# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **7-24-24** | **Sean Chase** |  |

## 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

Sean Chase

**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 financial company that deals with important information of their clients. Secure communication is a must to protect client information.

I didn’t see that there are international transactions, however, being a financial company, I think they probably do business internationally as well.

Threats, such as breaches, are present now, and will be in the immediate future.

Updates to their libraries will ensure that current fixes for bugs and security threats will be implemented to keep the data safe.

**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: When collecting user input, validation is crucial. It’s necessary to avoid any failures or SQL injections.

APIs: A well developed API is important. This application will run internally and externally. It will define how an end user interacts with the program.

Cryptography: It is important if transactions will be taking place internationally. This will protect customer information that is included with the transactions.

Code Error: This is necessary to work with input validation and prevent unauthorized access, or access to privileged information.

Code Quality: This is necessary to ensure there is no unintentional data exposure.

**3. Manual Review**

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

I found a vulnerability within the DocData.java file with the data access method. The username and password had many possible vulnerabilities. The root users and the password are not recommended for use by the root user. The root is used for the username and password and the root password could be easily guessed. Also, unauthorized users can easily gain access to the system.

I found a vulnerability within the CRUDController.java file. The application could be exposing the inside objects, being retrieved and passed through a sequence of code injection.

**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

I wasn’t able to do this part.

**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 the vulnerabilities could be mitigated by keeping everything up-to-date, and running current versions.