****

# 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

Fisal Ikhmayes

## Interpreting Client Needs

**What is the value of secure communications to the company?**

Secure comiunications are very valuable to the company because they contain sensitive and confidential client data. Secure comunictaions will protect the company from being hacked and their sensitive data being stolen.

**Does the company make any international transactions?**

If they do interntnational transactions they need to obliage by compliance standards for cross border data transit so that they can be protetcted. There is specific security standards for international transactions.

**Are there governmental restrictions about secure communications to consider?**

There are specific requirements to meet standards especially in fields that have sensitive data such as finance and healthcare. This is crucial to avoid any compliance issues and penalties.

**What external threats might be present now and in the immediate future?**

It is cruicial to identify and address any secuirity vulrnabilities. Sql injection, DOS, are a few of the vulrnabilities malicious actors may try to exploit.

**What are the modernization requirements that you must consider? For example:**

**The role of open-source libraries**

**Evolving web application technologies**

It is essential to stay up to date on framworks and staying up to date on the libraries used is crucial to a secure application. Using outdated libraries can introduce vulrnabilities that hackers can exploit.

## Areas of Security

Input Validation: Input validation is necessary in this application to protect from sql injection attacks because in the code base it takes in the input and passes it to the query. There is no input validation.

API: secure Api are necessary because there is sensitive data and it cannot be accessable to outside sources.

Cryptography: this will ensure that the data is secured when accessed by outside sources.

Code error: Secure error messages and handeling is cruicial to this application.

Code quality: properly written code is cruicial to a secure application. Proper code can control who has access to what information.

## Manual Review

In the DocData.java there is no input validation or paramterization, this is a vulrnability for sql injection.

In the DocData.java there is no secureity for the connection to the database.

## Static Testing

bcprov-jdk15on-1.46.jar: JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.7. Update it to the latest version.

spring-boot-2.2.4.RELEASE.jar: v2.2.11.RELEASE was vulnerable to temporary directory hijacking. Update to latest version.

logback-core-1.2.3.jar : an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers. Upgrade to latest version.

log4j-api-2.12.1.jar . 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. Upgrade to Apache Log4j 2.12.3 and 2.13.1.

snakeyaml-1.25.jar The Alias feature in SnakeYAML before 1.26 allows entity expansion during a load operation, Upgrade to latest version.

jackson-databind-2.10.2.jar 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. Upgrade to latest version.

tomcat-embed-core-9.0.30.jar 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. Upgrade to the latest version

hibernate-validator-6.0.18.Final.jar A 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. Update to the latest version.

spring-web-5.2.3.RELEASE.jar suffers from a potential remote code execution (RCE) issue if used for Java deserialization of untrusted data. Upgrade to latest version.

## Mitigation Plan

We should paramterize the query and use input validation to protect from sql injection attacls.

We should use a secure connecrtion when connecting to the database. This way there is an encryption.

Update all libraries and frameworks frequenty to stay up to date.

Use secure codeing practices and error handeling and input validation.

Use HTTPS secure communication for API interaction.

Use penteration testing to find security flaws, this is important because this application has sensitive data and its important to have a secure application.