****

# 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** | **23 March 2022** | **Zachary Carper** |  |

## 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

Zachary Carper

## 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?

Since the company handles individuals’ money as well as financial outlook and goals for its customers, they hold very sensitive PII (personal identifiable information). Secure communication is of extreme importance for Artemis because of this. Due to it being a financial institution it must comply with government regulations and restrictions when it comes abiding by legality of being a financial institution. If the company didn’t abide by these rules, it could cause security risks for the company and its customers. The risk of threats a company such as Artemis faces are huge. They are massive targets due to their large cash holdings. Due to Artemis being a large target they need to ensure they are following all the proper precautions such as ensuring the API is secure enough, they are utilizing features such as 2FA (two-factor authentication) and using proper encryption methods when communicating.

## 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.

Ensuring that all the code is throughout and secure is going to negate the chance of any vulnerabilities to potentially pass through or be exploited. With the utilization of RESTful API in web services it is important that it holds a certain level of secure communication.

## 3. Manual Review

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

It does not utilize HTTPS which is almost a necessity nowadays when combating adversarial threats that attempt to infiltrate companies such as Artemis to obtain sensitive information. An authentication system should be in place. Requests are also not validated which could pose vulnerability issues.

## 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

CVE-2020-1938 / CVE-2020-1935 / CVE-2020-17527 / CVE-2020-13943 / CVE-2020-13935 / CVE-2020-13934 / CVE-2020-11996 / CVE-2019-17569 / CVE-2020-25649 / CVE-2017-18640 / CVE-2020-9488 / CVE-2018-5382 / CVE-2018-1000613 / CVE-2017-13098 / CVE-2016-1000352 / CVE-2016-1000346 / CVE-2016-1000345 / CVE-2016-1000344 / CVE-2016-1000343 / CVE-2016-1000342 / CVE-2016-1000341 / CVE-2016-1000339 / CVE-2016-1000338 / CVE-2015-7940 / CVE-2015-6644 / CVE-2013-1624 / CVE-2020-8022 / CVE-2020-9484 / CVE-2021-24122 / CVE-202-10693 / CVE-2020-5421

## 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.

Based off the findings we need to ensure that security is the main priority. The first solution would be to switch the company to utilizing HTTPS instead of what they are currently utilizing. After that just more the parameters into headers. Implementing 2FA will be of great usage for the company and customer due to the enhanced security protocol it gives. Adding these would ensure that the security is met the most it can be, aside from that ensuring to update the dependencies.