# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **05-26-2024** | **Nicholas Wyrwas** | **N/A** |

## 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

Nicholas Wyrwas

**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?

When looking at Artemis Financial and their value of secure communications is that “Security is everyone’s responsibility”. Where they focus on financial plans, which include savings, retirement, investments, and insurance plans. Stating that secure communications are invaluable to Artemis Financial. Especially with the sensitive nature of the data they would handle. It would be beneficial to consider governmental restrictions on secure communications. Especially when regarding the protection of classified information and trading secrets. Some external threats that may be present could be hacking attempts and possible data breaches. Which would pose as a risk for the company’s security. Some modernization requirements that I would consider would be having up-to-date maintenance checks and utilizing open-source libraries to allow frequent checks on the software vulnerabilities and security weaknesses.

**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.

When it comes to vulnerability assessments I would consider the following:

Input Validation – Which would allow the company to validate owner information. As well as, providing protection.

Code Quality - Providing a layer of security, by updating their code to allow only certain types of access to be provided to certain individuals. For example, having a user only be provided with the information that is necessary for them.

APIs – Creating secure API interactions.

Code Error – By having handling for the code allows the company to see where the software is posing issues, which would allow the company to fix the code promptly.

Cryptography – having encryptions for the sensitive information that the company possesses.

**3. Manual Review**

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

When conducting the vulnerability assessment process flow diagram. I looked at the POM.XML and Greeting Controller files. In the POM.XML file, I saw that there was an Apache Validator. And from the greeting controller that there was not as much input validation. When inspecting the code I saw that the code was at a good quality. But there was a lack of error handling. When it came to the API, there was much that they could improve on. And with that being stated I think that with what is currently in the code there is a higher chance of vulnerability and hacking to occur.

**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

A screenshot of a computer

Description automatically generated

**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.

I think some steps to be taken would be updating all of their dependencies. As that would allow the software to be more or so up-to-date. Adding some checks to the greeting controller to ensure that input from users are safe. And by adding more error handling, just so if something happens and an error occurs the company would easily be able to address and resolve the issue. For the API, I would make sure that it has safer methods when it comes to certain tasks. Ensuring that there are controls made for who can access it. Then update the Apache Validator to ensure that it helps with checking user inputs. And finally with adding encryption it will allow the data to be secure and safe.