# CS 305 Project One Template

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2/1/2025** | **Jorge Rodriguez** |  |

## 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

Jorge Rodriguez

**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?
  + When regarding the value of secure communications for Artemis Financial, the value should be a high priority. The company in question deals with individuals' finances. The company would want to ensure confidential and secure communications to protect highly sensitive and valuable client information. Secure communications will prevent any potential data breaches and unauthorized access to client information.

* Are there any international transactions that the company produces?
  + If international transactions are engaged by Artemis Financial, they should be aware of both local and foreign laws and regulations to follow to avoid any setbacks.
* Are there governmental restrictions on secure communications to consider?
  + Yes, Artemis Financial is in a business of dealing with highly sensitive and highly regulated data. Just in the US alone the company must be mindful of not only State laws and regulations but also Federal laws and regulations.
* What external threats might be present now and in the immediate future?
  + Regardless of what type of software or application is being created, the looming threat of external threats is always present. Examples include and are not limited to DDos attacks, malware, unauthorized access and data breaches.
* What modernization requirements must be considered, such as the role of open-source libraries and evolving web application technologies?
  + When it comes down to modernization, it essentially means to keep up with the current technology that is available in the market at the time. AS time progresses new programs help strengthen security in the softwares by either creating new security protections. IF a software is utilizing older technologies it may be susceptible to more security risks as the newer technologies also bring in newer ways to attack said technologies.

**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 is an area of security that is relevant to this software application because it is a requirement for RESTful API. INput validation helps avoid potential vulnerabilities such as SQL injections and other injection attempts.
* Code quality is another area that should have high priority. Practicing standard procedures is one of the first lines of defense when it comes to security.
* APIs - the web application in question will include a RESTful API, it needs to be ensured that the communication that will take place will be secure.
* Code errors must be fixed to ensure any and all potential vulnerabilities are handled in a secure manner to prevent any leakage of potential sensitive information.

**3. Manual Review**

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

* Not using HTTPS, this is important especially when dealing with sensitive information
* no validation for the request parameters.
* The business names are being sent through the CRUDController class as request parameters.
* The software is not running on the update version of the program
* Within the DocData there are databases connections in the parameters

**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
* Bouncy Castle,
  + CVE-2013-1624
  + CVE-2015-6644
  + CVE-2015-7940
  + CVE-2016-1000338
  + CVE-2016-1000339
  + CVE-2016-1000341
  + CVE-2016-1000342
  + CVE-2016-1000343
  + CVE-2016-1000344
  + CVE-2016-1000345
  + CVE-2016-1000346
  + CVE-2016-1000352
  + CVE-2017-13098
  + CVE-2018-1000613
  + CVE-2018-5382
  + For Bouncy castle, I recommend updating this application frequently to the most up to date version to avoid any compromises within the application .
* Apache Log4j SMTP appender,
  + CVE-2020-9488.
  + If updated to the up to date version and including a new feature to have verifications
* Core Tomcat,
  + CVE-2019-17569
  + CVE-2020-11996
  + CVE-2020-13934
  + CVE-2020-13935
  + CVE-2020-13943
  + CVE-2020-17527
  + CVE-2020-1935
  + CVE-2020-1938
  + CVE-2020-8022
  + CVE-2020-9484
  + CVE-2021-24122
  + The dependency should be the main focus on this vulnerability when updating to the current 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.

* The original did not include utilizing HTTPS for all communication needs. I would recommend utilizing HTTPS moving forward, by using a stronger more secure communication protocol in place will be beneficial.
* It should be implemented by conducting regular security checks which include but not limited to ethical hacking, scanning for potential vulnerabilities and addressing potential security issues.
* Proper code practices as stated before is one of the first lines of defense when it comes to security .
* One major thing is to always keep up with the application versions. ensuring that everything is up to date with back up in case of any mishaps. Staying up to date ensures the highest security possible, and having a backup is to ensure if the newer version happens to have potential hazards.
* The security in the DocDate class should be improved. The database should utilize secure communications such as SSL or TLS. This will make sure that the data that is being transmitted within in encrypted and secure.