# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **[Date]** | **[Your name]** |  |

## Client



## Developer

Leigh Ann Stack

**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?

We need to make sure the company is using secure communications to keep the customers information private. The secure data method is used to receive and send data between the client and the server. This company is handling customers financial data and it could be at risk without a through vulnerability assessment. This kind of data is the information hackers are looking for. They handle financial data and there are some government regulations and restrictions when it comes to handling transactions and communication. The API needs to be secure to help deter hackers from entering the software and stealing information. Two factor authentication should help stop any fake login attempts.

**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.

There are a few areas of security that can apply to Artemis Financial’s software application. Code quality is one of them. We need to make sure the application is written with secure coding practices in mind. They are using a RESTful API. This allows two computer systems to exchange information securely. ([What is RESTful API? - RESTful API Explained - AWS](https://aws.amazon.com/what-is/restful-api/)) RESTful API supports a secure exchange of information because they follow secure, reliable and efficient software communication standards.

**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 don’t see any code to address error handling. This step would put in place methods to identify, report and manage problems.
* There seems to be lack of input validation in the Greeting Controller.
* No signs of cryptography.
* Service does not use HTTPS

**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.

* Switch to HTTPS protocol
* Add error handling
* Add input validation