****

# 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

[Olorunjuwon Olutoki.]

## Interpreting Client Needs

Artemis Financial wants to modernize their operations of financial planning for their customers. Financial information is highly sensitive, communication between the company and their customers must be secure. The company must follow government regulations for financial transactions and communications, which will affect security requirements and policies. Artemis Finacial’s API’s are vulnerable to interception if the responses and requests are not secured. They must use HTTPS for all communications and send confidential information for all responses,

## Areas of Security

API’s – RESTful API will need to communicate securely for the web service.

Code Error – User input errors must be secure.

Input Validation - The input will need to be validated so RESTful API will accept the user input.

Secure Coding

## Manual Review

Service doesn’t use HTTPS.

Request parameters aren’t validated.

An authentication scheme isn’t present.

In the CRUD Controller class, business names are sent as request parameters.

## Static Testing

Bouncy castle has several vulnerabilities. Recommend updating.

- CVE-2016-1000352

- CVE-2016-1000346

- CVE-2016-1000345

- CVE-2016-1000344

- CVE-2016-1000343

- CVE-2016-1000342

- CVE-2016-1000341

- CVE-2016-1000339

- CVE-2016-1000338

- CVE-2018-5382

- CVE-2017-13098

- CVE-2013-1624

FasterXML Jackson Data bind 2.10.2 Recommend updating.

- CVE-2023-35116

- CVE-2021-46877

- CVE-2022-42004

- CVE-2022-42003

- CVE-2020-36518

- CVE-2016-1000338

- CVE-2018-5382

- CVE-2017-13098

- CVE-2013-1624

FasterXML Jackson Data bind 2.10.2 Recommend updating.

- CVE-2023-35116

- CVE-2021-46877

- CVE-2022-42004

- CVE-2022-42003

- CVE-2020-36518

- CVE-2020-25649

Apache Log 4j API 2.12.1 has 5 vulnerabilities. Recommend updating.

- CVE-2021-44832

- CVE-2021-45105

- CVE-2021-45046

- CVE-2021-44228

- CVE-2020-9488

SnakeYAML 1.25 has 8 vulnerabilities. Recommend updating.

- CVE-2022-1471

- CVE-2022-41854

- CVE-2022-38752

- CVE-2022-38751

- CVE-2022-38750

- CVE-2022-38749

- CVE-2022-25857

- CVE-2017-18640

Apache Tomcat 9.0.30 has 20 vulnerabilities. Recommend updating.

- CVE-2023-46589

- CVE-2023-45648

- CVE-2023-427956

- CVE-2023-44487

- CVE-2023-41080

- CVE-2023-28708

- CVE-2022-42252

- CVE-2022-34305

- CVE-2021-43980

- CVE-2022-29885

- CVE-2021-41079

- CVE-2021-33037

- CVE-2021-30640

- CVE-2021-25329

- CVE-2021-25122

## Mitigation Plan

Use HTTPS protocol for communications.

Instead of URI move request parameters to headers or body.

Implement authentication scheme.

Update dependencies.