****

# 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** | **1/26/24** | **Bryce Cooperrider** |  |

## 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

Bryce Cooperrider

## Interpreting Client Needs

Artemis Financial would like us at Global Rain to develop software to help them modernize their operations. They offer individualized financial plans for their customers. These plans include savings, retirement, investments, and insurance. Artemis Financial has a RESTful API. They are seeking our help with how to protect the organization from external threats.

Artemis Financial places a strong value on secure communications. They specifically ask to use the most current and effective software security, as it is a crucial part of its success.

The company doesn’t seem to be making any international transactions, meaning there are a couple less rules and regulations to follow. However, this doesn’t mean the software won’t be safe and secure. If they do end up making international transactions, it would be required to follow foreign laws about communication, data retention, and any other applicable pieces to follow.

Because Artemis is a financial group, they are required by law to protect their data. In 2021, the FTC strengthened security safeguards and consumer financial information standards. From the FTC, “The changes adopted by the Commission to the [Safeguards Rule](https://www.ftc.gov/policy/federal-register-notices/16-cfr-part-314-standards-safeguarding-customer-information-final) include more specific criteria for what safeguards financial institutions must implement as part of their information security program such as limiting who can access consumer data and using encryption to secure the data. Under the updated Safeguards Rule, institutions must also explain their information sharing practices, specifically the administrative, technical, and physical safeguards the financial institutions use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customers’ secure information. In addition, financial institutions will be required to designate a single qualified individual to oversee their information security program and report periodically to an organization’s board of directors, or a senior officer in charge of information security.”

Because Artemis will be online, there will always be the threat of attacks and cybercrimes. Some of these threats could be something that is more of an annoyance, such as a DDOS attack, but other threats could be much more harmful, such as an entity trying to breach their database to access user records and financial information. Both should be treated with care.

One modernization requirement to consider is the use of open-source libraries. While they are incredibly useful and do amazing things for programmers, Artemis must be aware that not all open-source libraries are secure. Even if they develop everything up to standard and make it secure, just drawing upon a compromised library could open up the whole program and make it vulnerable to attacks. The best way to mitigate this is to research the libraries you are going to use.

Another requirement to consider is evolving web technologies. Having strict passwords that have multiple requirements can often help with security, but at the same time can limit the results that external programs have to generate a password. It is important to have secure and encrypted connections between Artemis’s database and the user.

## Areas of Security

Artemis uses a RESTful API. With that in mind, I would focus on input validation, secure API interactions, cryptography, code errors, and encapsulation.

Input validation is important because you need to sanitize user inputs, even from trusted users. A bad input could cause odd and malicious behavior, even if it’s not on purpose.

Securing the API is necessary to make sure the connection between the user and the server is trustworthy. This will help anyone trying to exploit connectivity issues.

Because Artemis has access to financial information and personal identity information, cryptography is very important. All data flows need to be encrypted to ensure data is safe in transit.

Code Errors is a focus because any error handling needs to be generic. If it’s not, a hacker can use that information to understand more about the code structure.

Encapsulation is on the focus list because the data needs to be secure when it is not in motion. To protect the data, variables need to be set to private, and need to use get and set functions.

## Manual Review

When implementing the static testing in the pom.xml file, Maven is using version 4.0.0. It needs to be updated to the latest version to ensure better static testing results.

Looking at the classes, Greeting.java does well setting its variables to private. However, GreetingController.java doesn’t use the available get and set functions.

All of the methods that accept user input need to be checked for length to prevent buffer overflows.

Customer.java has account\_number set to private, which is needed, but doesn’t set account\_balance to private. Account balance should be private for security reasons. It should also be using get and set methods.

In myDateTime.java, the setMyDateTime method is incomplete.

There isn’t a lot of error checking built in the code. The only one I see is in DocData.java catching the SQLexception. When working with error handling it is important to remember not to output any identifying information about the code base as a hacker could use this information to understand the codebase better.

