****

# CS 305 Project One

**Artemis Financial Vulnerability Assessment Report**

Table of Contents

[Document Revision History 3](#_Toc32574607)

[Client 3](#_Toc32574608)

[Instructions 3](#_Toc32574609)

[Developer 4](#_Toc32574610)

[1. Interpreting Client Needs 4](#_Toc32574611)

[2. Areas of Security 4](#_Toc32574612)

[3. Manual Review 4](#_Toc32574613)

[4. Static Testing 4](#_Toc32574614)

[5. Mitigation Plan 4](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **5/20/2022** | **Christopher Hageman** | **Project One** |

## Client



## Instructions

Deliver this completed vulnerability assessment report, identifying your findings of security vulnerabilities and articulating recommendations for next steps to remedy the issues you have found.

Respond to the five steps outlined below and include your findings. Replace the bracketed text on all pages with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

## Developer

Christopher Hageman

## 1. Interpreting Client Needs

Determine your client’s needs and potential threats and attacks associated with their application and software security requirements. Consider the following 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 about secure communications to consider?
* What external threats might be present now and in the immediate future?
* What are the “modernization” requirements that must be considered, such as the role of open source libraries and evolving web application technologies?

The value for secure communications to this company is extremely high because we are guarding the customers financial security. There are international transactions dealing with trading of stock which affects the customer’s savings, retirement, and other investments. The governmental restrictions about secure communications that should be looked at are “Gramm-Leach-Bliley Act which requires companies defined under the law of “financial institutions” to ensure the security and confidentiality of this type of information. As part of its implementation of the GLB Act, the Federal Trade Commission (FTC) issued the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have measures in place to keep customer information secure.” (Staff & This blog is a collaboration between CTO and DPIP staff and the AI Strategy team, 2020). A couple of external threats that are always present are ransomware and Trojans. There are always going to be threats to financial institutions if money is worth something so there will always need to be security and protections. We can use open-source library for functionality and work in sand-box mode for better security in the world of evolving web applications.

## 2. Areas of Security

Referring to the Vulnerability Assessment Process Flow Diagram, identify which areas of security are applicable to Artemis Financial’s software application. Justify your reasoning for why each area is relevant to the software application.

Input Validation – Validation of user input will be necessary with the RESTful API.

APIs – Secure communication will be necessary because of the RESTful API.

Cryptography – Encryption is a must for proper security of personal information.

Client/Server – Secure communications between client and server with no interference.

Coding Errors – Improper input that causes errors must be secure.

Coding Quality – Quality will be a must for secure communication.

Encapsulation – Data structures must be secure for communications so no data is lost.

## 

## 3. Manual Review

Continue working through the Vulnerability Assessment Process Flow Diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

* Parameters that are requested are not validated
* No HTTPS
* Authentication is not used
* Encryption of the connection parameter should be done
* Use of business names in the CRUDController class for request 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 dependency check report. Include the following:

1. The names or vulnerability codes of the known vulnerabilities
2. A brief description and recommended solutions provided by the dependency check report
3. Attribution (if any) that documents how this vulnerability has been identified or documented previously

bcprov-jdk15on-1.46.jar (Legion of the Bouncy Castle) needs updates.

CVE-2018-1000613 (OSSINDEX)

CVE-2015-6644 (OSSINDEX)

CVE-2016-1000338

CVE-2016-1000342

CVE-2016-1000343

CVE-2016-1000344

CVE-2016-1000352

CVE-2016-1000341

CVE-2016-1000345

CVE-2017-13098

CVE-2020-15522

CVE-2016-1000339

CVE-2020-26939 (OSSINDEX)

CVE-2015-7940

CVE-2018-5382

CVE-2013-1624

CVE-2016-1000346

hibernate-validator-6.0.18.Final.jar allows attacks to bypass input sanitation

CVE-2020-10693

jackson-databind-2.10.2.jar data-binding functionality works on core streaming API

CVE-2020-25649

log4j-api-2.12.1.jar (Apache Log4j) update to most recent version

CVE-2020-9488

logback-core-1.2.3.jar code could be loaded from LDAP servers

CVE-2021-42550

snakeyaml-1.25.jar update to most recent version

CVE-2017-18640

spring-aop-5.2.3.RELEASE.jar update to most recent version

CVE-2016-1000027

CVE-2022-22965

CVE-2021-22118

CVE-2020-5421

CVE-2022-22950

CVE-2022-22968

CVE-2021-22060

CVE-2021-22096

spring-boot-2.2.4.RELEASE.jar update to most recent version

CVE-2022-27772

spring-core-5.2.3.RELEASE.jar update to most recent version

CVE-2016-1000027

CVE-2022-22965

CVE-2021-22118

CVE-2020-5421

CVE-2022-22950

CVE-2022-22968

CVE-2021-22060

CVE-2021-22096

tomcat-embed-core-9.0.30.jar update to most recent version

CVE-2020-1938

CVE-2020-11996

CVE-2020-13934

CVE-2020-13935

CVE-2020-17527

CVE-2021-25122

CVE-2021-41079

CVE-2021-42340 (OSSINDEX)

CVE-2020-9484

CVE-2021-25329

CVE-2021-30640

CVE-2021-24122

CVE-2021-33037

CVE-2019-17569

CVE-2020-1935

CVE-2020-13943

tomcat-embed-websocket-9.0.30.jar update to most recent version

CVE-2020-1938

CVE-2020-8022

CVE-2020-11996

CVE-2020-13934

CVE-2020-13935

CVE-2020-17527

CVE-2021-25122

CVE-2021-41079

CVE-2020-9484

CVE-2021-25329

CVE-2021-30640

CVE-2021-24122

CVE-2021-33037

CVE-2019-17569

CVE-2020-1935

CVE-2020-13943

## 5. Mitigation Plan

After interpreting your results from the manual review and static testing, identify the steps to remedy the identified security vulnerabilities for Artemis Financial’s software application.

* Require two factor authentications
* Update dependencies to most recent versions
* Use HTTPS for communications
* Encryption of connections credentials
* Validate requested parameters by moving to head or body

**Citations**

Staff, the P. N. O., & This blog is a collaboration between CTO and DPIP staff and the AI Strategy team. (2020, July 16). *Financial Institutions and customer information: Complying with the Safeguards Rule*. Federal Trade Commission. Retrieved May 19, 2022, from https://www.ftc.gov/business-guidance/resources/financial-institutions-customer-information-complying-safeguards-rule