****

# CS 305 Project One

**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** | **03/20/2022** | **Aws Albayati** |  |
| **1.1** | **01/22/2023** | **Aws Albayati** |  |

## Client



## Instructions

Deliver this completed vulnerability assessment report, identifying your findings of security vulnerabilities and articulating recommendations for the next steps to remedy the issues you have found.

Respond to the five steps outlined below and include your findings. Replace the bracketed text on all pages with your own words. If you choose to include images or supporting materials, be sure to insert them throughout.

## Developer

Aws Albayati

## 1. Interpreting Client Needs

It’s very important to keep communication safe to protect the client's information. Since Artemis Financial is a global financial consulting company that makes international transactions, it is an obligation to keep all client information confidential. While there are no government restrictions to consider building the safety requirements base on modern standards is a priority. It’s also important to be alert for any external threats such as spyware, adware, SQL injection and other attacks.

## 2. Areas of Security

* Input Validation: The project is a command input app and it's very important to validate all inputs to prevent any un-secure injection by hackers.
* APIs: Validate APIs and restrict their use when allowing access to the application from outside the system.
* Cryptography: Valid encryption and decryption of data applications especially on APIs to prevent keeping the data safe.
* Client/Server: To Secure all HTTP requests validation of certificate is required
* Code Error: Code reviews the entire project to find any Code errors that cause volubility in security.

## 3. Manual Review

* The Spring Data Rest version is outdated and probably missing some of the important security patches. In pom.xml file, overriding the version in line 42 to an old version 2.6.5. According to spring.io website article “Security issue in Spring Data REST”, in version 2.6.5 there is a security vulnerability allowing arbitrary code execution. The vulnerability has been fixed in version 2.6.9 and up. It’s highly recommended to update the Spring Data Rest version to the latest version as soon as possible.

## 4. Static Testing

|  |  |
| --- | --- |
| hibernate-validator-6.0.18.Final.jar | CVE-2020-10693A flaw was found in Hibernate Validator version 6.1.2.Final. A bug in the message interpolation processor enables invalid EL expressions to be evaluated as if they were valid. This flaw allows attackers to bypass input sanitation (escaping, stripping) controls that developers may have put in place when handling user-controlled data in error messages. |
| jackson-databind-2.10.2.jar | CVE-2020-25649 A flaw was found in FasterXML Jackson Databind, where it did not have entity expansion secured properly. This flaw allows vulnerability to XML external entity (XXE) attacks. The highest threat from this vulnerability is data integrity.CWE-611 Improper Restriction of XML External Entity Reference ('XXE') |
| log4j-api-2.12.1.jar | CVE-2020-9488 Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender. Fixed in Apache Log4j 2.12.3 and 2.13.1 |
| logback-core-1.2.3.jar | CVE-2021-4255In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configuration files could craft a malicious configuration allowing to execute of arbitrary code loaded from LDAP servers.0 |
| snakeyaml-1.25.jar | CVE-2017-18640 The Alias feature in SnakeYAML 1.18 allows entity expansion during a load operation, a related issue to CVE-2003-1564. |
| spring-aop-5.2.3.RELEASE.jar | CVE-2020-5421In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of path parameter. |
| tomcat-embed-core-9.0.30.jar | CVE-2019-17569The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely. |
| tomcat-embed-websocket-9.0.30.jar | CVE-2019-17569The refactoring present in Apache Tomcat 9.0.28 to 9.0.30, 8.5.48 to 8.5.50 and 7.0.98 to 7.0.99 introduced a regression. The result of the regression was that invalid Transfer-Encoding headers were incorrectly processed leading to a possibility of HTTP Request Smuggling if Tomcat was located behind a reverse proxy that incorrectly handled the invalid Transfer-Encoding header in a particular manner. Such a reverse proxy is considered unlikely. |

## 5. Mitigation Plan

* Update Spring Data Rest version to latest version 3.6.2 to make sure all the security fixes of Spring Security’s PreAuthorization model present in current application.
* Update for tomcat to version 9.0.31 fixes the issue
* Ambari 2.7.4/2.7.5 contains Spring 5.1.8 => should be upgraded to 5.1.18 at least
* Upgrade snakeyaml to a version without CVE-2017-18640
* Update jackson-databind to 2.11.0 and later
* Update logback-core to Red Hat Single Sign-On 7.4.2
* Update to hibernate-validator-6.0.20.
* Update log4j-api to 2.12.3

**References**

* Aws Albayati (2021). *Project One: Artemis Financial Vulnerability Assessment Report* [Unpublished manuscript]. Southern New Hampshire University.