# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **July 21, 2024** | **Lillian Martinez** |  |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In this report, identify your security vulnerability findings and recommend 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 include images or supporting materials. If you include them, make certain to insert them in 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

Lillian Martinez

**1. Interpreting Client Needs**

Determine your client’s needs and potential threats and attacks associated with the company’s application and software security requirements. Consider the following questions 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 on secure communications to consider?
* What external threats might be present now and in the immediate future?
* What modernization requirements must be considered, such as the role of open-source libraries and evolving web application technologies?

Artemis Financial is a company that develops individualized financial plans for its customers, these plans include savings, retirement, investments, and insurance. The value of secure communications to the company is crucial because this company is handling sensitive client information, including SSNs, tax information. This kind of information is enticing for any outsiders to pry into. This company is not stated that it is strictly in the US, so international transactions would be having to be dealt with as well. A governmental restriction that might have to be considered regarding secure communications is ensuring that Artemis Financial explain its information sharing practices and to make sure sensitive data is secured. Because this company needs to safeguard a lot of sensitive information, a main external threat to consider is client information being targeted. Data needs to be encrypted from anyone outside of the company. Some modernization requirements that need to be considered are up to date maintenance checks regarding any found bugs and security threats.

**2. Areas of Security**

Refer to the vulnerability assessment process flow diagram. Identify which areas of security apply to Artemis Financial’s software application. Justify your reasoning for why each area is relevant to the software application.

* Code Quality: To ensure secure coding practices and patterns. This would also control who can access what information through the API.
* APIs: Controls what information is accessible to outside sources.
* Input Validation: This would be able to validate the accounts owner information.
* Cryptography: Ensures that information is properly encrypted. So that if information is accessed through the API this information is protected.
* Code Error: This will be able to highlight any errors in the code which are weak and need to be fixed.

**3. Manual Review**

Continue working through the vulnerability assessment process flow diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

During my manual review I noticed vulnerabilities in the code:

1. of input validation in Greeting Controller.
2. No signs of cryptography being used.
3. Does not use HTTPS, this can be used when sharing sensitive information.
4. No authentication system in place for verification uses.

**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 items:

* The names or vulnerability codes of the known vulnerabilities
* A brief description and recommended solutions provided by the dependency-check report
* Any attribution that documents how this vulnerability has been identified or documented previously
* Bcprov-jdk15on-1.46.jar : This has a lot of vulnerabilities, to fix this we would need to update to the latest version of Bouncy Castle.
* Hibernate-validator-6.0.18.Final.jar : one vulnerability, to fix this we need to update to the most current version.
* Jackson-databind-2.10.2.jar : One vulnerability, the solution would also be to update to the latest version.
* Log4j-api-2.12.1.jar : one vulnerability, to fix this we just need to update to the latest version 2.13.1
* Tomcat-embed-core-9.0.30.jar : three vulnerabilities found here; the solution would be to update to Apache Tomcat.
* Snakeyami-1.25.jar : one vulnerability, to fix this also update to the latest version.
* Spring-core -2.2.4.RELEASE.jar: Four vulnerabilities found here; the solution would be update to the current version.

**5. Mitigation Plan**

Interpret the results from the manual review and static testing report. Then identify the steps to mitigate the identified security vulnerabilities for Artemis Financial’s software application.

To fix the vulnerability findings would first be to update the systems to the latest versions of the vulnerabilities. Such as Snakeyami, Apache Tomcat, Bouncy Castle, and also hibernate validator. We can also implement HTTPS so that all client information is secure, and this will help to prevent outsiders from prying into the information. Also adding an authentication system so that we can protect the client information.