## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **05/25/2024** | **Coltin Meyer** |  |

## 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

Coltin Meyer

**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 is looking to protect their organization from external threats while modernizing its operations. As a financial company they have personal data that must be kept safe as it proves the companies integrity. Confidentiality of financial data is what maintains trust between their clients and Artemis Financial. Should Artemis Financial decide to expand internationally they would need to be compliant with international cypersecurity standards and data protection laws. There are legal requirements for private data that requires secure communications such as encryption to be used in practice. A company like our client has potential threats such as SQL injection, DDoS attacks, and phishing which can be present currently or threaten future expansions. To assist Atemis Financial’s goal in modernizing the company incorporating updated web technologies while ensuring the open-source libraries are secure.

**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.

Listed below are the areas of security that I found are important to Artemis Financial.

Input Validation - prevents injection attacks by verifying values provided by the user

Secure API’s - Preventing attacks on the web-based applications are necessary to ensure the confidentiality of Artemis Financial

Cryptography - This can be utilized on important documents but preventing attacks by addressing vunerabilities is a large component of securing Artemis Financial

Client / Server - Secure distribution of files from the company is to be practiced as protecting the code is pointless if the documents arent secure in the first place

Code Quality - Secure coding practices are necessary to any project especially one handling personal financial data.

**3. Manual Review**

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

* Lack of input validation in DocData return id line 16
* The lack of input validation is returned to CRUDController
* CrudController returns “id” to CRUD which is not input validated
* In customer class, lack of encryption for account\_number
* Lack of input validation in class Customer for which customer account number you are reviewing
* greeting class requires encryption for Id and Content to keep files safe
* Lack of input validation in Greeting or Greeting Controller class to greet hello world

**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

A total of 13 vulnerable dependencies and 135 vulnerabilities. Ill list a few of the important ones.

The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms.

* Improper validation of certificate with host mismatch

Hibernate's Bean Validation (JSR-380) reference implementation.

* A bug in the message interpolation processor enables invalid EL expressions to be seen as valid

General data-binding functionality for Jackson: works on core streaming API

* Flaw found in FasterXML Jackson Databind where it ididnt have entity expansion secured properly

The Apache Log4j API

* Improper validation of certificate with host mismatch in Apache Log4j SMTP appender

logback-core module

* Serialization vulnerability in logback receiver

**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.

A Mitigation plan that I would begin to introduce is to require input validation on anything that requires input from the user. The account number and ability to deposit shouldnt be available unless the user is validated to be the owner of the account via card number or id number. If able I would introduce encryption of personal data as well to keep the customers information confidential and secure. I would also have the entire team at Artemis Financial take Phishing avoidance classes to avoid leaking the employee logins.