****

# 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 5](#_Toc32574613)

[4. Static Testing 7](#_Toc32574614)

[5. Mitigation Plan 8](#_Toc32574615)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **11-13-2020** | **Jeffrey Dominguez** | **Gave information over clients needs, area of security, reviews, testing and a mitigation plan** |

## 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**

Jeffrey Dominguez

## 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 communication to a company is increased customer confidence. Secure communications affect more than just office emails. It affects the privacy or your customers too.

* Are there any international transactions that the company produces?

Artemis Financials’ does have internal transactions due to it being a web-based company. The transactions are consisted of the buying and selling of stock to make money for client’s savings, retirement, and investments.

* Are there governmental restrictions about secure communications to consider?

There are many governmental restrictions about making communications secure especially when dealing with money, stocks, and retirements. However, currently there is a bill to add back doors into all American communications which will not only delete privacy, it will open the software to unwanted (non-American Government) from hacking into and stealing any private information and/or money.

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

The current threats we are facing now and, in the future, include rival companies, non-US governments. The hacker group anonymous. With this information, security is extremely important for the company and the protection of its users.

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

The modernization requirements include being making the company completely web based and adding extra security. This includes advancements in security and making the web application that works in a sand-boxed mode to ensure great security. The company can take advantage of an open source library to add more layers of protection and functionality to their program.

## 2. Areas of Security

The main areas of security include API, cryptography, client/server, and secure coding.

API – This is an area of security is needed because the web application has the use of APIs. We need a secure configuration for the APIs to allow no compromise between the system and the API. This is required to ensure everything is safe and secure.

Cryptography – This is used because there is the ability to access and transmit information through the internet. With lack of proper encryption during a transfer; there can be a compromise of the integrity and confidentiality of the private information during transit. The process of the information being transmitted over the internet between the company and customer is the prime time to attack. With proper certificate validation and encryption, this can be avoided.

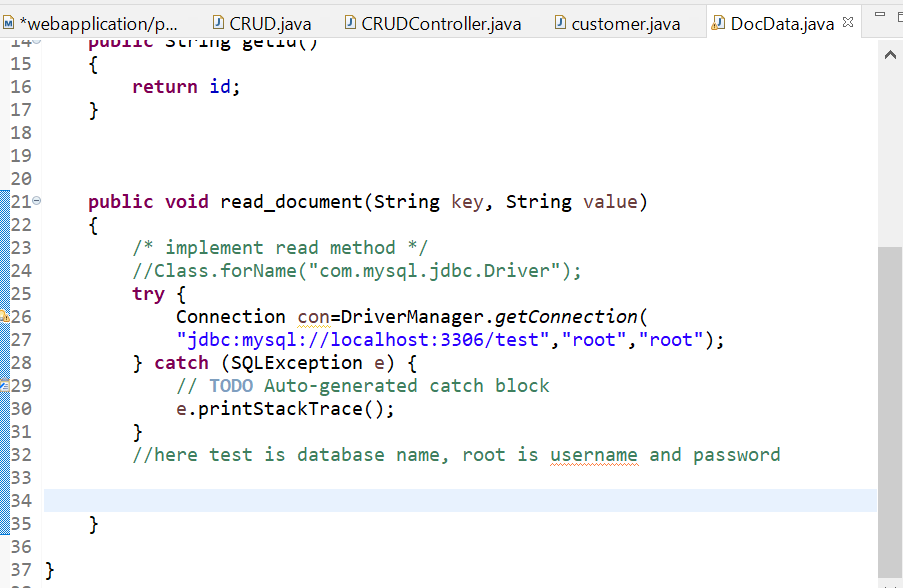
Client/Server – This part of security is used due to how the web application involves the communication between the client and the backend of the web application (server) where it retrieves and transact financial transactions. This security is very important because the connection between the two can build or destroy trust.

Secure Coding – Secure coding applies to the application because here are multiple situation and scenarios that require the code to be secure to maintain a consistency in the logic of the application. Like handing error checks for example.

