# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **6/1/2025** | **Michael Armstrong** |  |

## 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

Michael Armstrong

**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?

Secure communications is incredibly important for Artemis Financial because their clients are looking to secure their financial futures and protecting their clients sensitive information is their number one priority. The company helps clients across the globe. This lets in a lot of potential customers. Since Artemis Financial supports customers across the globe, they need to be aware of many governmental restrictions and rules to follow, so that the company obeys the laws of all these governments. Open-source libraries are helpful so that other programmers can review the program, and copy the parts for their own programs. Open source libraries are a community oriented, so that if errors are found, the members of the community help debug the program and fix issues together. Using open-source libraries do require constant observation and licensing per government policies and laws.

**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.

According to the dependency check, error code CVE=2024-21733 generates an error message containing sensitive information in Apache Tomcat. Generating an error message when filling out forms full of sensitive information . Another error found CVE-2020-13943, could send In pseudo headers from previous requests rather than the intended headers, leading to unexpected responses for unexpected resources. This is a major problem because a hacker could get into someone’s financial information and steal bank account information, social security, address information, etc. by logging into someone’s page by accident, or on purpose.

**3. Manual Review**

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

In class DocData.java, there is a method also called DocData, that is empty. This could lead issues into unnessecary data to be filled into forms.

**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

There are a lot of dependency errors in this code. There are 437 errors in the code. Some of the errors are to update other parts of the code to remove errors, while some errors, don’t have suggestions to be updated.

**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 plan of action is to review each dependency check provided, and find a fix to keep Artemis Financial up to date, secure, and easy to use, for both the development team and the end users.