****

**CS 305 Software Security**

# 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 5](#_Toc32574612)

[3. Manual Review 5](#_Toc32574613)

[4. Static Testing 7](#_Toc32574614)

[5. Mitigation Plan 10](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **January 16, 2023** | **Sergio Mateos** | **Artemis Financial examination to identify any vulnerability** |

## Client



## Instructions

Conduct a vulnerability assessment to examine Artemis Financial’s web-based software application. The venerability Assessment will include the following material: interpreting client needs, areas of security, manual review, static review, and mitigation plan. Every section will contain the result of our vulnerability assessment to prevent any security issues.

## Developer

Sergio Mateos, developer from Global Rain.

## Interpreting Client Needs

Artemis Financial is a consulting company that develops individualized plans for its customers. Artemis Financial orientate customer to have healthier finance by creating financial plans that include savings, retirement, investments, and insurance. Since Artemis has been successful in its operations, Artemis Financial would like to modernize their operations, and they want to ensure they are protected from vulnerabilities, that’s why they are seeking Global Rain expertise on how to protect the organization from external threats. To prevent vulnerabilities, Global Rain developers review the scenario to determine the potential threats and needs of their customers.

* What is the value of secure communication to the company?
  + Artemis Financial deals with a high amount of personal information, that include full name, bank accounts, address, etc. Artemis Financial must ensure that the communication between them and their customer must be secure to prevent any leak of information and ensure that their customer feels comfortable sharing their personal information. Assuming that the communication would be constant between Artemis Financials and customers, ensuring all the channels are secure would be prioritized.
* Does the company make any international transactions?
  + During the research about Artemis Financials, Global Rain developers did not find enough information that indicates that Artemis Financial makes international transactions. But this does not indicate that this type of service will not be included in the future of Artemis Financial, so Global Rain developers need to ensure that the application is secure enough to develop this new service in case that would be available in the future.
* Are there governmental restrictions on secure communication to consider?
  + The due diligence from Global Rain, there are some criteria that must be made for companies who handle dedicated information like Artemis Financial. The rule will be different in different countries in case Artemis Financial stated to provide international services.
* What external threats might be present now and in the immediate future?
  + Artemis Financial handles important information and it could be crucial if customer information gets leaked. Today, there are many sophisticated hackers group that are able to access many systems, but the most effective type of method that is seen as more effective for hackers is social engineering. From fake calls to phishing, hackers use many ways to persuade users to give away their information. For example, if a hacker pretends to be an Artemis Financial employee and convinces the customers to prove their information to access their account, hackers are available to access their personal information and hurt the victims. Educating their customers and providing easy access to information can prevent this type of attack on their customers.
* What are the modernization requirements that you must consider?
  + Technology is modernizing at a fast speed, and malicious users are finding different ways to have access to many systems. The best way to prevent malicious users to have access to our system is update our systems and team, so it could be prepared for any type of hack and know how to deal with it.

## Areas of Security

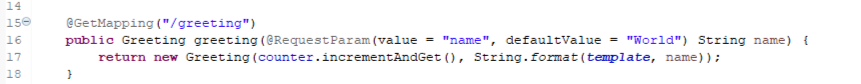
Global Rain developers following the Vulnerability Assessment Process Flow Diagram have determined the area of security vulnerabilities that the Artemis Financial web application will be vulnerable to if it is not handled appropriately.

* Validation of Inputs: Validation of inputs is important since customers are dealing with personal information, and it must manage correctly. The inputs would be stored in the data system which is not validated which can cause them problems with their goals. Also, malicious users can find these types of problems and have access to functions in the code that were not supposed to be approachable as easily.
* APIs: APIs are crucial in the Artemis Financial web application since the application would be outside the environment. APIs would secure communication between the customers and will accept data if is valid. Malicious users will find a way to access our system, that why is crucial to secure the API interaction.
* Cryptography: If a malicious user gets access to our system, Artemis Financial needs to make sure the malicious user is not available to access customer data. Encrypting customer information is important for the security of their customers. Since Artemis Financial is dealing with delicate information is important to keep it secure at all times.
* Code Quality: Code Quality is very important to prevent any leak of information. If the code has a high standard and is well-developed, it can prevent easy access to the system by malicious users.

