# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **July 18, 2024** | **Win Inlaw** |  |

## 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

Win Inlaw

**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?

My client is Artemis Financial and they are in charge of coming up with reasonable and needed financial help. For example they take part in people investments. This client as you can tell will be handeling classied information from their clients in which beacuse its a financial business we can expect things like Social Security Number, your W-2(taxes), and many other key things. Where people can still your identity etc. There is a governmental restriction that comes to mind with this secure communications is a must. Again this is because the whole company life depends on protecting all information they have. Talking about the client information throught Artemis Financial.

**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.

*Inout Validation* = security for users

*API’s* = allowing which data accessed is acceptable

*Crytography*= A second support in it’s own way compared to validation. helps ensure user information can’t be compromised.

**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 inspecting the GreetingController file i became aware that there is a great lack of correct input validation. This would leave the system vulnerable to potential leaks and hacks into the software. Further more API has a more concerning issue. Which is a more secure method that even includes the parameter in the URL. It should have been API. Moving on again I tried to tackle the cryptography yet there is no forseeable data encryption set present.

*Vulnerabilities:*

1. *Input validation*
2. *APIs*
3. *Cryptography*

**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

SnakeYaml = one vulnerability {CVE-2017-18640}

(

Log4J = one vulnerability {CVE-2020-9488}

Tomcat = many vulnerabilities {

CVE-2020-1759

CVE-2020-13934

CVE-2020-1935

CVE-2020-9484

etc.}

(More dated version)

**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.

Like many common companies sometimes updating can patch up vulnerabilities you have. This allows things that have been coded to be involved to make everything easier for you. With many of the security risks in most assignments regarding this company, it is updating. Tomcat especially needs updating on its files for the current version. This can be confirmed through static testing. Also, SnakeYaml has a different vulnerability where we can modify the security factor there. Doing the needed updates would increase the security for this company.

Also, we need to add API’s in the post method.