****

# Artemis Financial Vulnerability Assessment Report

Table of Contents

[Artemis Financial Vulnerability Assessment Report 1](#_Toc146181578)

[Document Revision History 3](#_Toc146181579)

[Developer 4](#_Toc146181580)

[1. Client Requirements 4](#_Toc146181581)

[2. Security Area Assessment 4](#_Toc146181582)

[3. Manual Code Review 5](#_Toc146181583)

[4. Static Testing 8](#_Toc146181584)

[5. Mitigation Plan 8](#_Toc146181585)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **13 Sep 2023** | **Nur Faizah** |  |



## Developer

Nur Faizah

## Client Requirements

Artemis Financial creates financial plans for their clients (mostly individuals), which range from savings to investments, insurance and retirement. To Artemis Financial, secure communications are essential to client trust and to protect sensitive information and financial data. The company is also involved in international transactions, which means that high security measures are needed to comply with international laws and standards. In addition, since the company operates globally, it has to adhere to governmental regulations on factors like secure communications and encryption.

## Security Area Assessment

Based on my initial assessment, the following are the areas of security that are relevant to Artemis Financial’s web application at hand:

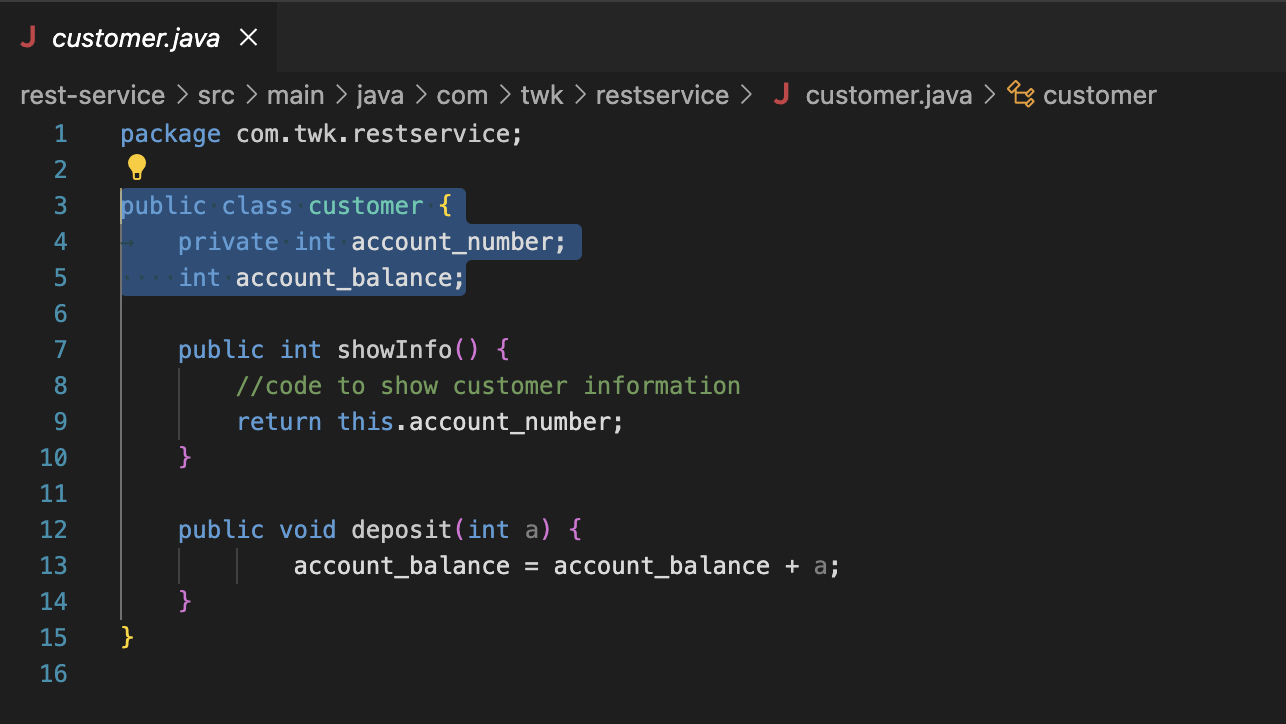
1. **Input Validation:**  Artemis Financial requires input validation to validate the owner of any information. This helps provide protection for users. This input validation will be written as strings.
2. **API Development –** The API sets parameters for acceptable data access, which provides an additional layer of security. An API is important for Artemis Financial as it operates both internally and externally.
3. **Cryptography –** Artemis Financial operates internationally. It’s understood that there will be multiple currencies at play, so cryptography is crucial to make sure of integrity and confidentiality of user data to protect from any global threats.
4. **Code Quality and Access Control -** High-quality code that follows best practices is important for any secure application. In the case of Artemis Financial, unauthorised access is a risky prospect, so proper access controls need to be in place to allow only the authorised to access what is theirs.

