****

# 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** | **5/21/2023** | **Adela Martinez** |  |

## 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

Adela Martinez

## Interpreting Client Needs

The client, Artemis Financial, is a company that helps develop customed financial plans for their customers that include savings, investment, retirement, and insurance. Artemis Financial uses a RESTful web-based API programming application interface. They they are dealing with their client’s financials, they have access to sensitive information that would include SSN numbers, account numbers, tax information. They would like to have the most current and effective software security to protect from external threats that could steal sensitive information from their clients.

## Areas of Security

Input Validation – users need to input their information to validate their account.

API – An API is needed to run the program and to access data externally.

Code Quality – the quality of the code needs to be up to par to maintain the security of the program.

Code Error – making sure that any issues or code errors are attended to and fixed.

Cryptography – to ensure information and data are encrypted to protect against vulnerabilities.

## Manual Review

After overlooking the code there were no signs of cryptography to help encrypt the data and protect it from outside sources. As for input validation, there was no authentication in the code to verify user’s information entered is correct. On the pom.xml file I noticed that the Spring Framework shows an outdated version and that needs to be updated.

## Static Testing

* [bcprov-jdk15on-1.46.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l1_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7)
  + Description: 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.
  + Solution: Update Bouncy Castle to the most updated version.
* [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l3_7fd00bcd87e14b6ba66279282ef15efa30dd2492)
  + Description: Hibernate's Bean Validation (JSR-380) reference implementation.
  + Solution: Update hibernate-validator to current version
* [jackson-databind-2.10.2.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l5_0528de95f198afafbcfb0c09d2e43b6e0ea663ec)
  + Description: General data-binding functionality for Jackson: works on core streaming API
  + Solution: Update to current version
* [log4j-api-2.12.1.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l10_a55e6d987f50a515c9260b0451b4fa217dc539cb)
  + Description: The Apache Log4j API
  + Solution: Update to the most recent version
* [logback-core-1.2.3.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l12_864344400c3d4d92dfeb0a305dc87d953677c03c)
  + Description: logback-core module
  + Solution: Update to the most recent version
* [snakeyaml-1.25.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l14_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421)
  + Description: YAML 1.1 parser and emitter for Java
  + Solution: Update to most recent system
* [spring-boot-2.2.4.RELEASE.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l15_225a4fd31156c254e3bb92adb42ee8c6de812714)
  + Description: Spring Boot
  + Solution: Update to current version
* [spring-boot-autoconfigure-2.2.4.RELEASE.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l16_36d2bb5d0eeb616eb84f754c4076b30e6b61614c)
  + Description: Spring Boot AutoConfigure
  + Solution: Update to current version
* [spring-boot-starter-web-2.2.4.RELEASE.ja](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l17_ec75d01d212b5229c16d872fb127744c0ed46ed8)r
  + Description: Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container
  + Solution: Update to current version
* [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l18_3734223040040e8c3fecd5faa3ae8a1ed6da146b)
  + Description: Spring Core
  + Solution: Upgrade to current version
* [spring-web-5.2.3.RELEASE.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l19_dd386a02e40b915ab400a3bf9f586d2dc4c0852c)
  + Description: Spring Web
  + Solution: Update to current version
* [spring-webmvc-5.2.3.RELEASE.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l20_745a62502023d2496b565b7fe102bb1ee229d6b7)
  + Description: Spring Web MVC
  + Solution: Update to current version
* [tomcat-embed-core-9.0.30.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l21_ad32909314fe2ba02cec036434c0addd19bcc580)
  + Description: Core Tomcat implementation
  + Solution: Update to current version
* [tomcat-embed-websocket-9.0.30.jar](file:///C:\Users\amart\eclipse-workspace\CS%20305%20Project%20One%20Code%20Base.zip_expanded\rest-service\target\dependency-check-report.html#l23_33157f6bc5bfd03380ebb5ac476db0600a04168d)
  + Description: Core Tomcat implementation
  + Solution: Update to current version

## Mitigation Plan

After overlooking all the vulnerabilities from the static testing, the mitigation plan is to update everything that came up on the dependency check report to the most current version. After updating everything I will run another dependency check to make sure all the vulnerabilities have cleared and focus on maintaining the code to make sure it is always secured.