****

# 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** | **3/15/2021** | **Kyle Pavlack** |  |

## 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

Kyle Pavlack

## 1. Interpreting Client Needs

Determine your client’s needs and potential threats and attacks associated with their application and software security requirements. Consider the following regarding how companies protect against external threats based on the scenario information:

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

The value of secure communications has increased the confidence of the customer not only through email threads but the overall privacy of the company and the customer as well.

* **Are there any international transactions that the company produces?**

There are some internal transactions as the company is a web based company. With that being said the transactions come from buying and selling stocks throughout the company to help grow the customers savings, investments, and retirement.

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

When you are talking about stocks, money, investments there are always government regulations that want to control how your communicating amongst the client and the industry. The government is trying to regulate the communication by allowing passageways through private communication so that way the private communication chain is broke and can allow the possibility of hackers to access information and steal.

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

With the government having their feet in the pool, the threat is like I said above and that breaking the private communication chain, it leaves clients/businesses vulnerable for attacks of private and financial information.

* **What are the “modernization” requirements that must be considered, such as the role of open source libraries and evolving web application technologies?**

Some examples of modernization happening amongst the company is that they went completely web based and that their adding double authentication for extra layers of security. Having open source libraries helps the business have more functionality and can help improve the layers of security.

## 2. Areas of Security

Referring to the Vulnerability Assessment Process Flow Diagram, identify which areas of security are applicable to Artemis Financial’s software application. Justify your reasoning for why each area is relevant to the software application.

Some areas that I found important to incorporate within the security for the software application have been including API’s, Cryptography, Client/Server, and Secure Coding.

API’s – this stands for Application Programming Interface and since the company is a web based business having this will help with the security and functionality of the website. Creating a configuration between the API and the software system will help create a layer of security that keeps the information safe and secure

Cryptography – I find this security feature quite important as being a web based business, all your performance and actions are online and without having the proper encryption to have all your communication and transactions covered leaves gaps for compromise. The time from transactions happening between the customer and client are the times of most vulnerability and increasing the security footstep to strengthen communication barriers only benefits in the long run.

Client/Server – This feature seems straight forward as there is communication between the client and the server that has been created to perform the functions and transactions amongst the financial software. Having a weak client/server bond can destroy the opportunities the client is looking for within the company.

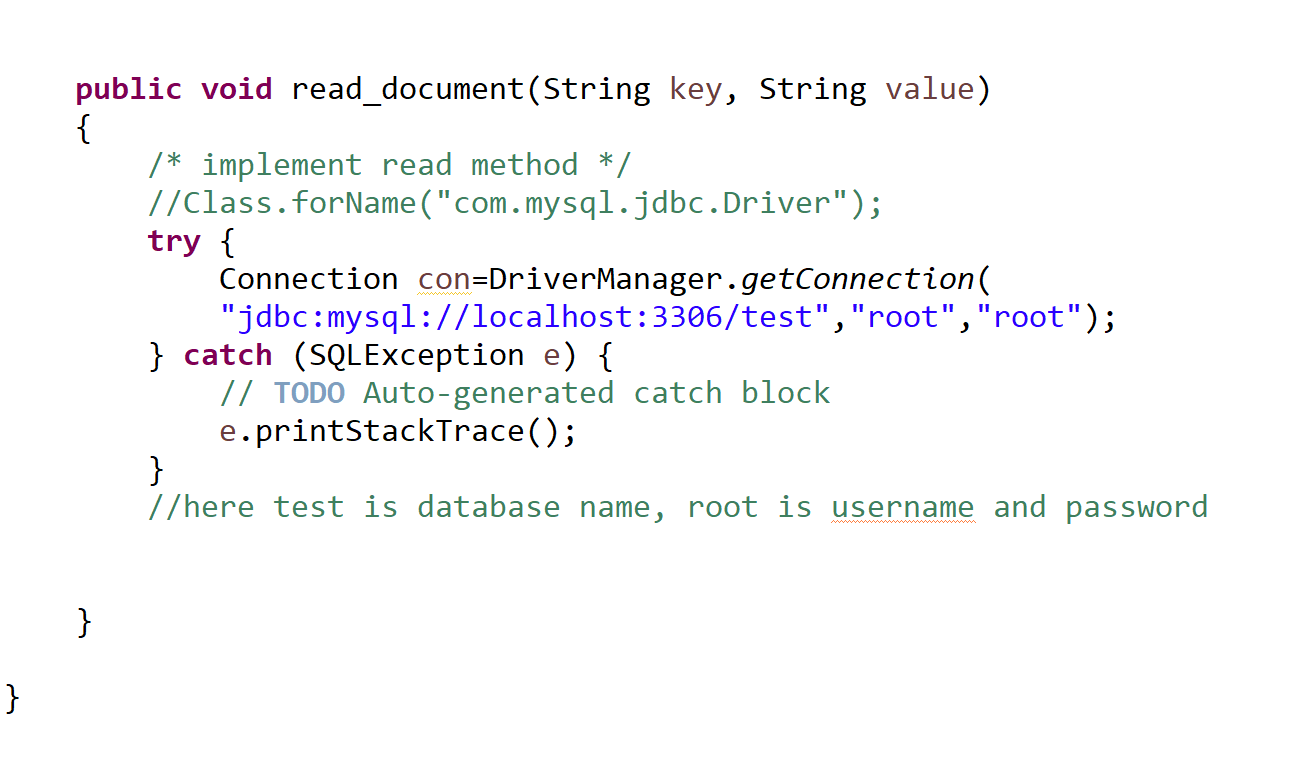
Secure Coding – Maybe the most important part of the security features as its essentially the base layer of the business for security. Without having a good code base that promotes consistency and logic to the application you can see yourself having syntax errors and problems down the road.

