****

# 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** | **05/22/2023** | **Hong Luu** | **Added section 1 to 5** |

## 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

Hong Luu

## Interpreting Client Needs

* **What is the value of secure communications to the company?** Secure communications are highly valuable to Artemis Financial as they ensure the confidentiality, integrity, and authenticity of sensitive financial data exchanged with clients and partners. Protecting communication channels from unauthorized access and data breaches is essential to maintain trust and prevent financial fraud.
* **Does the company make any international transactions?** If Artemis Financial engages in international transactions, it is important to consider any governmental restrictions or regulations related to secure communications. Compliance with international data protection laws and privacy regulations is necessary to ensure the lawful transfer and protection of sensitive financial information across borders.
* **Are there governmental restrictions about secure communications to consider?** Depending on the geographical locations where Artemis Financial operates, there may be specific governmental restrictions or industry regulations governing secure communications. Adhering to these requirements is essential for maintaining compliance and avoiding legal and reputational risks.
* **What external threats might be present now and in the immediate future?** The web application of Artemis Financial should be subject to an analysis of potential external risks, both present and future. These dangers can take the form of sophisticated cyber-attacks, data breaches, phishing scams, ransomware, and other malicious activities. For security measures to be put in place effectively, it is essential to comprehend the evolving threat circumstance.
* **What are the modernization requirements that you must consider?** The vulnerability assessment should address the need for modernization while considering the function of open-source libraries and the potential dangers they pose. It's critical to evaluate how open-source components are being used and make sure they receive regular updates to fix any identified vulnerabilities. Additionally, the evaluation should consider developing web application technologies, including secure coding procedures, consistent security upgrades, and keeping up with new security threats and mitigation techniques.

## Areas of Security

After evaluating Artemis Financial's web application, the following areas of security are relevant:

* **Architecture Review**: Assessing the application's architecture ensures that it is designed in a secure and robust manner, considering factors like data flow, component interaction, and system integration.
* **Input Validation:** Implementing secure input validation is crucial to prevent malicious input from compromising the application's functionality and introducing vulnerabilities.
* **APIs:** Securing API interactions is important to protect sensitive data transmitted between the application and external systems, ensuring proper authentication, access control, and data encryption.
* **Cryptography:** Proper encryption usage is essential to protect confidential information, such as customer financial data, and mitigate vulnerabilities related to encryption algorithms and key management.
* **Client/Server Security:** Ensuring secure communication and data exchange between the client and server components is vital to prevent unauthorized access, tampering, and data breaches.
* **Code Error Handling:** Implementing secure code handling practices helps prevent information leakage and reduces the risk of exploitation by handling errors and exceptions securely.

## Manual Review

Based on the provided dependency check report, the vulnerabilities identified in the Project One Code Base are as follows:

* Architecture Review: No specific vulnerabilities related to the overall architecture were identified in the report.
* Input Validation: No specific vulnerabilities related to input validation were identified in the report.
* APIs: Secure API Interactions:

Vulnerabilities found in the following packages:

bcprov-jdk15on-1.46.jar

hibernate-validator-6.0.18.Final.jar

jackson-databind-2.10.2.jar

snakeyaml-1.25.jar

spring-boot-2.2.4.RELEASE.jar

spring-boot-autoconfigure-2.2.4.RELEASE.jar

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

spring-core-5.2.3.RELEASE.jar

spring-web-5.2.3.RELEASE.jar

spring-webmvc-5.2.3.RELEASE.jar

tomcat-embed-core-9.0.30.jar

tomcat-embed-websocket-9.0.30.jar

* Cryptography: Encryption Use and Vulnerabilities:

Vulnerabilities found in the bcprov-jdk15on-1.46.jar package.

* Client/Server: Secure Distributed Composing:

No specific vulnerabilities related to client/server interactions were identified in the report.

