****

# 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** | **09/19/2023** | **Justin Murray** | **Created document and ran dependency check** |

## Client



## Instructions

Submit this completed vulnerability assessment report. Replace the bracketed text with the relevant information. In the report, identify your findings of security vulnerabilities and provide recommendations for 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 choose to include images or supporting materials. If you include them, make certain to insert them in all 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

Justin Murray

## Interpreting Client Needs

Artemis Financial is a company centered around financial planning such as saving, retirement, investments, and insurance for their clientele. This means that as they modernize their company, software security be a top priority to provide protection for themselves and their clients. Secure communication would be a must have to guarantee data protection for their clients. Since they are a financial institution, they must follow government banking regulations for all communication as well as transaction and any other actions taken between the client and themselves. Any threats to the database would be attackers looking for sensitive information allowing them to control someone or get control of their assets and would need higher measures to prevent information leaks.

## Areas of Security

Major areas to focus on from the Vulnerability Assessment Process Flow Diagram are

Input validation – Need focus on input validation because the REST API receives user input, the user input should be validated.

APIS – The REST API used for secure communication is a strong asset to the overall design.

Cryptography – end to end encryption would ensure if it got intercepted it would be harder to access the information

Code Quality – If we can develop the code from the start with a strong security purpose in mind and create a quality product at a level of security that prevents outside inference to communication between the client and company.

## Manual Review

* The service is not currently using HTTPS which is the recommended when dealing with sensitive information
* There is currently no authentication.
* The request parameter for business names in Crudcontroller is vulnerable to leaks
* Needs better validation for input

## Static Testing

A screenshot of a computer

Description automatically generated

bcprov-jdk15on-1.46.jar- The Bouncy Castle Crypto package is a Java implementation of

cryptographic algorithms. This jar contains JCE provider and lightweight API for the Bouncy

Castle Cryptography APIs for JDK 1.5 to JDK 1.7.

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-2020-0187

CVE-2016-1000339

CVE-2020-26939

CVE-2015-7940

CVE-2018-5382

CVE-2013-1624

CVE-2016-1000346

snakeyaml-1.25.jar- YAML 1.1 parser and emitter for Java

CVE-2017-18640

CVE-2022-25857

CVE-2022-38749

CVE-2022-38751

spring-boot-2.2.4.RELEASE.jar- Spring Boot

CVE-2022-27772

spring-core-5.2.3.RELEASE.jar- Spring Core

CVE-2022-22965

CVE-2021-22118

CVE-2020-5421

CVE-2022-22950

CVE-2022-22971

CVE-2022-22968

CVE-2022-22970

CVE-2021-22060

CVE-2021-22096

spring-web-5.2.3.RELEASE.jar- Spring Web

CVE-2016-1000027

CVE-2021-22118

CVE-2020-5421

CVE-2022-22950

CVE-2022-22971

CVE-2022-22968

CVE-2022-22970

CVE-2021-22060

CVE-2021-22096

## Mitigation Plan

To start address the vulnerabilities found and progress the company towards its goal of modernization we need to start by switching the structure of the code over to HTTPS for the added security, add in better input validation and authentication of the user for access to their information. We need to update all the current vulnerabilities and then run another dependency check.