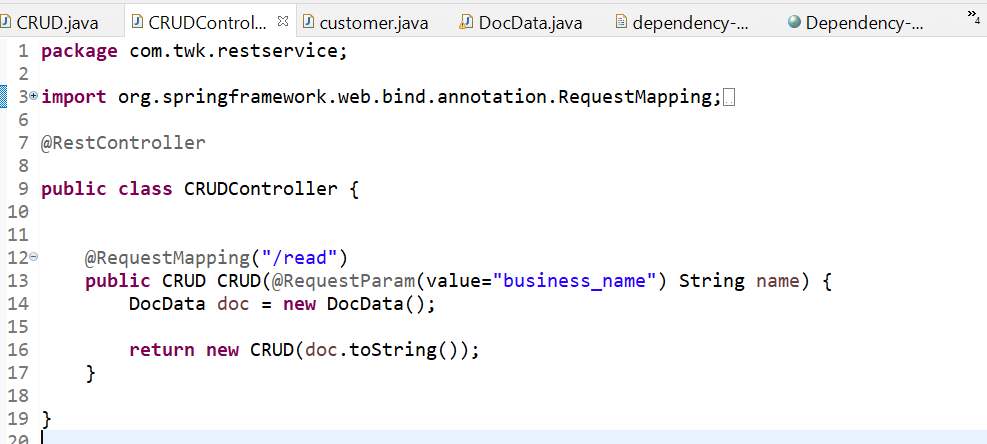
## 3. Manual Review

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

Data Access – There is a vulnerability in the data access. In DocData.java, the data access method that is used involved the definition of where he location for the database, username, and password has some vulnerabilities. There is the root users and the password which is not recommendable to use the root user. The root password can be easily guessed and compromised. The root is used as the username and as the password. This makes it easy to crack and unauthorized users can access the system by brute force attacks.



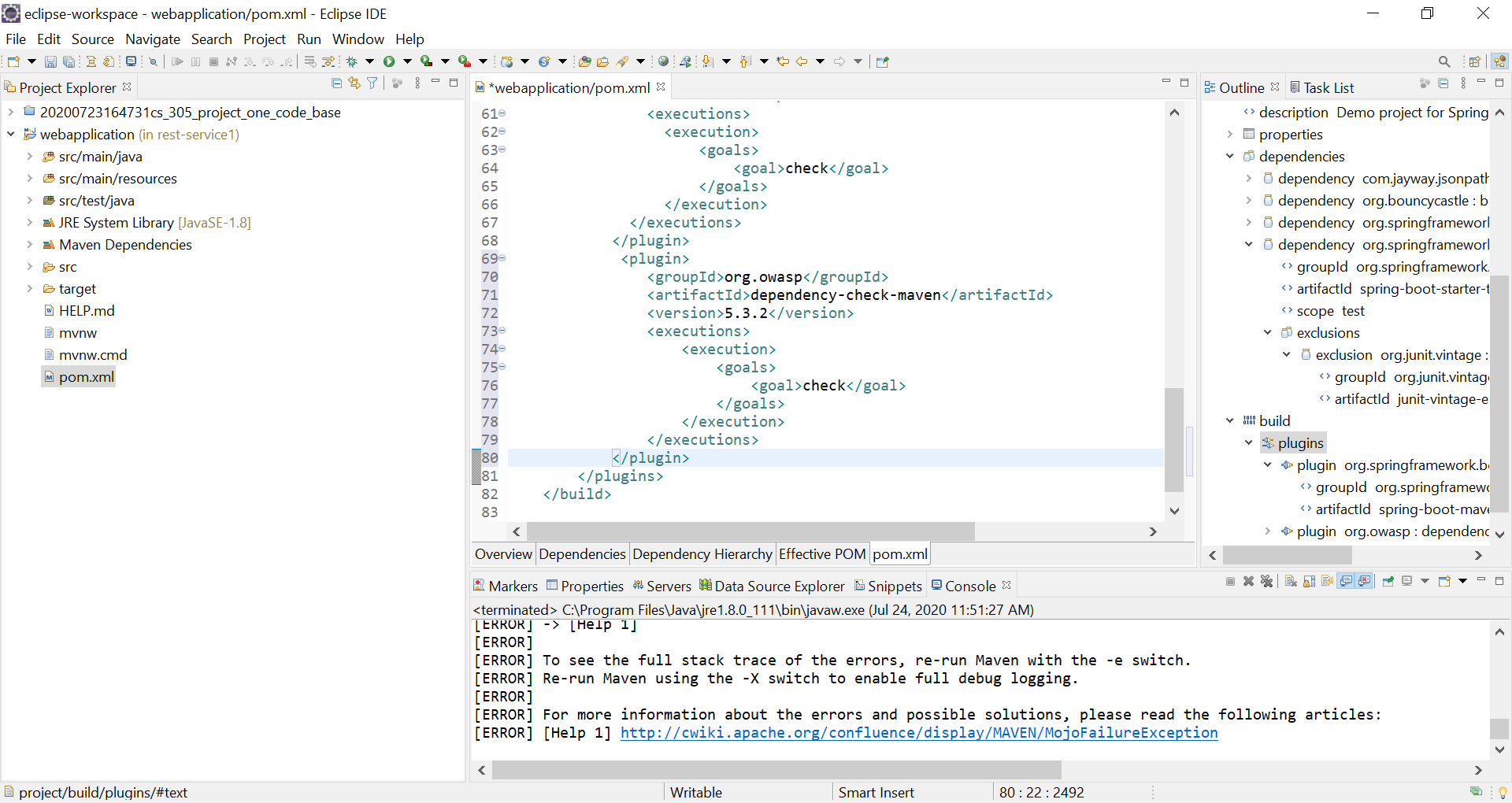
Direct Object Reference – There is one vulnerability in the CRUDController.java where these is a possibility of the application possibly showing the internal objects. This can be passed and accessed through a series of code injection. The **Value = “business\_name”** is passed into the CRUD method which might expose the **DocData** object data access vulnerability.