## Static Testing

|  |  |  |  |
| --- | --- | --- | --- |
| Dependency | Vulnerability IDs | Description | Mitigation |
| [bcprov-jdk15on-1.46.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l1_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7) | 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:bouncy\_castle\_for\_java:1.46:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Abouncycastle&cpe_product=cpe%3A%2F%3Abouncycastle%3Abouncy_castle_for_java&cpe_version=cpe%3A%2F%3Abouncycastle%3Abouncy_castle_for_java%3A1.46) [cpe:2.3:a:bouncycastle:legion-of-the-bouncy-castle-java-crytography-api:1.46:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Abouncycastle&cpe_product=cpe%3A%2F%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api&cpe_version=cpe%3A%2F%3Abouncycastle%3Alegion-of-the-bouncy-castle-java-crytography-api%3A1.46) cpe:2.3:a:bouncycastle:the\_bouncy\_castle\_crypto\_package\_for\_java:1.46:\*:\*:\*:\*:\*:\*:\* | The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms. This jar contains JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.7. | Update Bouncy Castle to the latest version |
| [hibernate-validator-6.0.18.Final.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l3_7fd00bcd87e14b6ba66279282ef15efa30dd2492) | [cpe:2.3:a:redhat:hibernate\_validator:6.0.18:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aredhat&cpe_product=cpe%3A%2F%3Aredhat%3Ahibernate_validator&cpe_version=cpe%3A%2F%3Aredhat%3Ahibernate_validator%3A6.0.18) | Hibernate's Bean Validation (JSR-380) reference implementation. | Upgrade Hibernate to latest release |
| [jackson-databind-2.10.2.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l5_0528de95f198afafbcfb0c09d2e43b6e0ea663ec) | |  |  | | --- | --- | |  | [cpe:2.3:a:fasterxml:jackson-databind:2.10.2:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Afasterxml&cpe_product=cpe%3A%2F%3Afasterxml%3Ajackson-databind&cpe_version=cpe%3A%2F%3Afasterxml%3Ajackson-databind%3A2.10.2) cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:\*:\*:\*:\*:\*:\*:\* | | General data-binding functionality for Jackson: works on core streaming API | Upgrade version past 2.15.2 |
| [log4j-api-2.12.1.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l10_a55e6d987f50a515c9260b0451b4fa217dc539cb) | |  |  | | --- | --- | |  | [cpe:2.3:a:apache:log4j:2.12.1:\*:\*:\*:\*:\*:\*:\*](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%3Alog4j&cpe_version=cpe%3A%2F%3Aapache%3Alog4j%3A2.12.1) | | The Apache Log4j API | Update log4j to at least 2.13.1 |
| [logback-core-1.2.3.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l12_864344400c3d4d92dfeb0a305dc87d953677c03c) | [cpe:2.3:a:qos:logback:1.2.3:\*:\*:\*:\*:\*:\*:\*](https://nvd.nist.gov/vuln/search/results?form_type=Advanced&results_type=overview&search_type=all&cpe_vendor=cpe%3A%2F%3Aqos&cpe_product=cpe%3A%2F%3Aqos%3Alogback&cpe_version=cpe%3A%2F%3Aqos%3Alogback%3A1.2.3) | logback-core module | Update logback core to at least 1.2.8 |
| [snakeyaml-1.25.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l14_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421) | |  |  | | --- | --- | |  | [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) | | YAML 1.1 parser and emitter for Java | Update jar to latest version |
| [spring-boot-2.2.4.RELEASE.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l15_225a4fd31156c254e3bb92adb42ee8c6de812714) | [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 | Update spring boot to at least 2.7.11+ or 3.0.6+ |
| [spring-boot-starter-web-2.2.4.RELEASE.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l16_ec75d01d212b5229c16d872fb127744c0ed46ed8) | [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. | Update spring boot to latest version |
| [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l17_3734223040040e8c3fecd5faa3ae8a1ed6da146b) | |  |  | | --- | --- | |  | [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\_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 a more recent supports version |
| [spring-web-5.2.3.RELEASE.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l18_dd386a02e40b915ab400a3bf9f586d2dc4c0852c) | |  |  | | --- | --- | |  | [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\_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 | Apply updates per vender instruction |
| [spring-webmvc-5.2.3.RELEASE.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l19_745a62502023d2496b565b7fe102bb1ee229d6b7) | [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\_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 MVC | Update jar to latest version |
| [tomcat-embed-core-9.0.30.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l20_ad32909314fe2ba02cec036434c0addd19bcc580) | |  |  | | --- | --- | |  | [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 tomcat to latest version |
| [tomcat-embed-websocket-9.0.30.jar](file:///C:\Users\Bryce\Documents\SNHU\CS-305\Module%203\CS%20305%20Project%20One%20Code%20Base\rest-service\target\dependency-check-report.html#l22_33157f6bc5bfd03380ebb5ac476db0600a04168d) | |  |  | | --- | --- | |  | [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 tomcat to latest version |

## Mitigation Plan

The first and most important step in the mitigation plan is to update all of the dependent libraries. With the library updates, it may lead to how code is written so it is at the top of the list.

The second step is to update the code. Adding proper encapsulation is a good start. From there, work on adding input validation, sanitize error messages, and add security improvements to the API, and login information.

The last step is to have a group peer programming session, or a group code review. Having multiple programmers look over the code will help discover any large security issues within the code.