

# Artemis Financial Vulnerability Assessment Report

Table of Contents

[Artemis Financial Vulnerability Assessment Report 1](#_Toc1878073921)

[Document Revision History 2](#_Toc1010205938)

[Client 3](#_Toc910919335)

[Instructions 3](#_Toc1267982157)

[Developer 3](#_Toc637539318)

[1. Interpreting Client Needs 4](#_Toc321184058)

[2. Areas of Security 4](#_Toc877209649)

[3. Manual Review 4](#_Toc1745206850)

[4. Static Testing 4](#_Toc2032054402)

[5. Mitigation Plan 7](#_Toc683852277)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **3/10/23** | **Brandon Randall** |  |

## 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

Brandon Randall

## Interpreting Client Needs

Artemis Finance wants to modernize their operations using the most current and effective software security. Artemis Financial currently has a RESTful web application programming interface and is seeking help with protection from external threats. Artemis Finance specializes in individualized financial plans, such as savings, retirement, investment, and insurance plans. companies in this business tend to handle users' sensitive information, such as social security numbers and account numbers, as well as facilitating user to account transactions. This business faces external threats like phishing and spoofing attempts on users and more direct threats such as ransom and malware.

## Areas of Security

* Input Verification
  + User input is an important part of this program. Users will access personal accounts with confidential information, so verifying that a user's inputs are important for validating whether a user can access key information.
* API’s
  + This program utilizes an API to connect users with the Artemis Finance’s databases, which can contain sensitive information. Users should not have full access to every bit of information available and steps should be taken to secure this information using
* Cryptography
  + Encryption is a major step for keeping transactions private. In this program users will be transferring funds between their own accounts and other user accounts. These transactions may also be international transactions which fall under different regulations from domestic transactions. Utilizing encryptions that can cover all bases will be important.
* Code Error
  + Error handling is an important part of making sure any program is secure. Code errors can be used by threat actors to access information that they are not authorized to access by causing the program to perform in unexpected ways.
* Code Quality
  + Quality code is important in all aspects of a program. it encompasses all the above aspects and ensures they are done properly.

## Manual Review

Looking into the classes containing rest controllers, CRUDController and GreetingController, there are no authentication systems in place, all users have full access. These classes also use GET methods with the parameters in the URL. This can leak the user's sensitive data. In the DataDoc class the username and password for the test database are hardcoded into the class. The program uses HTTP rather than HTTPS which could pose security risks. There is also a lack of error handling within the program, the only error handling is within the DataDoc class with a try/catch statement.

## Static Testing

bcprov-jdk15on-1.46.jar

* [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)
* The key issues surrounding this dependency include Cryptographic issues and information exposure.
  + The issues associated with this dependency can be resolved by updating to a later version.1

hibernate-validator-6.0.18.Final.jar

* [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)
* A bug in this version allows for invalid expressions to be evaluated as valid.
  + Redhat bugzilla states that you can pass user input as an expression variable by unwrapping the context to HibernateConstraintValidatorContext to avoid this issue. You could also update to a current version.2

jackson-databind-2.10.2.jar

* [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)
* This version does not have proper entity expansion security leading to vulnerability to XXE attacks that can affect data integrity. Another issue allows for StackOverflow exceptions and DDS attacks. There are also issues with resource exhaustion.
  + The issues associated with this dependency can be resolved by updating to a later version.3

log4j-api-2.12.1.jar

* [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)
* This version contains improper certificate validation that could allow SMTPS connections to be intercepted, leaking appender log messages.
  + The issues associated with this dependency can be resolved by updating to a later version.4

logback-core-1.2.3.jar

* [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)
* Users with access to edit configuration files could modify files to execute arbitrary code. The issues with this dependency are less to do with the dependency itself and more with authorization control.
  + The issues associated with this dependency can be resolved by updating to a later version.5

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)
* Use of untrusted YAML files could lead to DOS attacks and issues that can lead to data deserialization.
  + The issues associated with this dependency can be resolved by updating to a later version.6

spring-boot-2.2.4.RELEASE.jar

spring-boot-starter-web-2.2.4.RELEASE.jar

* [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) (spring-boot-starter-web-2.2.4.RELEASE.jar only)
* These dependencies are vulnerable to directory hijacking through a specific method.
  + The issues associated with these dependencies can be resolved by updating to a later version.7

spring-core-5.2.3.RELEASE.jar

spring-web-5.2.3.RELEASE.jar

spring-webmvc-5.2.3.RELEASE.jar

* [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-5.2.3.RELEASE.jar & spring-webmvc-5.2.3.RELEASE.jar only)
* These dependencies have multiple issues that can lead to DOS atacks as well as code injection under the right context.
  + The issues associated with these dependencies can be resolved by updating to a later version.8
  + spring-web-5.2.3.RELEASE.jar only: [CVE-2016-1000027](http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1000027) cannot be resolved, as stated in the CVE details, “the vendor's position is that untrusted data is not an intended use case. The product's behavior will not be changed because some users rely on deserialization of trusted data.”

tomcat-embed-core-9.0.30.jar

tomcat-embed-websocket-9.0.30.jar

* [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)
* These dependencies have issues involving DOS attacks as well as information exposure. There is also a major issue that treats AJP connections as higher trust then other connections allowing attacks to use these connections as exploits.
  + The issues associated with these dependencies can be resolved by updating to a later version.9

## Mitigation Plan

For most dependency issues an update would resolve the current security risks. Authentication should be added to the controller classes to secure and validate inputs. POST methods should be used instead of only GET methods to avoid having parameter information in the URL by putting it in the body of the POST method. Using an HTTPS connection could also mitigate this issue. The bouncycastle dependency should be utilized to secure username and password information through encryption.

Citations

1. Retrieved March 16, 2023, from <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>
2. 1805501 – (CVE-2020-10693) CVE-2020-10693 hibernate-validator: Improper input validation in the interpolation of constraint error messages. (n.d.). Retrieved March 16, 2023, from <https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-10693>
3. Retrieved March 16, 2023, from <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>
4. Retrieved March 16, 2023, from <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>
5. Retrieved March 16, 2023, from <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>
6. Retrieved March 16, 2023, from <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>
7. Retrieved March 16, 2023, from <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>
8. Retrieved March 16, 2023, from <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>
9. Retrieved March 16, 2023, from <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>