* Code Error: Secure Code Handling: No specific vulnerabilities related to code errors were identified in the report.
* Code Quality: Secure Coding Practices/Patterns:

Vulnerabilities found in the log4j-api-2.12.1.jar, logback-core-1.2.3.jar, snakeyaml-1.25.jar, spring-core-5.2.3.RELEASE.jar, spring-web-5.2.3.RELEASE.jar, spring-webmvc-5.2.3.RELEASE.jar, tomcat-embed-core-9.0.30.jar, and tomcat-embed-websocket-9.0.30.jar packages.

## Static Testing

After integrating the dependency-check plugin into Maven and running a dependency check on Artemis Financial's software application, the following vulnerabilities were identified:

**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.

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

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

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

Recommendation: It is recommended to update the library to the latest version to address this vulnerability.

**jackson-databind-2.10.2.jar:**

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

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

**log4j-api-2.12.1.jar:**

Description: The Apache Log4j API.

Recommendation: It is recommended to update the library to the latest version to address this vulnerability.

**logback-core-1.2.3.jar:**

Description: logback-core module

Recommendation: It is recommended to update the library to the latest version to address this vulnerability.

**snakeyaml-1.25.jar:**

Description: YAML 1.1 parser and emitter for Java.

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

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

Description: Spring Boot

Recommendation: It is recommended to update the library to the latest version to address this vulnerability.

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

Description: Spring Boot AutoConfigure

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

**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.

Recommendation: It is recommended to update the library to the latest version to address this vulnerability.

**spring-core-5.2.3.RELEASE.jar:**

Description: Spring Core

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

**spring-web-5.2.3.RELEASE.jar:**

Description: Spring Web

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

**spring-webmvc-5.2.3.RELEASE.jar:**

Description: Spring Web MVC

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

**tomcat-embed-core-9.0.30.jar:**

Description: Core Tomcat implementation

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

**tomcat-embed-websocket-9.0.30.jar:**

Description: Core Tomcat implementation

Recommendation: It is recommended to update the library to the latest version to address these vulnerabilities.

## Mitigation Plan

**Dependency: bcprov-jdk15on-1.46.jar**

Action: Update the bcprov-jdk15on library to the latest version to address the 17 high-severity vulnerabilities.

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

Action: Update the hibernate-validator library to the latest version to address the medium-severity vulnerability.

**Dependency: jackson-databind-2.10.2.jar**

Action: Update the jackson-databind library to the latest version to address the 5 high-severity vulnerabilities.

**Dependency: log4j-api-2.12.1.jar**

Action: Update the log4j-api library to the latest version to address the low-severity vulnerability.

**Dependency: logback-core-1.2.3.jar**

Action: Update the logback-core library to the latest version to address the medium-severity vulnerability.

**Dependency: snakeyaml-1.25.jar**

Action: Update the snakeyaml library to the latest version to address the critical-severity vulnerability.

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

Action: Update the spring-boot library to the latest version to address the high-severity vulnerability.

**Dependency: spring-boot-autoconfigure-2.2.4.RELEASE.jar**

Action: Update the spring-boot-autoconfigure library to the latest version to address the high-severity vulnerabilities.

**Dependency: spring-boot-starter-web-2.2.4.RELEASE.jar**

Action: Update the spring-boot-starter-web library to the latest version to address the high-severity vulnerability.

**Dependency: spring-core-5.2.3.RELEASE.jar**

Action: Update the spring-core library to the latest version to address the critical-severity vulnerabilities.

**Dependency: spring-web-5.2.3.RELEASE.jar**

Action: Update the spring-web library to the latest version to address the critical-severity vulnerabilities.

**Dependency: spring-webmvc-5.2.3.RELEASE.jar**

Action: Update the spring-webmvc library to the latest version to address the critical-severity vulnerabilities.

**Dependency: tomcat-embed-core-9.0.30.jar**

Action: Update the tomcat-embed-core library to the latest version to address the critical-severity vulnerabilities.

**Dependency: tomcat-embed-websocket-9.0.30.jar**

Action: Update the tomcat-embed-websocket library to the latest version to address the critical-severity vulnerabilities.