242>

## 3. Manual Review

When inspecting the code, I see there is a log in id required to access the account information in class Greeting.java. We can add some modifications to this by asking for a specific log in with at least 8 letters, one being capital. This would belong in the input validation and code quality process.

Text

Description automatically generated

I also see in DocData.java class, that the code is being tested. This would be a part of the code security process.

Graphical user interface, text, application

Description automatically generated

## 5. Mitigation Plan

After reviewing the manual review, some identified vulnerabilities that were found is that this application requires weak password id and username. The software application can improve in this matter.