****

Zheen H. Suseyi

03/19/2023

CS 305

SNHU

# Artemis Financial Vulnerability Assessment Report

**Table of Contents**

[Document Revision History 3](#_gjdgxs)

[Client 3](#_30j0zll)

[Instructions 3](#_1fob9te)

[Developer 4](#_3znysh7)

[1. Interpreting Client Needs 4](#_2et92p0)

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

[3. Manual Review 4](#_3dy6vkm)

[4. Static Testing 4](#_1t3h5sf)

[5. Mitigation Plan 4](#_4d34og8)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **03/19/2023** | **Zheen H. Suseyi** | **Worked from 03/15-03/19** |

## 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

Zheen H. Suseyi

## Interpreting Client Needs

***What is the value of secure communications to the company?***

Artemis Financial is requesting the most modern and effective means of software security possible no matter the cost. Because of this, secure communications are at a premium at this company and they really are looking for the most secure methods possible.

***Does the company make any international transactions?***

Artemis Financial is a consulting company that is in charge of a variety of different accounts which include savings, retirement, investments, and insurance. It is unclear at this moment if Artemis Financial offers their services outside the country but it is known that their website needs additional protection.

***Are there governmental restrictions about secure communications to consider?***

Again, not much is known about where exactly Artemis Financial operates because something that may be legal in one country may be completely illegal in another. Due to this, once more information is gathered then it can be determined if the software complies.

***What external threats might be present now and in the immediate future?***

There are many external threats that could really hinder the progress of Artemis Financial if left unchecked. Some threats include hackers, rogue insiders, social engineering and phishing scams, and vulnerabilities in the applications they use.

***What are the modernization requirements that you must consider?***

Open source libraries are very commonly used in development these days but can contain vulnerabilities that are prone to cyberattacks. The same issue comes with using web application technologies as there may also be vulnerabilities especially with constant updates and changes.

## Areas of Security

The most import Areas of Security to focus on are the following:

***Input Validation***

Input validation is extremely important to prevent common attacks such as SQL injections.

***Cryptography***

Without cryptography, there is no guarantee that data is safe or secure especially when being sent to others.

***Client/Server***

Making sure that only authorized users are allowed access and only certain users can perform certain actions is an extremely critical part of being secure.

