****

# 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** | **01/23/2022** | **Rosario Robinson** | **This report identifies my findings of vulnerabilities within the Artemis Financial system and recommendations to solve said issues. I have included APA citations for reference.** |

## Client



## Instructions

Deliver this completed vulnerability assessment report, identifying your findings of security vulnerabilities and articulating recommendations for 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

Rosario Robinson

## 1. Interpreting Client Needs

Artemis Financial is a financial consulting company that focuses on developing individualized financial plans for savings, retirement, investments, and insurance for their current customer base. Keeping this in mind, financial companies, in particular, must focus on ensuring their security is kept up to date and as secure as possible to protect their customer’s private information. At this time, it is not indicated that there are international transactions occurring at the company. Clients of theirs may live abroad in the future or may travel for business so it may be important to consider in future updates. This may be integrated in the future, so it is important to keep this in mind while updating Artemis Financial’s software security. The same goes for governmental restrictions, as they seem more focused on individualized plans for their customers. However, Artemis Financial may consider working with government institutions, so having the proper encryption and up-to-date security would be highly important.

In the future, many external threats may occur via the lack of updates that have happened within their current system. This may include the need to update encryptions for website authentication logins and passwords to ensure a customer’s information is secure and ensuring there are limits to input validations for customers. Since Artemis Financial will heavily rely on and focus on solving issues regarding money, it is important that their system is up to date and as secure as possible to prevent cyber-attacks that would compromise their reputation and their customer’s private information.

Since web application technologies are constantly evolving, I believe that utilizing security dependency checks the most would help prevent major vulnerabilities within Artemis Financial’s system. Incorporating open-source libraries may depend on the type of library, especially since we are dealing with a company that deals with finances. As for additional web application technologies, deciding on which frameworks and languages to use will also depend on what is best for the company. In my opinion, using languages like HTML, CSS, JavaScript and even Python would be the best idea. Python is used often when dealing with numbers and statistics, so it may be beneficial in this case. Django or Express.js for the frameworks should be considered, as they are consistently updated and help developers through the process (Timotic, 2021).

## 2. Areas of Security

For Artemis Financial, there are five out of the seven areas within the Vulnerability Assessment Process Flow Diagram I have identified for the software application: Input Validation, APIs, Cryptography, Code Error, and Code Quality. Each of these areas assists in resolving issues that Artemis Financial is currently trying to solve, while also ensuring the capture of future issues when they arise.

**Input Validation:** Since input validation is considered one of the “first lines of defense” in a web application (Manico & Detlefsen, Chapter One, 2014), it is important to ensure Artemis Financial’s inputs are correctly validated when customers have access to the site. For example, whitelisting is something Artemis Financial may have to consider when asking clients for information. Only allowing correctly formatted numbers, which may include the country code and parenthesis, will prevent hackers or any incorrect information to be inputted in that specific section (Manico & Detlefsen, Input Validation Positive Patterns: Whitelisting, 2014).

**APIs:** This area, in particular, is highly important to what Artemis Financial needs for its software application. They are currently using a RESTful API, which requires headers and parameters to ensure protection and request authorization (RedHat, 2020). Since a REST API is more flexible, this allows developers to go in and update their current API while protecting Artemis Financial’s secure information.

**Cryptography:** Cryptography is an area that ties into other areas for Artemis Financial’s software application. Including more secure cryptography sources such as Google Keyczar, which is an open-source cryptographic toolkit that helps developers add cryptography to web applications, will absolutely benefit Artemis Financial, especially in further protecting their software security (Manico & Detlefsen, 2014)

**Code Error:** This area is specifically designed for developers to create secure error handling to ensure that for other areas like the input validation, the system will catch incorrect inputs or formatting. This protects not only Artemis Financial on the back end, but also protects their clients and their private financial information.

**Code Quality:** Ensuring that the code provided for Artemis Financial displays secure coding practices and patterns is another important area to consider while updating the software application. This essentially means including practices such as data validation, authentication and password management, access management, and other system updates required (The OWASP Foundation, 2010). Many of the practices listed provided by The OWASP Foundation essentially cover any and all practices to ensure the code quality will be at the best of its ability for Artemis Financial.

## 3. Manual Review

While inspecting the code alongside the Vulnerability Assessment Process Flow Diagram, I have identified a few vulnerabilities present. For input validation, I noticed that within the customer.java file, there needs to be more code showing specifics of what is required of the customer aside from the account number and account balance. They may wish to input new information, such as a change of address, new phone number, or any changes they may wish to edit. As for the APIs, although Artemis Financial has a RESTful API, it is not fully implemented in the code. They have CRUD files created, but the DocData.java file could include additional information. Alongside the dependency check I ran, I noticed there were issues with the spring framework and updates that will be required. In addition to this, cryptography has issues that are shown in that the Bouncy Castle Crypto package, which focuses on cryptographic algorithms for security purposes, must be updated to resolve any vulnerabilities in the previous package.

The other areas of the Vulnerability Assessment Process Flow — client/server, code error, code quality, and encapsulation, also have slight vulnerabilities that are displayed not only within the code but more specifically within the dependency check done. Some of these issues evident within the code include implementations that are needed with the myDateTime.java file that focuses on the accessor methods, an incomplete try-catch statement to catch errors that could occur in the code, and updates of the pom.xml file that had to be edited in order to properly complete a dependency check. Overall, the code provided must be further updated to not only correct current vulnerabilities, but to ensure no other vulnerabilities appear with future updates of the software and web application.

## 4. Static Testing

I have provided the recording given from the dependency check reported. There were 10 dependencies given in total, which include brief descriptions and subsequently recommended solutions. I will also be including a screenshot of the summary provided via Dependency-Check Maven.