## 

## Manual Code Review

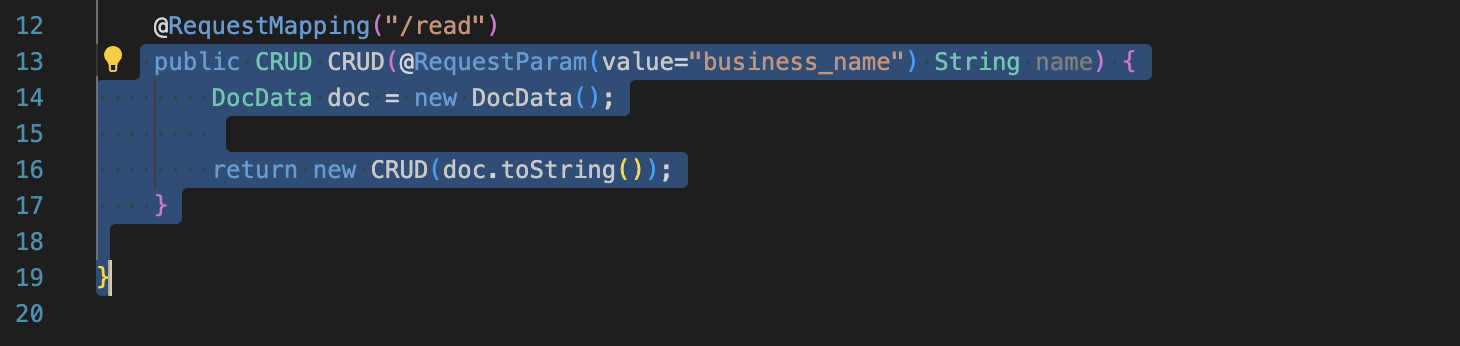
“**customer.java”**

* The field ‘account\_balance’ has package-level access. This potentially can expose sensitive data and unauthorised change in the bank account balance.
* It is recommended to set access to private and use getter/setter modes to access the account\_balance. Doing so encapsulates the field and protects it against data manipulation.



**“CRUDController.java”**

* The exposure of sensitive data through the ‘toString()’ method is the main issue.
* To safely expose data, serialisation methods need to be implemented. Explicitly specify which fields need to be or should not be exposed.

