****

# 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 5](#_Toc32574613)

[4. Static Testing 5](#_Toc32574614)

[5. Mitigation Plan 6](#_Toc32574615)

6. References.............................................................................................................................................7

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.01** | **3/15/2023** | **Frederick Wahab** | **CS-305 Project One** |

## 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

Frederick Wahab

## Interpreting Client Needs

Artemis Financial is an independent wealth management firm that focuses on serving private clients with all financial needs. Aside from traditional financial portfolios, they offer sustainable investment options including insurance, investments, savings, and retirement. As an institution that put the safety and security of its clients first, Artemis Financial has tasked Global Rain with modernizing its operations to protect against external threats. Global Rain will review Artemis Financial’s web-based software application that interacts with a RESTful API to identify any security vulnerabilities.

## Areas of Security

* **Input Validation –** This is often the primary focus from external threats which makes it the highest priority in security. Properly validating input includes restricting input variables to a specific type and a limited character length. Java can also utilize external security libraries that prevent known string exploits from being entered into the application. Input Validation can be exploited by injection attacks, cross-site scripting attacks, canonicalization attacks, and buffer overflow attacks (Fitzgibbons, 2019).
* **APIs –** Since Artemis Financial’s web-based software application does interact with a RESTful API, the security of the API will need to be assessed. The API should have a simple structure with all external component easily identifiable and known. It should also include a zero-trust policy from external applications and proper privilege management requiring multiple conditions to access sensitive content. RESTful API vulnerabilities include access control/authorization compromise, code injection, replay attacks, and DDoS attacks (*REST API Security - Why It Matters to Be Secure*, n.d.).
* **Cryptography –** The transmission of sensitive data can provide an opportunity for attacks if not properly secured. This process includes implementing strong security protocols, generating effective security keys with a limited lifespan, and limiting the amount of plain text known to characters. Cryptography vulnerabilities include plaintext attacks, ciphertext attacks, differential cryptanalysis attacks, and brute force attacks (Muqeet, 2018).
* **Code Quality/ Error free –** One of the main ways to prevent security violations in the application is to address security in every phase of a software development life cycle. To ensure proper code quality, during the development phase, it is important to use industry standard coding conventions, adopt continuous integration, and leave detailed comments (Ghani, 2022). Coding errors need to be identified prior to publishing any phase of the application. This includes addressing compilation errors, utilizing certified error scan tools, and manually reviewing all code. While code quality and code error review can be done simultaneously, it is important to address them individually to improve any additional code that will be developed in the future.

## Manual Review

After performing a manual review of the Artemis Financial web-based software application, a couple of security vulnerabilities have been identified. In lines 15 -18 of the GreetingController.java file, input is received and formatted into the template without input validation. This is also a concern for the business name value in the CRUDController.java file, line 13. Finally, in the DocData.java file, line 27 has the database path with the username and password in plain text.

## Static Testing

Graphical user interface, text, application, email

Description automatically generated

|  |  |  |
| --- | --- | --- |
| **Vulnerabilty IDs** | **Resolution** | **Attribution** |
| cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.46:\*:\*:\*:\*:\*:\*:\* cpe:2.3:a:bouncycastle:bouncy\_castle\_crypto\_package:1.46:\*:\*:\*:\*:\*:\*:\* cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:\*:\*:\*:\*:\*:\*:\* cpe:2.3:a:bouncycastle:the\_bouncy\_castle\_crypto\_package\_for\_java:1.46:\*:\*:\*:\*:\*:\*:\* | Update to bcprov-jdk15on-1.60 or newer | <https://access.redhat.com/errata/RHSA-2018:2669> |
| cpe:2.3:a:redhat:hibernate\_validator:6.0.18:\*:\*:\*:\*:\*:\*:\* | Update to hibernate-validator-6.1.5 or newer | <https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10693> |
| cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\* cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | Update to Jackson-databind-2.13.4 or newer | <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50490> |
| cpe:2.3:a:apache:log4j:2.12.1:\*:\*:\*:\*:\*:\*:\* | Update log4j-api-2.12.1.jar to version 2.13.2 or newer | <https://lists.debian.org/debian-lts-announce/2022/11/msg00035.html> |
| cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\* | Update logback-core-1.2.3.jar to version 1.2.9 or newer | <https://jira.qos.ch/browse/LOGBACK-1591> |
| cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25:\*:\*:\*:\*:\*:\*:\* | Update to snakeyaml-1.3.1 or newer | <https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=50355> |
| cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\* | Update to spring-boot-2.2.11 or newer | <https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85> |
| cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:web\_project:web:2.2.4:release:\*:\*:\*:\*:\*:\* | Update to spring-boot-2.2.11 or newer | <https://github.com/JLLeitschuh/security-research/security/advisories/GHSA-cm59-pr5q-cw85> |
| cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:vmware:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* | Update spring-core-5.2.3.RELEASE.jar to version 5.3.2 or newer | <https://security.netapp.com/advisory/ntap-20220616-0003/> |
| cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:vmware:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:web\_project:web:5.2.3:release:\*:\*:\*:\*:\*:\* | Update to spring-boot-2.2.11 or newer | <https://security.netapp.com/advisory/ntap-20220616-0003/> |
| cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:vmware:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\* cpe:2.3:a:web\_project:web:5.2.3:release:\*:\*:\*:\*:\*:\* | Update to spring-boot-2.2.11 or newer | <https://security.netapp.com/advisory/ntap-20220616-0003/> |
| cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\* cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\* | Update to apache\_tomcat-9.0.68 or newer and insure rejectIllegalHeader is set to true | <https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq> |
| cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\* cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\* | Update to apache\_tomcat-9.0.68 or newer and insure rejectIllegalHeader is set to true | <https://lists.apache.org/thread/zzcxzvqfdqn515zfs3dxb7n8gty589sq> |

## Mitigation Plan

The manual and stat testing on the Artemins Financial web-based software application has resulted in several identifiable security vulnerabilities. Please make the following changes to the application to fix those vulnerabilities and ensure the security of Financial Artemis and its clients.

* Add input validation to the GreetingsController.java file and CRUDController.java files using both code written in the functions and using an input validation library.
* Encrypt the database path in DocData.java file.
* Update all dependency to at least their minimum recommended version and complete any additional requirements in the resolution portion of the stat test analysis.

**References**

Fitzgibbons, L. (2019, June 25). *input validation attack*. WhatIs.com. <https://www.techtarget.com/whatis/definition/input-validation-attack#:~:text=An%20input%20validation%20attack%20is,a%20normal%20user%20input%20field>.

Ghani, U. (2022, January 13). *4 tips to improve code quality*. Work Life by Atlassian. <https://www.atlassian.com/blog/add-ons/4-tips-to-improve-code-quality>

Muqeet, B. (2018, November 4). *Cryptography Vulnerabilities - Guide for Beginners*. PrivacyEnd. <https://www.privacyend.com/cryptography-vulnerabilities/>

*REST API Security - Why It Matters To Be Secure*. (n.d.). <https://www.gravitee.io/blog/rest-api-security-why-it-matters-to-be-secure>