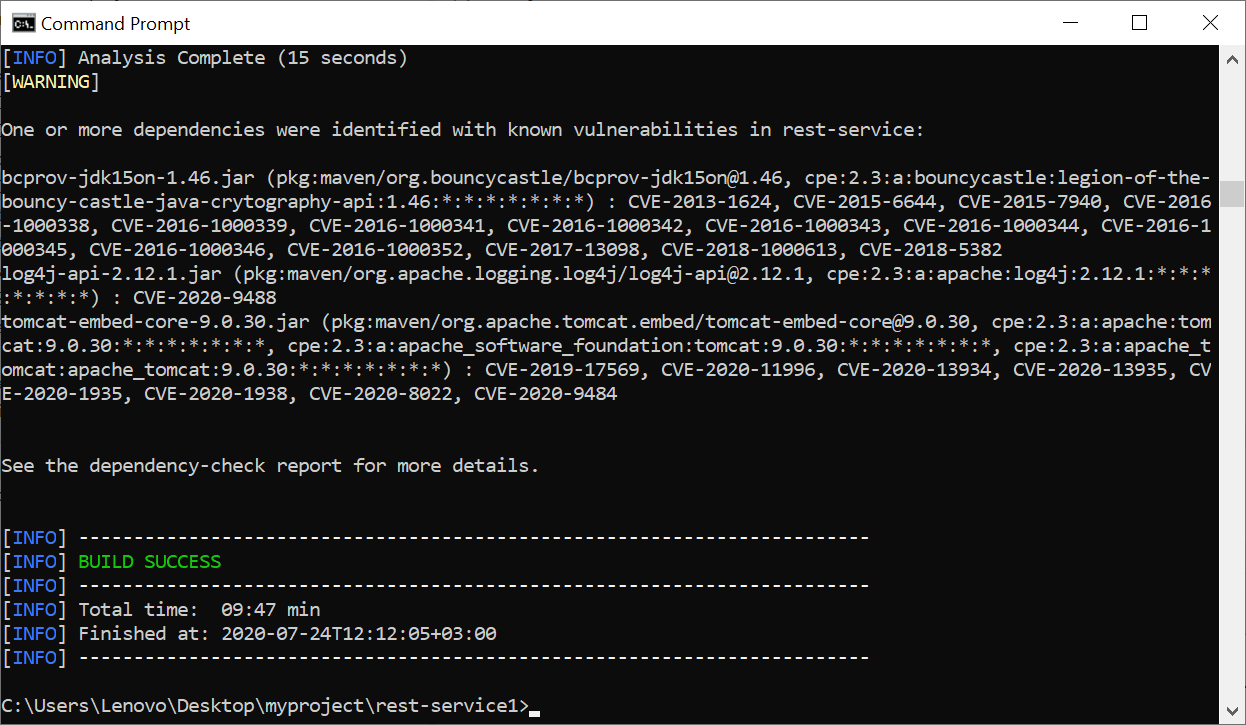
## 

## 4. Static Testing

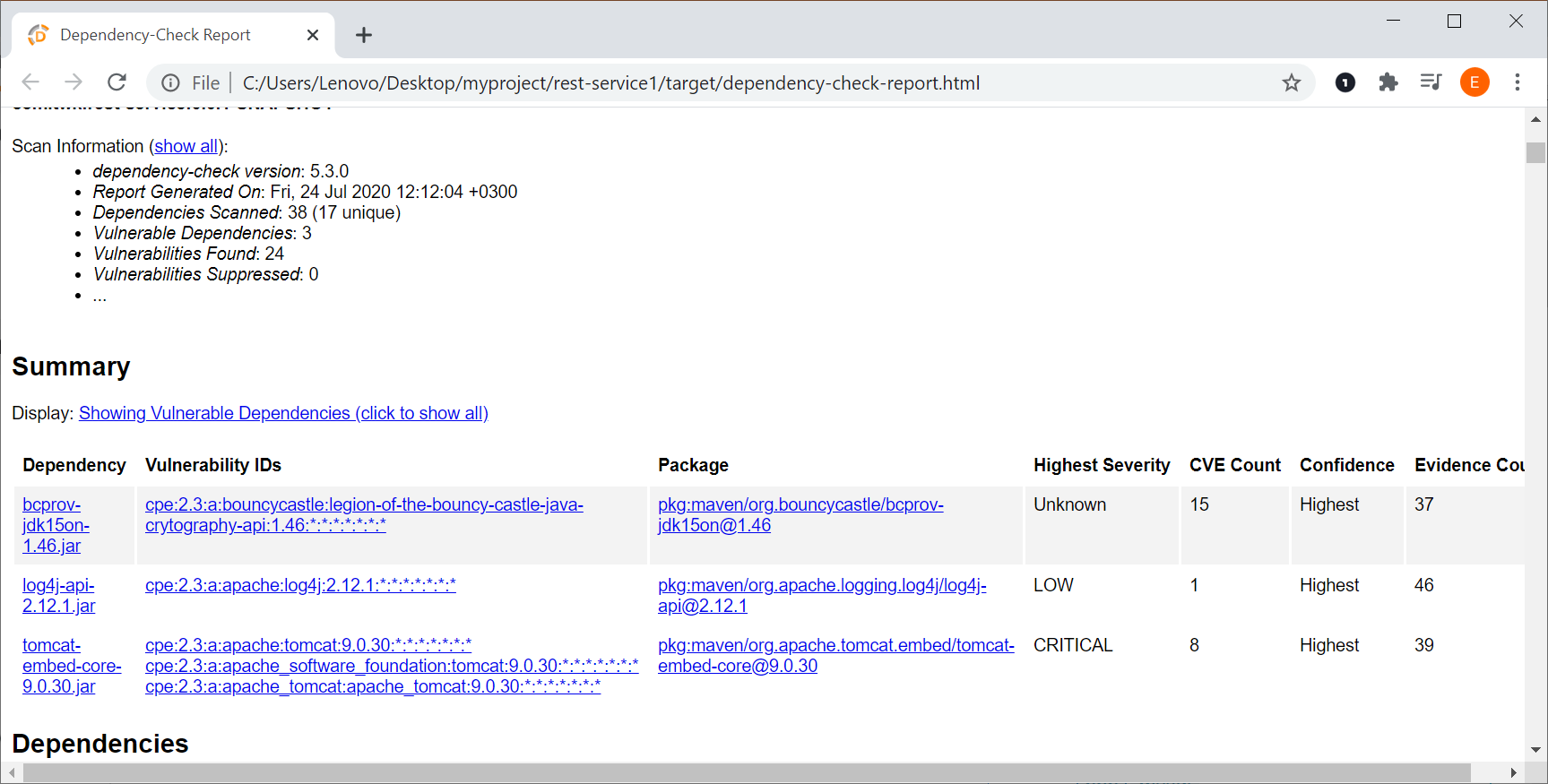
## Dependency check plug-in integration into Maven



Cleaning the plug-in code insertion using MVN clean verify command



Dependency check showing all vulnerabilities.



