# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **05/26/24** | **Kailah Whitted** |  |

## 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

Kailah Whitted

**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 form financial plans for individuals running from savings to retirement investments and insurance. Secure communications is very crucial to the company because it’s handling a lot of sensitive information from the clients. This can include SSN, tax information, etc. There’s nothing mentioning Artemis being a sole US company, so this company probably has international transactions. There is one major governmental restriction that the company would have to consider and that’s their trade secrets. They have a lot of sensitive information that they need to keep secure on. Routine data checks and maintenance should identify potential threats and issues.

**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.

Input Validation – The company requires this to validate the owner of information. This would protect all users and would be written as a string.

Code Quality- Control the access that’s available to the user.

APIs- This would run internally and externally and would control which accessed data is acceptable.

Code Error- This would identify which part of the API that needs to be fixed and it would protect sensitive from being exposed.

Cryptography- This would ensure sensitive user information wouldn’t be compromised.

**3. Manual Review**

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

After reviewing the code and utilizing the Vulnerability Assessment, I broke down the POM.XML and the Greeting Controller. From the XML file, I made sure I could locate an Apache Vaildator. From the Greeting Controller, I found there was little input validation. I did find the code quality to be in order but I noticed an issue that the error handling wasn’t there. From the API, I found there was a breach that could expose sensitive information because it was created through a POST method. Lastly, I didn’t find any signs of cryptology.

**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

[Include your findings here.]

**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.

The best solution to identify security vulnerabilities would be to run the current versions of Snakeyaml, hibernator validator, Apache Tomcat, and bouncy castle.