## Manual Review

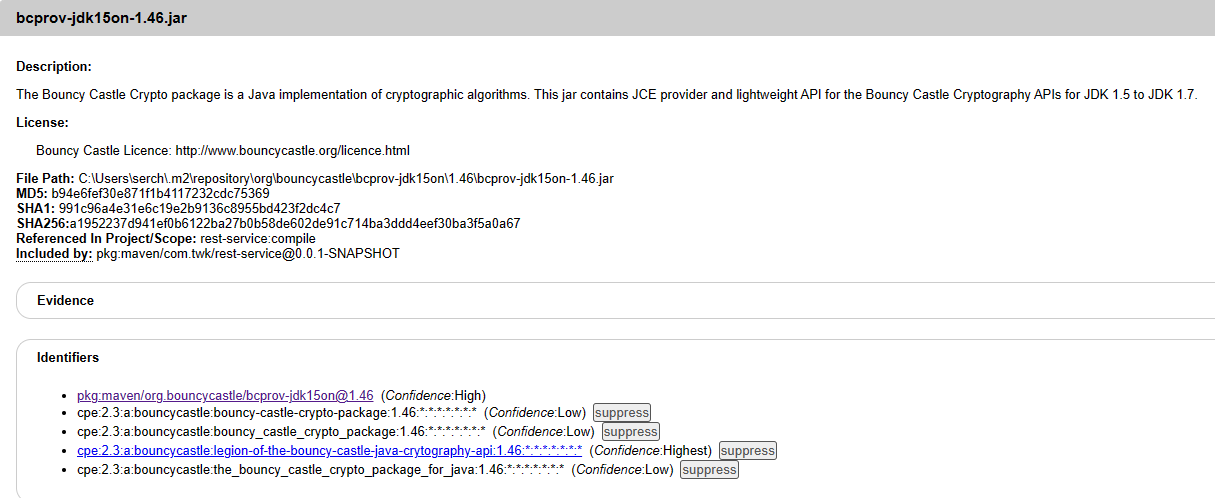
The Global Rain developers inspect the code carefully to find any type of vulnerability that could possibly cause access to malicious users. The code seen is well developed and reflects the effort from the developer but in the inspection, Global Rain developers found some problems:

* Text

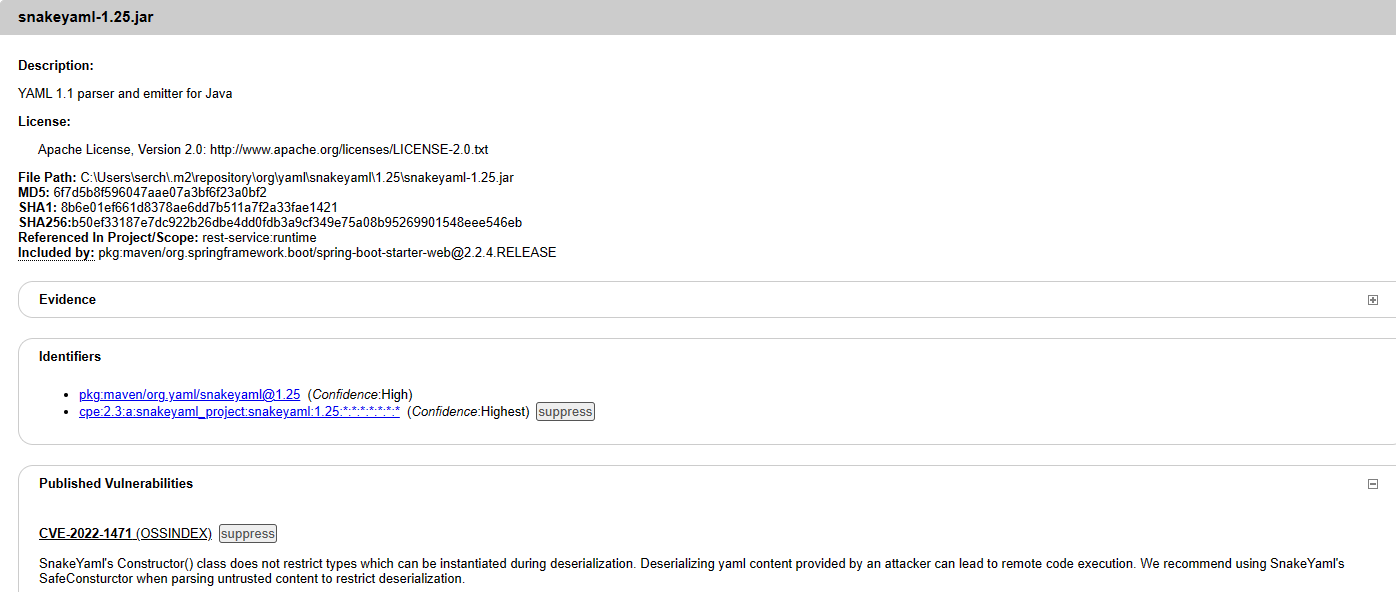
  Description automatically generatedCRUDCrontoller.java: The code exposes a vulnerability by passing business\_name the CRUD method and exposing DocData.java objects. The code does not validate the input.
* GreetingController.java: The output does not pass by the validator since the input was passed as a string. The developers were not able to confirm if the input was confirmed.
* Text