1. **Name**: bcprov-jdk15on-1.46.jar

**Identifiers**:

* + [pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46](https://ossindex.sonatype.org/component/pkg:maven/org.bouncycastle/bcprov-jdk15on@1.46?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + cpe:2.3:a:bouncycastle:bouncy-castle-crypto-package:1.46:::::::\* (Confidence:Low)
  + cpe:2.3:a:bouncycastle:bouncy\_castle\_crypto\_package:1.46:::::::\* (Confidence:Low)
  + [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) (Confidence:Highest)
  + cpe:2.3:a:bouncycastle:the\_bouncy\_castle\_crypto\_package\_for\_java:1.46:::::::\* (Confidence:Low)

**Description**: 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.

1. **Name**: hibernate-validator-6.0.18.Final.jar

**Identifiers**:

* + [pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final](https://ossindex.sonatype.org/component/pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)

**Description**: Hibernate's Bean Validation (JSR-380) reference implementation.

1. **Name**: jackson-databind-2.10.2.jar

**Identifiers**:

* + [pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2](https://ossindex.sonatype.org/component/pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)
  + cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:::::::\* (Confidence:Low)

**Description**: General data-binding functionality for Jackson: works on core streaming API

1. **Name**: log4j-api-2.12.1.jar

**Identifiers**:

* + [pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1](https://ossindex.sonatype.org/component/pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)

**Description**: The Apache Log4j API

1. **Name**: logback-core-1.2.3.jar

**Identifiers**:

* + [pkg:maven/ch.qos.logback/logback-core@1.2.3](https://ossindex.sonatype.org/component/pkg:maven/ch.qos.logback/logback-core@1.2.3?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)

**Description**: logback-core module

1. **Name**: snakeyaml-1.25.jar

**Identifiers**:

* + [pkg:maven/org.yaml/snakeyaml@1.25](https://ossindex.sonatype.org/component/pkg:maven/org.yaml/snakeyaml@1.25?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)

**Description**: YAML 1.1 parser and emitter for Java

1. **Name**: spring-aop-5.2.3.RELEASE.jar

**Identifiers**:

* + [pkg:maven/org.springframework/spring-aop@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-aop@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)
  + [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) (Confidence:Highest)
  + [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) (Confidence:Highest)

**Description**: Spring AOP

1. **Name**: spring-core-5.2.3.RELEASE.jar

**Identifiers**:

* + [pkg:maven/org.springframework/spring-core@5.2.3.RELEASE](https://ossindex.sonatype.org/component/pkg:maven/org.springframework/spring-core@5.2.3.RELEASE?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)
  + [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) (Confidence:Highest)
  + [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) (Confidence:Highest)
  + cpe:2.3:a:vmware:springsource\_spring\_framework:5.2.3:release:::::: (Confidence:Low)

**Description**: Spring Core

1. **Name**: tomcat-embed-core-9.0.30.jar

**Identifiers**:

* + [pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)
  + [cpe:2.3:a:apache\_software\_foundation: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_software_foundation&cpe_product=cpe%3A%2F%3Aapache_software_foundation%3Atomcat&cpe_version=cpe%3A%2F%3Aapache_software_foundation%3Atomcat%3A9.0.30) (Confidence:Highest)
  + [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) (Confidence:Highest)

**Description**: Core Tomcat implementation

1. **Name**: tomcat-embed-websocket-9.0.30.jar

**Identifiers**:

* + [pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30](https://ossindex.sonatype.org/component/pkg:maven/org.apache.tomcat.embed/tomcat-embed-websocket@9.0.30?utm_source=dependency-check&utm_medium=integration&utm_content=6.5.3) (Confidence:High)
  + [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) (Confidence:Highest)

suppress

* + [cpe:2.3:a:apache\_software\_foundation: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_software_foundation&cpe_product=cpe%3A%2F%3Aapache_software_foundation%3Atomcat&cpe_version=cpe%3A%2F%3Aapache_software_foundation%3Atomcat%3A9.0.30) (Confidence:Highest)

suppress

* + [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) (Confidence:Highest)

suppress

**Description**: Core Tomcat implementation

**Screenshot from Dependency-Check Maven**

Graphical user interface, application

Description automatically generated

## 5. Mitigation Plan

Based on the results from both my manual review and static testing report, there are a few steps to remedying the security vulnerabilities stated. Most of the actions that must be taken focus on updating packages and files to ensure the protection of data and encrypted information.

1. Updating the Bouncy Castle Crypto package to ensure the protection of client information and prevent malicious attacks on private information.
2. Update Hibernate Bean Validation, as there is a flaw that allows attackers to bypass input sanitation controls.
3. Updating flaw found in FasterXML Jackson Databind due to security vulnerabilities found that leave data vulnerable to attacks.
4. Updates required for Apache API, log back core, and SnakeYAML to prevent intercepted attacks that may occur.
5. Spring Framework updates to prevent RFD attacks via browser.
6. Apache Tomcat updates due to issues with HTTP Requests.

**References**

Timotic, M. (2021, March 28). 9 Web Technologies Every Web Developer Must Know in 2021. TMS. <https://tms-outsource.com/blog/posts/web-technologies/>

Manico, J., & Detlefsen, A. (2014, September). Iron-Clad Java. O’Reilly Online Learning. <https://www.oreilly.com/library/view/iron-clad-java/9780071835886/?sso_link=yes&sso_link_from=SNHU>

What is a REST API? (2020, May 8). RedHat. <https://www.redhat.com/en/topics/api/what-is-a-rest-api>

The OWASP Foundation. (2010, August). OWASP Secure Coding Practices Quick Reference Guide. <https://owasp.org/www-pdf-archive/OWASP_SCP_Quick_Reference_Guide_v1.pdf>