****

# CS 305 Project One

**Artemis Financial Vulnerability Assessment Report**

**Table of Contents**

[Document Revision History 3](#_gjdgxs)

[Client 3](#_30j0zll)

[Instructions 3](#_3znysh7)

[Developer 4](#_2et92p0)

[1. Interpreting Client Needs 4](#_tyjcwt)

[2. Areas of Security 4](#_3dy6vkm)

[3. Manual Review 4](#_1t3h5sf)

[4. Static Testing 4](#_4d34og8)

[5. Mitigation Plan 4](#_2s8eyo1)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **3/19/2022** | **Teodoir O’Ceallaigh** | **Initial review** |

## 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

Teodoir O’Ceallaigh

## 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?

It is integral that the company is using secure communication so that there is no loss or theft of data, hacking of the system, etc. This can be accomplished through using clearly outlined secure protocols to send and receive the data between the server and client. Because the company provides financial services to their clients, the protection of this data is especially important as there is a high level of sensitive information that needs to be communicated and the potential for malicious risks is significantly higher than generalized systems. As this is an online system that users need access to in order to complete financial-related tasks, it is possible that international transactions may be produced and this will need to be considered in the security protocol created for these interactions. It is highly likely that there will be government requirements regarding security based on the type of financial information they store/communicate to secure any federal/state insurances (America) as well as any other government policies to operate in other countries if users actively exist outside of the United States. Because of the immense amount of financial data that would be present in this company, the most immediate and prominent future threats are going to be malicious intent to attack the system and gain either knowledge of personal information of customers and or up to direct access to customers’ money. An important way to modernize requirements would be primarily instituting 2FA, an SSL (https), and a strict account locking method with a secure validation method for account unlocking procedures. While these can not for sure prevent every method of attack, it will likely deter less advanced threats.

## 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.

First, the code quality and secure code error handling will be an important start to ensure that there are no basic vulnerabilities present to be exploited on the backend level. It will also be integral to regularly perform updates to maintain security through any program iterations as the company continues to perform their expected business functions on the front end. Another important area of security is the API, which will allow for secure transmission that is not interrupted or easily adjusted for breach purposes. Secure client/server communication is another facet that will reduce the ability to break into the system, and this can be accomplished with the use of encryption and input validation once data is received but prior to allowing access.

## 3. Manual Review

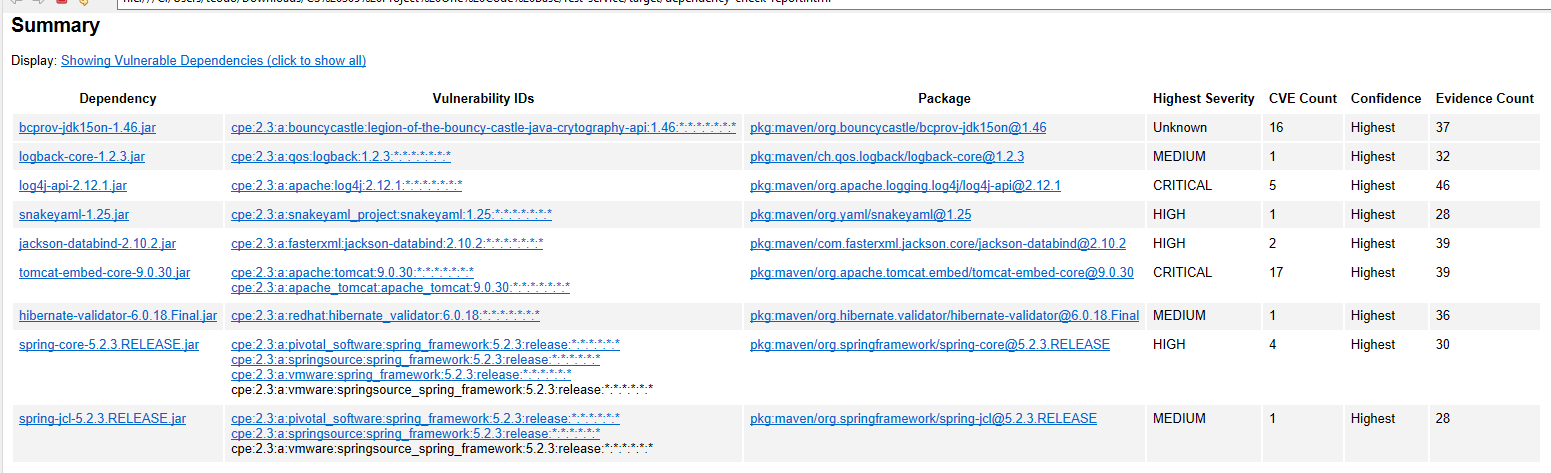
Continue working through the Vulnerability Assessment Process Flow Diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

Upon inspection of the code, there is not a secure validation method encoding into the program which opens the door for injection and other types of cyber attacks. There also doesn’t seem to be an enforced use of SSL (https) which means that there is not a secure layer of encryption on the service site.

## 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 the 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
4. bcprov-jdk15on-1.46.jar - Update to the latest version available
5. logback-core-1.2.3.jar - Update to the latest version available
6. log4j-api-2.12.1.jar - Update to the latest version available
7. snakeyaml-1.25.jar - Update to the latest version available
8. jackson-databind-2.10.2.jar - Update to the latest version available
9. tomcat-embed-core-9.0.30.jar - Update to the latest version available
10. hibernate-validator-6.0.18.Final.jar - Update to the latest version available
11. spring-core-5.2.3.RELEASE.jar - Update to the latest version available
12. spring-jcl-5.2.3.RELEASE.jar - Update to the latest version available



## 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.

The primary next steps would be to update the vulnerabilities listed to the latest versions and run the report again to verify that the updates do not create additional vulnerabilities. These updates are important to align with the recommendation for code quality and error mitigation going forward that could potentially contribute to security faults. In addition, implementing 2FA and ensuring the required usage of SSL (https) will further secure the system against malicious attacks.