****

# 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 5](#_Toc32574614)

[5. Mitigation Plan 6](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **12/27/22** | **Theresa Vassell** |  |

## 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

Theresa Vassell

## Interpreting Client Needs

Artemis Financial is a company that devises financial plans for individuals ranging from savings, and

retirements to investments and insurance.

Artemis Financial is a company that devises financial plans for individuals ranging from savings, and

retirements to investments and insurance.

Artemis Financial is a consulting company that develops individualized financial plans for their customers. The financial plans include savings, retirement, investments, and insurance. Artemis Financial is seeking to modernize their operations. They wish to Utilize Global Rain’s expertise on how to protect the organization from external threats. In order to do this, they want to use the most current and effective software security so that they will have a secure form of communication between their clients and the organization. Having a secured communication channel is very valuable to Artemis Financial as being that they deal with highly sensitive data that need to be protected.

It is safe to assume that Artemis Financial is not solely US based and that they most likely handle international transactions. I do not believe that there are government restrictions on secure communications as the government would want these companies to be able to effectively secure their client’s data and privacy. Considering that Artemis financial deals with clients finances they would be likely targets for hackers trying to gain access to their client’s personal information for financial gain. One modernization requirement to consider would be to incorporate open-source libraries into their program to improve functionality and the use of web application technologies to improve organization functions such as communication and finances. It would also be wise to have an IT team on staff in order to perform routine security tasks.

## Areas of Security

**API’s** - APIs would allow for the control of the flow and accessibility of data to different systems, applications, and devices.

**Cryptography** – This will allow for the proper encryption of data that is being communicated between the client and the organization.

**Input** **validation** – This will be used to validate client information assuring user protection. This is in part due to how susceptible RESTful is to security breaches.

**Code** **Quality** – The practice of secure coding will allow for a lower potential of a security breach.

## Manual Review

During my manual review of the project one base code, I have identified some vulnerabilities within the POM.XML and Greeting controller files.

* There is no use pf cryptography
* There is no use of HTTPS and considering that information is being shared over the internet it is needed.
* There is no method for authentication or input verification present to verify users.
* Error handling was not present in code.

## Static Testing

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Description | Recommendation | Attributes (If any) |
| 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. | update bouncycastle to: Version update to 1.60. | CVE Count 17. |
| hibernate-validator-6.0.18.Final.jar | Hibernate's Bean Validation (JSR-380) reference implementation. | Upgrade to hibernate-validator- 6.0.20. | CVE Count 1. |
| jackson-databind-2.10.2.jar | General data-binding functionality for Jackson works on core streaming API | Upgrade to current version  Upgrade to current version  Upgrade to current version. | CVE Count 4. |
| log4j-api-2.12.1.jar | The Apache Log4j API | Update to most recent version. | CVE Count 1. |
| logback-core-1.2.3.jar | logback-core module | Update to most recent version. | CVE Count 1. |
| snakeyaml-1.25.jar | YAML 1.1 parser and emitter for Java | Migrate to SnakeYAML Engine. | CVE Count 8. |
| spring-boot-2.2.4.RELEASE.jar | Spring Boot | Upgrade to current version. | CVE Count 1. |
| spring-core-5.2.3.RELEASE.jar | Spring Core | Upgrade to current version. | CVE Count 9. |
| spring-web-5.2.3.RELEASE.jar | Spring Web | Upgrade to current version. | CVE Count 10. |
| tomcat-embed-core-9.0.30.jar | Core Tomcat implementation | Upgrade to Apache Tomcat 10.0.6  or late  Upgrade to Apache Tomcat 10.0.6  or late  Upgrade to Apache Tomcat 10.0.6 or later. | CVE Count 19. |
| tomcat-embed-websocket-9.0.30.jar | Core Tomcat implementation | Upgrade to Apache Tomcat 10.0.6 or later. | CVE Count 20. |
|  |  |  |  |

## Mitigation Plan

After reviewing the results of the manual review and the static testing report, I have identified some steps to mitigate the security vulnerabilities.

* Add HTTPS to the code in order to secure data being sent over the web.
* Incorporate user authentication
* Update systems to their current versions
* Include request parameters in the body