****

# 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** | **March 24,2024** | **Jessica Bains** |  |

## 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

Jessica Bains

## Interpreting Client Needs

1. What is the value of secure communications to the company?

Artemis Financial is a consulting company that develops plans like savings, retirement, investment, and insurance for their customers. Artemis Financial has a RESTful web application programming interface. It is crucial for the company to have secure communication since there will be exchange of sensitive information like SSN, address, tax information, credit card information, etc.

1. Does the company make any international transactions?

The software is designed for entrepreneurs, businesses, and government agencies all around the world so it is safe to assume that they might make international transactions. Artemis Financial wants the customers to be able to trust the company with their personal information. They want to use the most current and effective software security to protect their organization from external threats.

1. Are there governmental restrictions about secure communications to consider?

It is important to consider government restrictions, adhering to local and international mandates and regulatory frameworks to ensure compliance and avoid legal issues.

1. What external threats might be present now and in the immediate future?

Some external threats that might be present now and in the immediate future for Artemis Financial can be cDDoS attacks, phishing, malware, software vulnerabilities and data breaches.

1. What are the modernization requirements that you must consider? For example:

The usage of open-source libraries may speed development but it can bring new vulnerabilities if it’s not updated and maintained. Evolving web application technologies can offer improved functionality and security but will still need to updated.

## Areas of Security

**API:** Artemis Financial has RESTful API so it is important to protect the sensitive information from being stolen. Measures like authentication and authentication can be taken.

**Input validation:** Input validation helps secure the API by making sure that the input received is valid and correct before allowing further processing. It can help validate customers and associates login credentials, and keep financial data and personal information safe.

**Code quality:** Code quality measures the quality of the code. Having a high quality code is more resistant to errors and bugs, and makes it easier to read, modify and maintain the code.

**Code error:** Errors in code can lead to security vulnerabilities so it important to handle it securely.

**Cryptography:** Cryptography can secure information and communication by using codes so only the intended parties can access the information. This can prevent malicious eavesdropping and tampering.

## Manual Review

During my manual review I noticed multiple vulnerabilities within the code.

1. I first looked for input validation. I checked the the pom.xml file in the given code for Apache validator. Then, I checked the GreetingController, the input here did not use any sort of validation. I was not able to validate because there was no output.
2. There was no API and I was able to access data. Input needs to be handled by post method instead of URL.
3. There were no signs of cryptography being used.
4. For code errors, DocData.java had no error handling and had a try and catch block.
5. The code quality was okay. It is lacking API and input validation. Input needs to be handled by post method instead of URL.

## Static Testing

### bcprov-jdk15on-1.46.jar

**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 bouncycastle to Version update to 1.60

**bcprov-jdk15on-1.46.jar**

**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 bouncycastle to Version update to 1.60

### spring-boot-starter-web-2.2.4.RELEASE.jar

### Description: Starter for building web, including RESTful, applications using Spring MVC. Uses Tomcat as the default embedded container

**Solution:** Upgrade to current version

**spring-boot-2.2.4.RELEASE.jar**

**Description:** Spring Boot

**Solution:** Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+.

**snakeyaml-1.25.jar**

**Description:** YAML 1.1 parser and emitter for Java

**Solution:** Use SnakeYaml's SafeConsturctor when parsing untrusted content to restrict deserialization. We recommend upgrading to version 2.0 and beyond.

**logback-core-1.2.3.jar**

**Description:** logback-core module

**Solution:** Upgrade to 2.13.2 which supports this feature. property mail.smtp.ssl.checkserveridentity to true to globally enable hostname verification for SMTPS connections.

**jackson-databind-2.10.2.jar**

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

**Solution:** Upgrade to current version

**hibernate-validator-6.0.18.Final.jar**

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

**Solution:** Upgrade to hibernate-validator-6.0.20

## 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.

The step to remedy the identified security vulnerabilities is upgrading the systems to their most current versions. I would implement input validation. I would also add API and move the input from URL to post method to secure the data.