**Vulnerabilities**

|  |  |  |
| --- | --- | --- |
| Code | Desc | Mitigation |
| CVE-2020-9488 | This vulnerability is associated with issues of certificate validation in Apache SMTP appender. Hence, there is a possibility of intercepting connections through the man-in-the middle attacks.  Improper validation of certificate with host mismatch in Apache Log4j SMTP appender.. | Updating the server to 2.13.2 will enhance the support of security measures. It prevents setting of mail.smtp.ssl.checkserveridentity to a true value which makes the app vulnerabile (Apache, 2020) |
| CVE-2013-1624 | The TLS implemented in Java library has no proper consideration on the timing side channel attacks. This enables a remote attacker to exploit the plaintext-recovery attacks through statistical analysis conducted on timing data. | Proper timing checks should e done and considerations on side-channel attacks should be implemented to prevent timing data attacks. |
| CVE-2015-6644 | This is a vulnerability that is associated with the Bouncy Castle and can result to information disclosure. A malicious application may access the private information stored in the database | Regular updates of the application should be done as well as the underlying operating system to prevent malicious applications to compromise the security of this application (Source, 2016) |
| CVE-2020-13935 | Payload length which is related to WebSocket does not have proper validation (found in the Apache Tomcat). Such would trigger infinite loop for DoS attacks | Proper validation is required for the WebSocket Framework |

## 5. Mitigation Plan

*Data access username and password*

The data access username/password needs to be properly created. The password should be strong combination of alphanumeric characters and should not have the words from username which are easy to guess. There should be a created user apart from the root to be used in accessing the database in the application.

*Code review and modification*

The code needs to be review and modified to integrate secure code practices. The quality of the code should be improved so as proper authentication and catching of errors should be done. (Bhalla et al. 2020). This will restrict attacks like man in the middle and other exploitations of authentication vulnerabilities.

*Updating Apache server*

It is extremely important to update the Apache server to the recent version so as to prevent the exploitation of the CVE-2020-9488 vulnerability. Regular updates are mostly used to fix any security problems that are found in older and current version of the software.

*Certificate Validation*

The various cryptographic certificates should be well validated. The codes should be sanitized to allow proper validation and verification of the digital certificates in the application and in the web server. This will prevent the exploitation of the CVE-2020-9488, CVE-2020-13935 and man-in-the middle vulnerabilities.

*TLS Certificate mutual checking*

There needs to be an implementation of the mutual check on both sides of the server/client done through pinned certificates. Doing this will slow down the chance of the bouncy castle vulnerabilities exploits (Hu et al. 2019). IT will also help stop the compromise of a client API request and authentication procedures.

Hu, Q., Asghar, M. R., & Brownlee, N. (2019). Checking certificate revocation efficiently using certificate revocation guard. *Journal of Information Security and Applications*, *48*, 102356.

Mooij, A. J., Ketema, J., Klusener, S., & Schuts, M. (2020, February). Reducing Code Complexity through Code Refactoring and Model-Based Rejuvenation. In *2020 IEEE 27th International Conference on Software Analysis, Evolution and Reengineering (SANER)* (pp. 617-621). IEEE.

Rahman, R. U., Wadhwa, D., Bali, A., & Tomar, D. S. (2020). The Emerging Threats of Web Scrapping to Web Applications Security and Their Defense Mechanism. In *Encyclopedia of Criminal Activities and the Deep Web* (pp. 788-809). IGI Global.

Mondschein, C. F., & Monda, C. (2019). The EU’s General Data Protection Regulation (GDPR) in a research context. In *Fundamentals of Clinical Data Science* (pp. 55-71). Springer, Cham.