# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **3/19/2025** | **Brandon Mullins** |  |

## 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

Brandon Mullins

**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 specializes in developing personalized financial strategies for clients, covering areas such as savings, retirement planning, insurance, and investment management. Due to the sensitive nature of the data they handle -- such as Social Security numbers, tax documents, and personal financial details – strong security and encrypted communication are essential to maintain client trust and data confidentiality.

**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- To ensure the data entered by users is properly sanitized and verified before processing to help prevent injection attacks or data corruption.

Code Quality- Applying strict coding standards and access controls ensures users only access their own data. High quality code reduces the risk of logic errors and security flaws.

Error Handling- Implementing detailed and secure error messages helps identify issues without exposing sensitive information to end users or attacks.

API Security- Since Artemis uses a Restful API, It’s essential to secure endpoints with authentication, rate limiting, and validation to prevent unauthorized access or data leaks.

Cryptography- Encryption of data both in transit and at rest protects sensitive financial records, especially when transmitting data over public or international networks.

**3. Manual Review**

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

1. Missing Input Validation
2. No Error handling
3. Insecure API Methods
4. Lack of Authentication
5. Outdated Dependencies
6. Missing Encryption
7. Exposed Endpoints
8. Unlogged Errors
9. No role-based Access
10. Hardcoded Config

**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

**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.

Input Validation use input sanitization libraries or frameworks. Update Dependencies which to upgrade all outdated libraries. Implement Authentication to add token-based or session-based authentication. Enable logging to use a secure logging framework to capture security events.