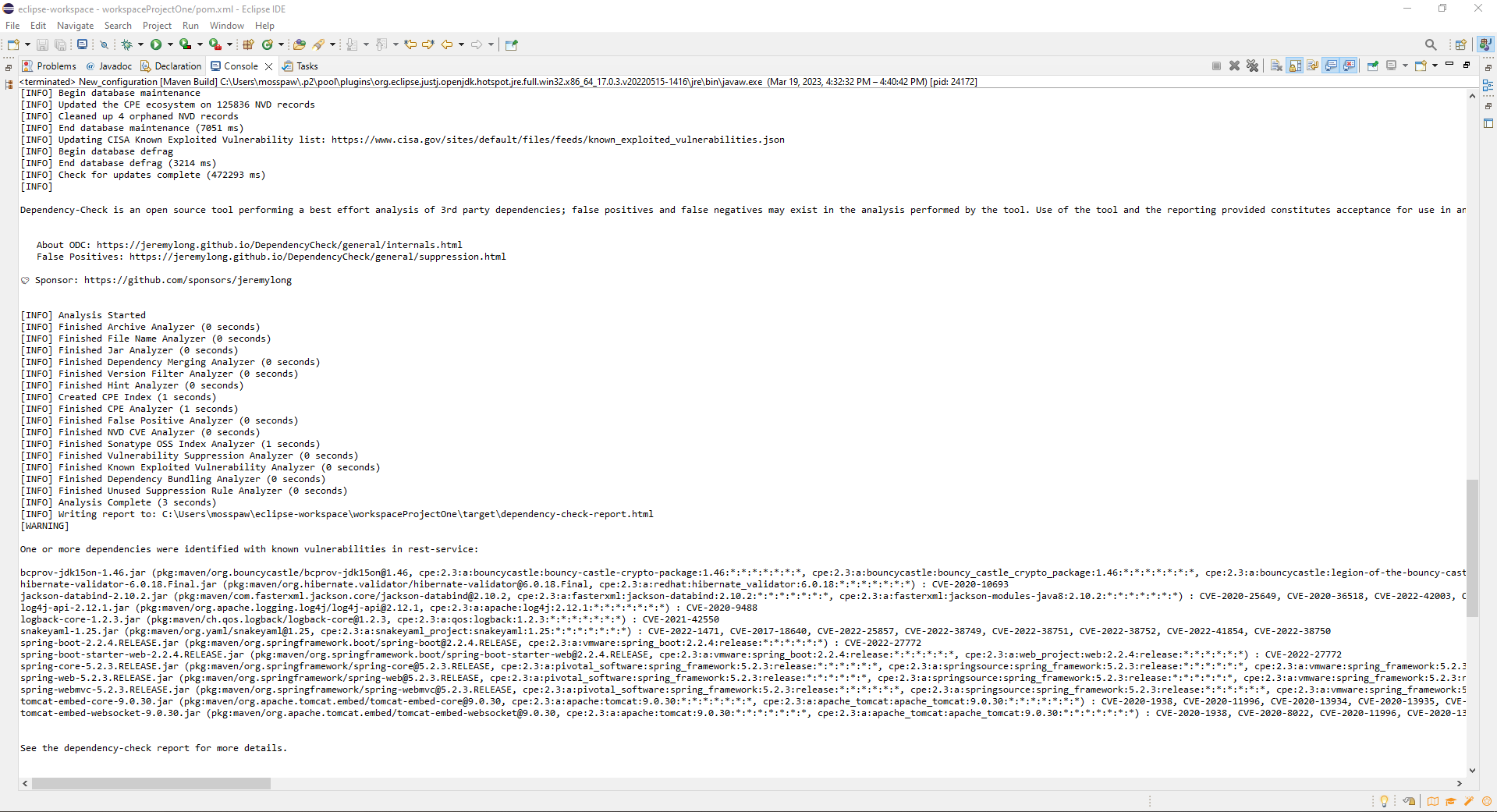
***Code Error***

Poor code can cause vulnerabilities and potentially break the entire system leaving sensitive information either wide open or lost forever.

## Manual Review

After a successful importation of the files to eclipse, in the DocData.java file, it appears that the read\_document function is incomplete and forgotten about by one of the programmers. It also appears that in this same class, sensitive information is just commented on the code. If the wrong person were to see this Java class, then they would know the database name, username, and password and could get ahold of extremely sensitive information. Another big blunder is the myDateTime.java class which shows more incomplete functions. Lastly, the pom.xml file owasp dependency check is outdated. I went ahead and corrected it from version 5.2.0 to version 8.1.2.

## Static Testing

Here is the result from a maven dependency check:  
  


If zoomed in, the following vulnerabilities were found:**bcprov hibernate jackson log4j logback snakeyaml spring-boot-2.2.4 spring-boot-starter web spring-boot-5.2.3 spring-web-5.2.3 spring-webmvc-5.2.3 spring-embed-core-0.0.30 tomcat-embed-websocket-0.0.30 tomcat-embed-core-9.0.30.**

Whether these vulnerabilities are serious or false alarms must be looked into, but this was the reality of the maven dependency check which took about 8 mins on my machine.

## Mitigation Plan

The first plan of action must be to determine whether Artemis Financial does any international business because then they may have to make some major changes depending on the countries they are doing business in. This includes compliance with the various governments in the countries they are dealing in and that all software is allowed from their website. The next thing that must be looked at is prevention from any future attacks and this can be done using education. It would be a good idea to have Artemis Financial employees attend a meeting where they can get educated on preventing unauthorized access and avoiding social engineering and phishing attempts. The areas of security mentioned earlier in this document still apply here and should definitely be considered in any further operations at Artemis Financial. The last area of recommendation I have for Artemis Financial would be to look at the code your programmers are writing especially in the comments because I found some extremely sensitive information just written in a comment that any attacker or rogue employee would have a field day with. The programs are also using outdated libraries and a lot of the functions were either not filled out yet or just simply forgotten about. Clearly, the programmers at Artemis Financial need to focus harder on their work and bring it up to speed.