## 3. Manual Review

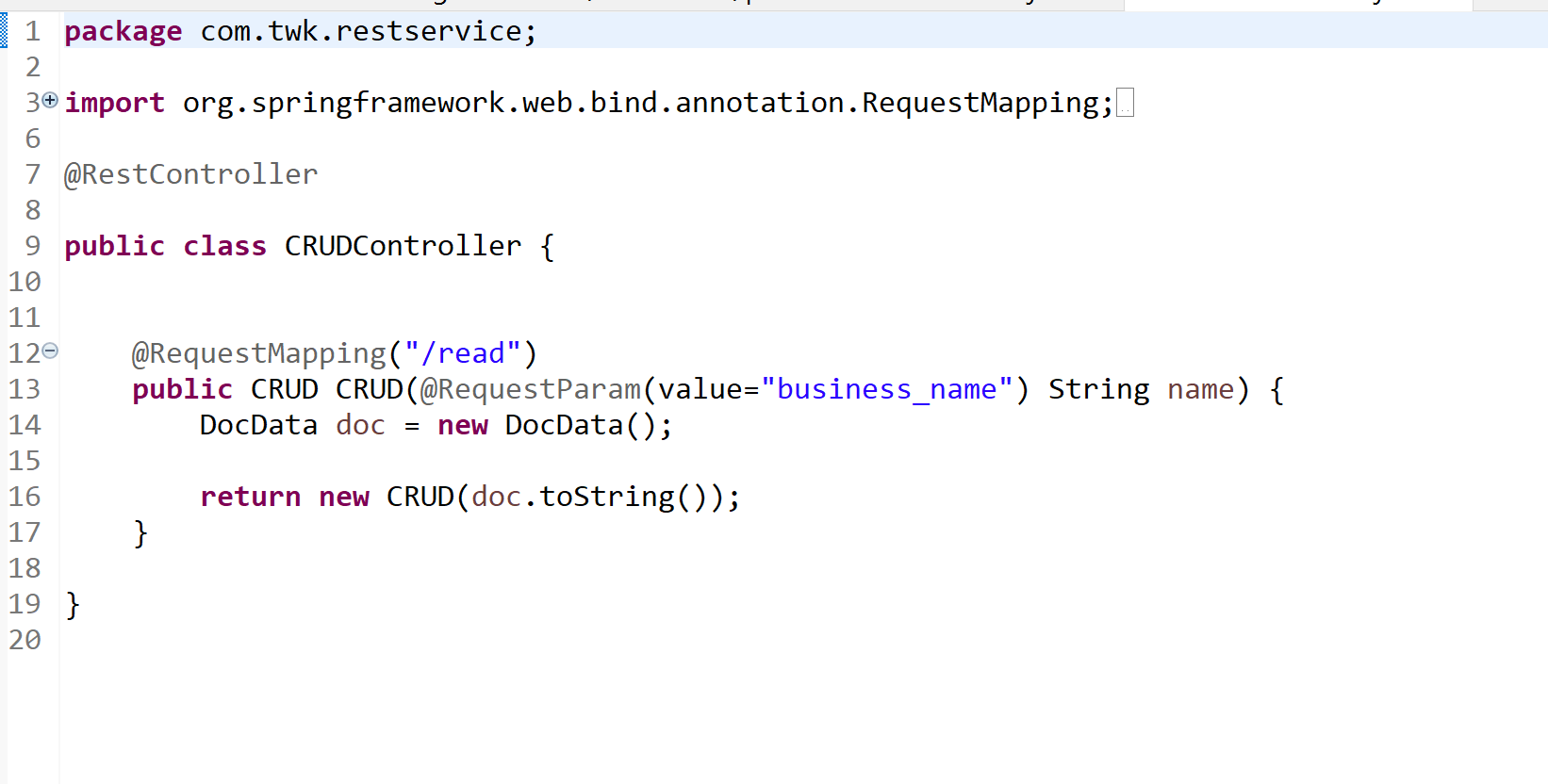
Continue working through the Vulnerability Assessment Process Flow Diagram. Identify all vulnerabilities in the code base by manually inspecting the code.