****

**“CRUD.java”**

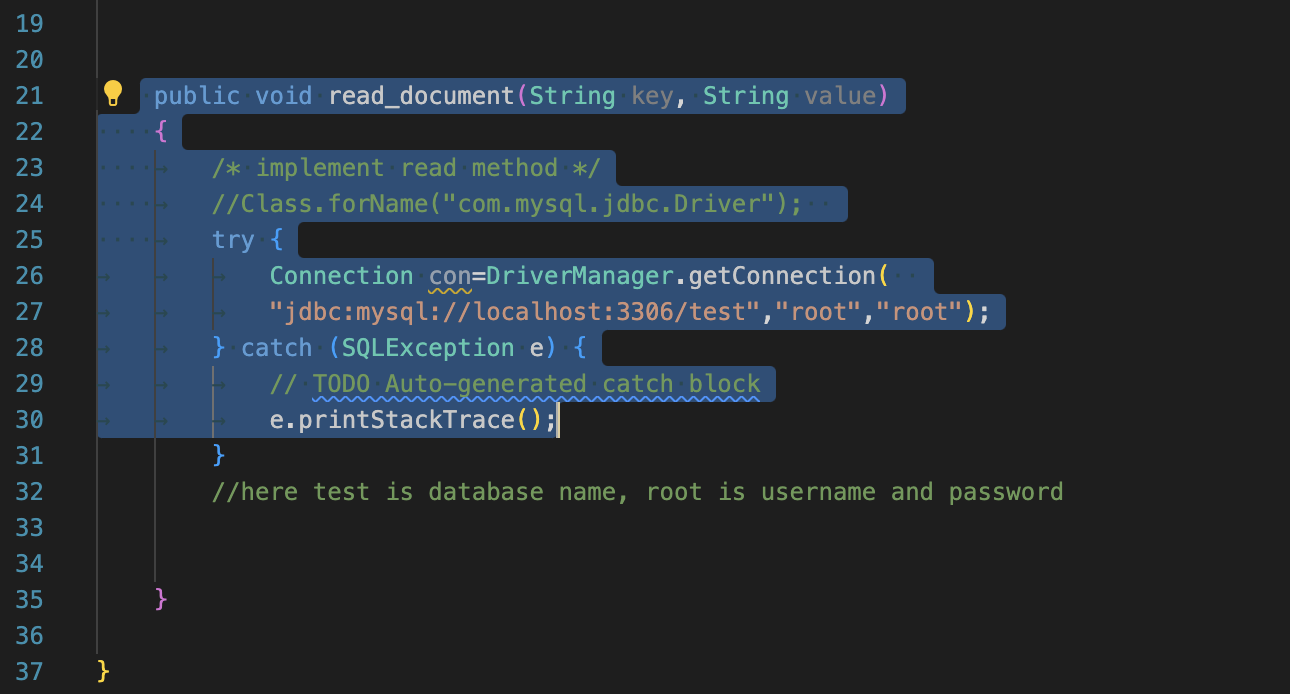
* The class naming “CRUD” is vague. It can lead to confusion. Usually, ‘CRUD’ stands for “Create, Read, Update and Delete” – the four basic operations in persistent database or storage. However, ‘CRUD.java’ holds some string content that does not do any CRUD activities. This can be misleading to developers who would expect that CRUD is what the CRUD.java file is meant to do. This means that the readability of the code is confused and would make it difficult to maintain the codebase.
* It is recommended to name the file to something which is more descriptive and which describes its functionality better.

**A screen shot of a computer program

Description automatically generated**

**“DocData.java”**

* This has the issue of hardcoded credentials, which poses a security risk. In the event that someone gains unauthorised access to the codebase, they could easily gain access to and compromise the database in question.
* It is recommended to use environment variables to store these sensitive credentials. They are more secure and allow for easier management of data that is meant to be a secret. For example, we can set ‘DATABASE\_URL’ and update the code to read from these variables, protecting against potential breaches.