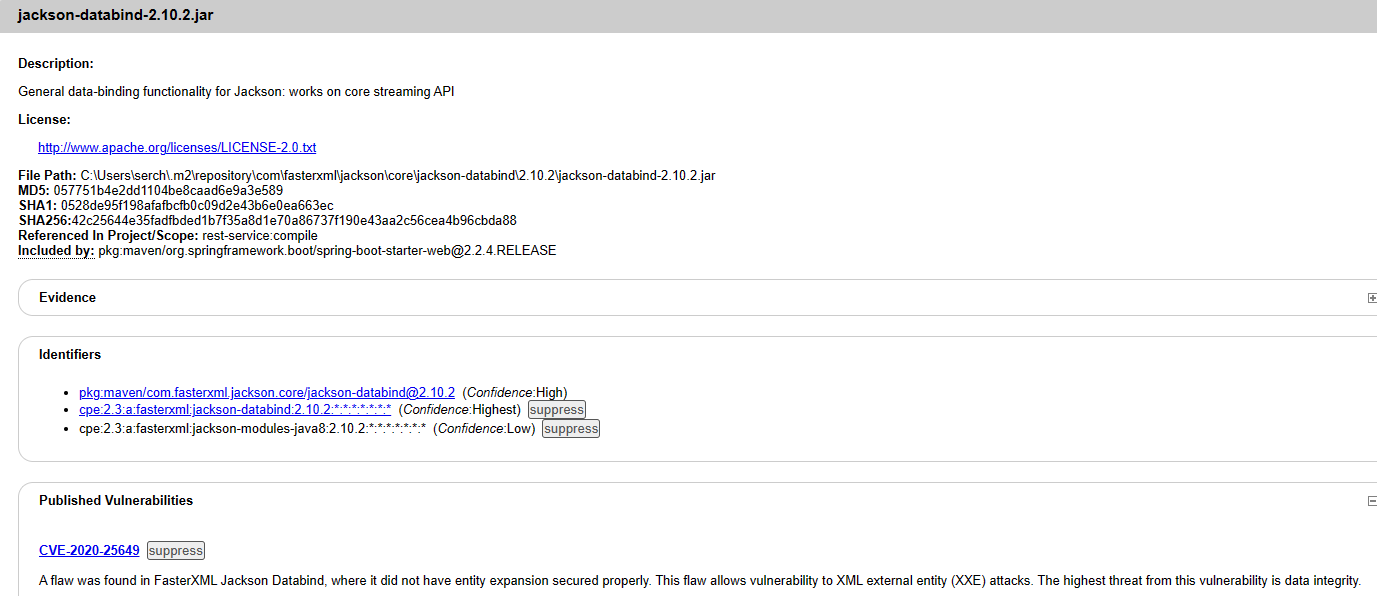
  Description automatically generatedDocData.java: There was no error present, but the code pops a try-and-catch block. No error was found but it’s something that developer must keep their eye on in case a problem appears.
* API: Global Rain developers were not able to locate the APIs, but even if the developer team were not successfully available to find the API, they still are available to access data unsecured.
* Cryptography: The Global Rain developers did not find a form of encryption in their customer information, as stated in Areas of Security, since Artemis Financial will be handling a lot of personal information, encrypting sensible information would prevent any leak of information.

## Static Testing

Graphical user interface, text

Description automatically generatedThe Global Rain developers run the code after updating the pom.xml and check the dependency-check-report to identify the possible problems that appear in the code.

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

## Mitigation Plan

After, Global Rain developers explore and analyze the results from the Manual Review and Static Testing and decide to assess Artemis Financial on how to solve these problems.

* [bcprov-jdk15on-1.46.jar](file:///C:\Users\serch\OneDrive\Escritorio\rest-service\target\dependency-check-report.html#l1_991c96a4e31e6c19e2b9136c8955bd423f2dc4c7): It must update to the latest version to mitigate the threat. Ensuring that is secured all the time since will help encrypt our information and it must be validated.
* [jackson-core-2.10.2.jar](file:///C:\Users\serch\OneDrive\Escritorio\rest-service\target\dependency-check-report.html#l4_73d4322a6bda684f676a2b5fe918361c4e5c7cca): XML parser will need to be configured. The expansion will need to be disabled to properly catch or ignore malicious codes.
* [log4j-to-slf4j-2.12.1.jar](file:///C:\Users\serch\OneDrive\Escritorio\rest-service\target\dependency-check-report.html#l11_dfb42ea8ce1a399bcf7218efe8115a0b7ab3788a): All the certificates must be valid. The browser will trust the SSL certificate, and this helps the user to identify the safe way to access the application.
* [snakeyaml-1.25.jar](file:///C:\Users\serch\OneDrive\Escritorio\rest-service\target\dependency-check-report.html#l14_8b6e01ef661d8378ae6dd7b511a7f2a33fae1421): Minimizing the number of loops and verifying that these do not cause any type of issues in the code.
* [spring-core-5.2.3.RELEASE.jar](file:///C:\Users\serch\OneDrive\Escritorio\rest-service\target\dependency-check-report.html#l17_3734223040040e8c3fecd5faa3ae8a1ed6da146b): Update to the latest version to prevent any access from the malicious user to our system.
* [tomcat-embed-core-9.0.30.jar](file:///C:\Users\serch\OneDrive\Escritorio\rest-service\target\dependency-check-report.html#l20_ad32909314fe2ba02cec036434c0addd19bcc580): Only privileged user has access to sensitive information to prevent any leak of information and preserve the security of the users.

Global Rain developers analyzed the system to prevent any malicious user access to the data and provided the results above.