Some vulnerabilities that I found looking through the code are as following:

Data Access – In the file DocData.java it shows that the data access method used has some vulnerabilities involved amongst the location of the database, username, and the password. There is the root user and password that has potential to be compromised due to the password being easily guessed making the data have cracks and weakness amongst the coding that can compromise the business.

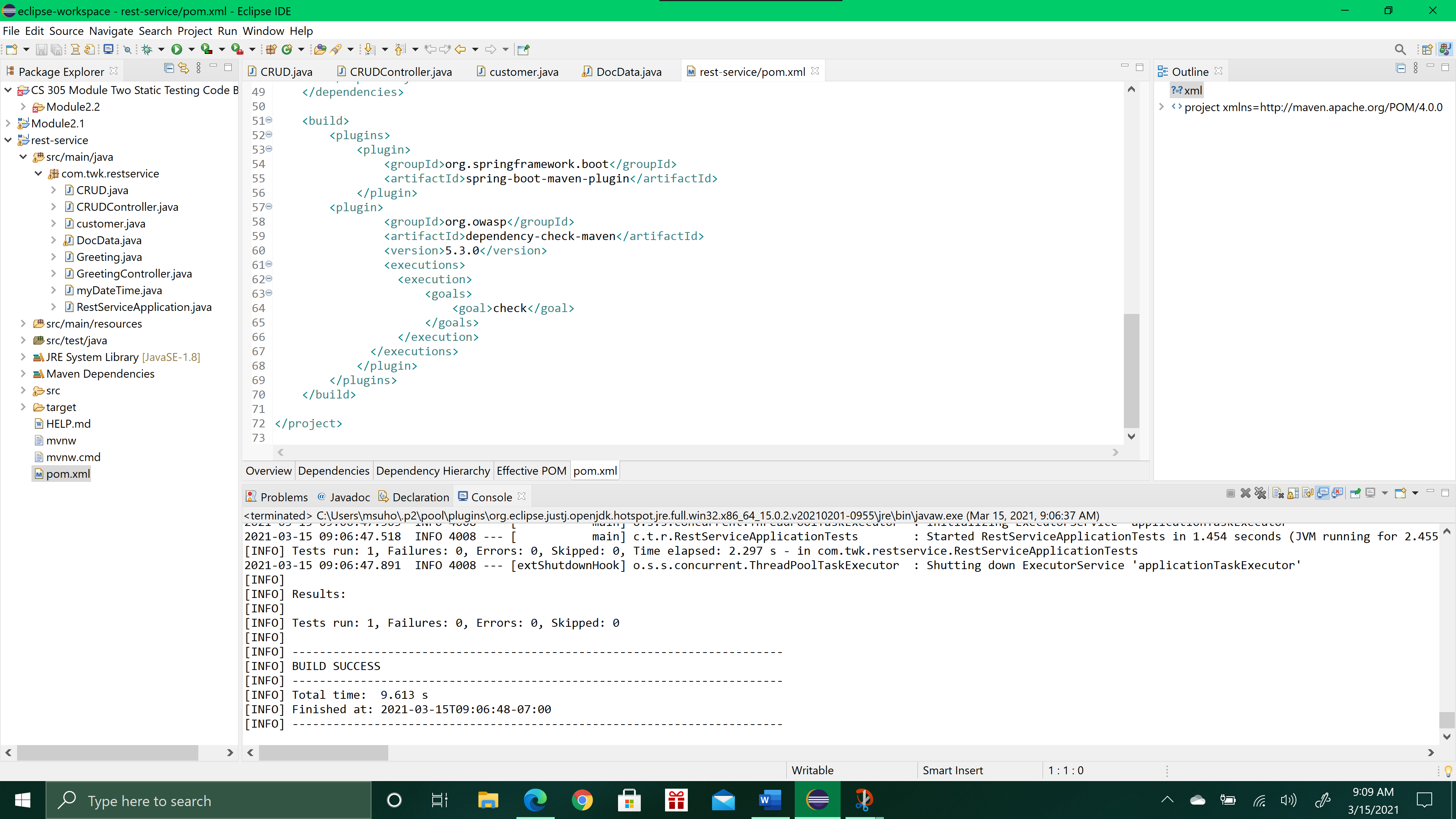


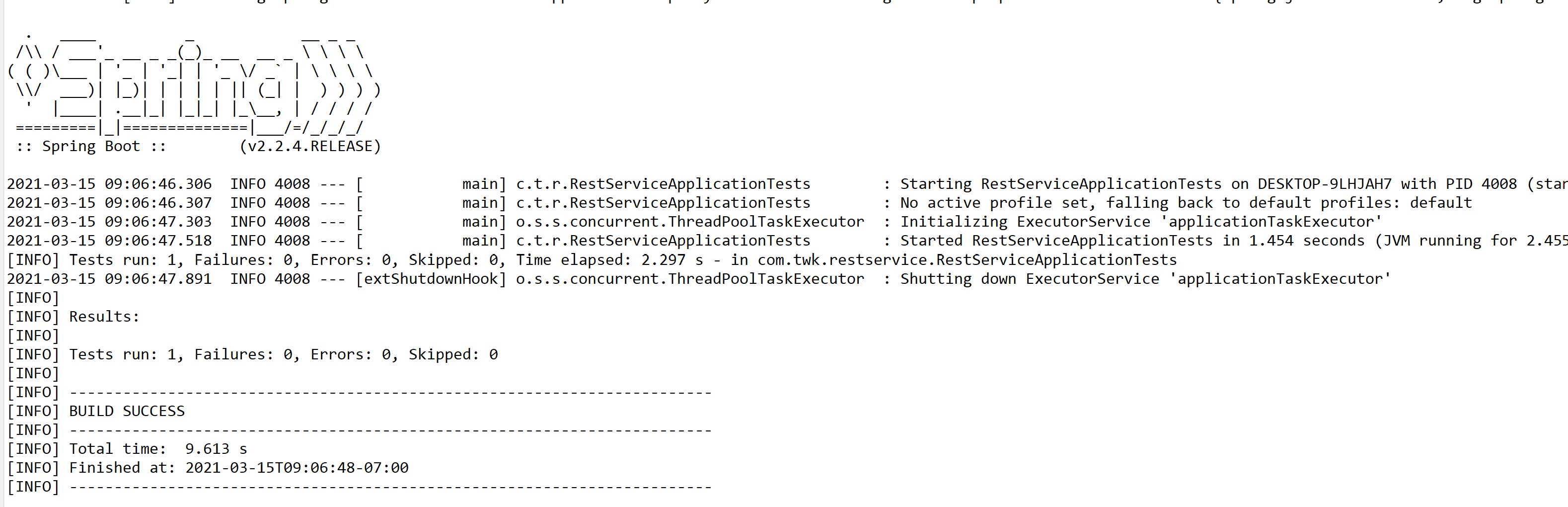
Another vulnerability that could be present was in the CRUDController.java file as it could fall into the Direct Object Reference security feature. The possibility of showing the internal objects can be passed with a series of code injections that can maybe expose the data access.



## 4. Static Testing

Run a dependency check on Artemis Financial’s software application to identify all security vulnerabilities in the code. Record the output from dependency check report. Include the following:





Some Vulnerabilities that were present in the dependency check were:

CVE-2020-9488 – This code interacts with the certificate validation. This can lead to possible connection attacks leaving the user stranded. To address this we will update the server that will enhance the security settings.

CVE–2013–1624 – This error is stating that the java library has no proper security on timing from side channel attacks. We would want to incorporate proper time checks to help prevent data attacks.

## 5. Mitigation Plan

After interpreting your results from the manual review and static testing, identify the steps to remedy the identified security vulnerabilities for Artemis Financial’s software application.

Some plans that we want to take action on are updating the data access username and passwords, increase the review of code and ability to modify it, and certificate validation.

Data Access Username/Password:

This area showed a little weakness throughout the base code file and needs to be improved. When creating the password you want to make it a strong combination of alphanumeric characters and shouldn’t incorporate your username. Creating double authorization for security is important to help add that extra layer of protection for the database and the user control.

Code Review:

Having a great base of code that outlines the ability and function needed is key. The quality of code needs to be improved to have proper authentication and the ability to catch errors almost instantaneously. Improving just those 2 things will help the exploitations of authentication vulnerabilities.

Certificate Validation:

There are various certificates that should be validated that will allow proper validation and verification of the applications in the web server.