****

## Static Testing

|  |  |  |  |
| --- | --- | --- | --- |
| Dependency | Vulnerability | Description | Recommendation |
| **snakeyaml-1.25.jar** | [cpe:2.3:a:snakeyaml\_project:snakeyaml:1.25:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Asnakeyaml_project&cpe_product=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml&cpe_version=cpe%3A%2F%3Asnakeyaml_project%3Asnakeyaml%3A1.25) | SnakeYaml's Constructor() class does not restrict types which can be instantiated during deserialization. Deserializing yaml content provided by an attacker can lead to remote code execution.  YAML 1.1 parser and emitter for Java | Upgrade to 2.0 and beyond. |
| **spring-boot-2.2.4.RELEASE.jar** | [**cpe:2.3:a:vmware:spring:2.2.4:release:\*:\*:\*:\*:\*:\***](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring&cpe_version=cpe%3A%2F%3Avmware%3Aspring%3A2.2.4)[**cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\***](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_boot&cpe_version=cpe%3A%2F%3Avmware%3Aspring_boot%3A2.2.4) | Spring Boot | Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+. |
| [**spring-boot-starter-web-2.2.4.RELEASE.jar**](#l16_ec75d01d212b5229c16d872fb127744c0ed) | [**cpe:2.3:a:vmware:spring:2.2.4:release:\*:\*:\*:\*:\*:\***](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring&cpe_version=cpe%3A%2F%3Avmware%3Aspring%3A2.2.4)[**cpe:2.3:a:vmware:spring\_boot:2.2.4:release:\*:\*:\*:\*:\*:\***](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_boot&cpe_version=cpe%3A%2F%3Avmware%3Aspring_boot%3A2.2.4)[**cpe:2.3:a:web\_project:web:2.2.4:release:\*:\*:\*:\*:\*:\***](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aweb_project&cpe_product=cpe%3A%2F%3Aweb_project%3Aweb&cpe_version=cpe%3A%2F%3Aweb_project%3Aweb%3A2.2.4) | Starter for building web, including RESTful, applications using Spring  MVC. Uses Tomcat as the default embedded container | In Spring Boot versions 3.0.0 - 3.0.5, 2.7.0 - 2.7.10, and older unsupported versions, an application that is deployed to Cloud Foundry could be susceptible to a security bypass. Users of affected versions should apply the following mitigation: 3.0.x users should upgrade to 3.0.6+. 2.7.x users should upgrade to 2.7.11+. Users of older, unsupported versions should upgrade to 3.0.6+ or 2.7.11+. |
| [spring-core-5.2.3.RELEASE.jar](#l17_3734223040040e8c3fecd5faa3ae8a1ed6d) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) [cpe:2.3:a:vmware:spring:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring&cpe_version=cpe%3A%2F%3Avmware%3Aspring%3A5.2.3) [cpe:2.3:a:vmware:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3) | Spring Core | Update to latest version. |
| [spring-web-5.2.3.RELEASE.jar](#l18_dd386a02e40b915ab400a3bf9f586d2dc4c) | [cpe:2.3:a:pivotal\_software:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Apivotal_software&cpe_product=cpe%3A%2F%3Apivotal_software%3Aspring_framework&cpe_version=cpe%3A%2F%3Apivotal_software%3Aspring_framework%3A5.2.3) [cpe:2.3:a:springsource:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aspringsource&cpe_product=cpe%3A%2F%3Aspringsource%3Aspring_framework&cpe_version=cpe%3A%2F%3Aspringsource%3Aspring_framework%3A5.2.3) [cpe:2.3:a:vmware:spring:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring&cpe_version=cpe%3A%2F%3Avmware%3Aspring%3A5.2.3) [cpe:2.3:a:vmware:spring\_framework:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Avmware&cpe_product=cpe%3A%2F%3Avmware%3Aspring_framework&cpe_version=cpe%3A%2F%3Avmware%3Aspring_framework%3A5.2.3) [cpe:2.3:a:web\_project:web:5.2.3:release:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aweb_project&cpe_product=cpe%3A%2F%3Aweb_project%3Aweb&cpe_version=cpe%3A%2F%3Aweb_project%3Aweb%3A5.2.3) | Spring Web | Update to the latest version. |
| [tomcat-embed-core-9.0.30.jar](#l20_ad32909314fe2ba02cec036434c0addd19b) | [cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Atomcat&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A9.0.30) [cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_tomcat&cpe_product=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat&cpe_version=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat%3A9.0.30) | Core Tomcat implementation | Update to the latest version. |
| [tomcat-embed-websocket-9.0.30.jar](#l22_33157f6bc5bfd03380ebb5ac476db0600a0) | [cpe:2.3:a:apache:tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache&cpe_product=cpe%3A%2F%3Aapache%3Atomcat&cpe_version=cpe%3A%2F%3Aapache%3Atomcat%3A9.0.30) [cpe:2.3:a:apache\_tomcat:apache\_tomcat:9.0.30:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aapache_tomcat&cpe_product=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat&cpe_version=cpe%3A%2F%3Aapache_tomcat%3Aapache_tomcat%3A9.0.30) | Core Tomcat implementation | Update to the latest version. |

## Mitigation Plan

The most basic form of mitigation in this case is to ensure that the latest versions of each of the technologies used for the web application. This is to patch any security problems and to protect against security threats that may surface and pose a risk to the web application.