****

# 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** | **[Date]** | **[Your name]** |  |

## 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

Urika Pye

## Interpreting Client Needs

Artemis Financial is needing their software of individualized financial plans reviewed for security threats. The value of secure communications would bring the ability to take financial documents from customers, when uploaded, and secure it from external threats, such as hackers. This would ensure the company’s reputation is not hindered by a data breach. Artemis Financials work with various businesses, entrepreneurs, and government agencies. They have 74 vulnerabilities found when running the dependency check and 13 vulnerable dependencies; thus, they have external threats that could become an issue from these vulnerabilities alone. To combat this, I would exclude the 13 dependencies below (in the screenshot), due to the vulnerabilities they pose.

## Areas of Security

They have a dependency that pose a threat to the Cryptography of the information being collected. Input validation, APIs, client/server, and code error is also at risk with the listed dependencies. Cryptography is at risk due to the bcprov-jdk15on-1.46.jar dependency, specifically the CVE-2017-13098. Input validation is at risk due to the log4j-api-2.12.1.jar, specifically the CVE-2021-44832. APIs are at risk due to the Jackson-databind-2.10.2.jar, specifically the CVE-2021-24122. The client/server is at risk due to the tomcat-embed-core-9.0.30.jar, specifically the CVE-2021-43980, and the spring-boot-2.2.4.RELEASE.jar, specifically the CVE-2022-27772. Lastly, code error is a risk due to the bcprov-jdk15on-1.46.jar, specifically the CVE-2016-10000346.

## Manual Review

When looking at the CRUD.java file, there aren’t any parameters to ensure the user is uploading valid input, and it’s the same for the CRUDController.java file; where the spring boot framework is being imported and has a known vulnerability. The account number and account balance isn’t being hashed in any way to protect user input in the customer.java file. The spring boot framework listed in the dependency check above is used in the RestServiceApplication.java file, so that puts the client/server at risk for that reason.

## Static Testing

A screenshot of a computer

Description automatically generated

The dependencies that are vulnerable are listed above. The solution to wipeout these vulnerabilities are to do away with these dependencies and hard code what they should do to ensure security of the application.

## Mitigation Plan

To mitigate these vulnerabilities, I would pose for Artemis Financials to deprecate the dependencies found in the dependency check report, and for them to have their developers hard code what those dependencies should do; that way they can use the DevSecOps approach to securely code the application, securely test the code being implemented, and then deploy the application for use; if the data they carry on their servers were to get breached, they would lose out on the government contracts and the contracts with other businesses and entrepreneurs because they put their reputation at risk along with their own.