****

# Practices for Secure Software Report

Table of Contents

[Document Revision History 3](#_Toc102040754)

[Client 3](#_Toc102040755)

[Instructions 3](#_Toc102040756)

[Developer 4](#_Toc102040757)

[1. Algorithm Cipher 4](#_Toc102040758)

[2. Certificate Generation 4](#_Toc102040759)

[3. Deploy Cipher 4](#_Toc102040760)

[4. Secure Communications 4](#_Toc102040761)

[5. Secondary Testing 4](#_Toc102040762)

[6. Functional Testing 4](#_Toc102040763)

[7. Summary 4](#_Toc102040764)

[8. Industry Standard Best Practices 4](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **6/23/24** | **Sally Keith** |  |

## Client



## Instructions

Submit this completed practices for secure software report. Replace the bracketed text with the relevant information. You must document your process for writing secure communications and refactoring code that complies with software security testing protocols.

* Respond to the 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 Two Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Sally Keith

## Algorithm Cipher

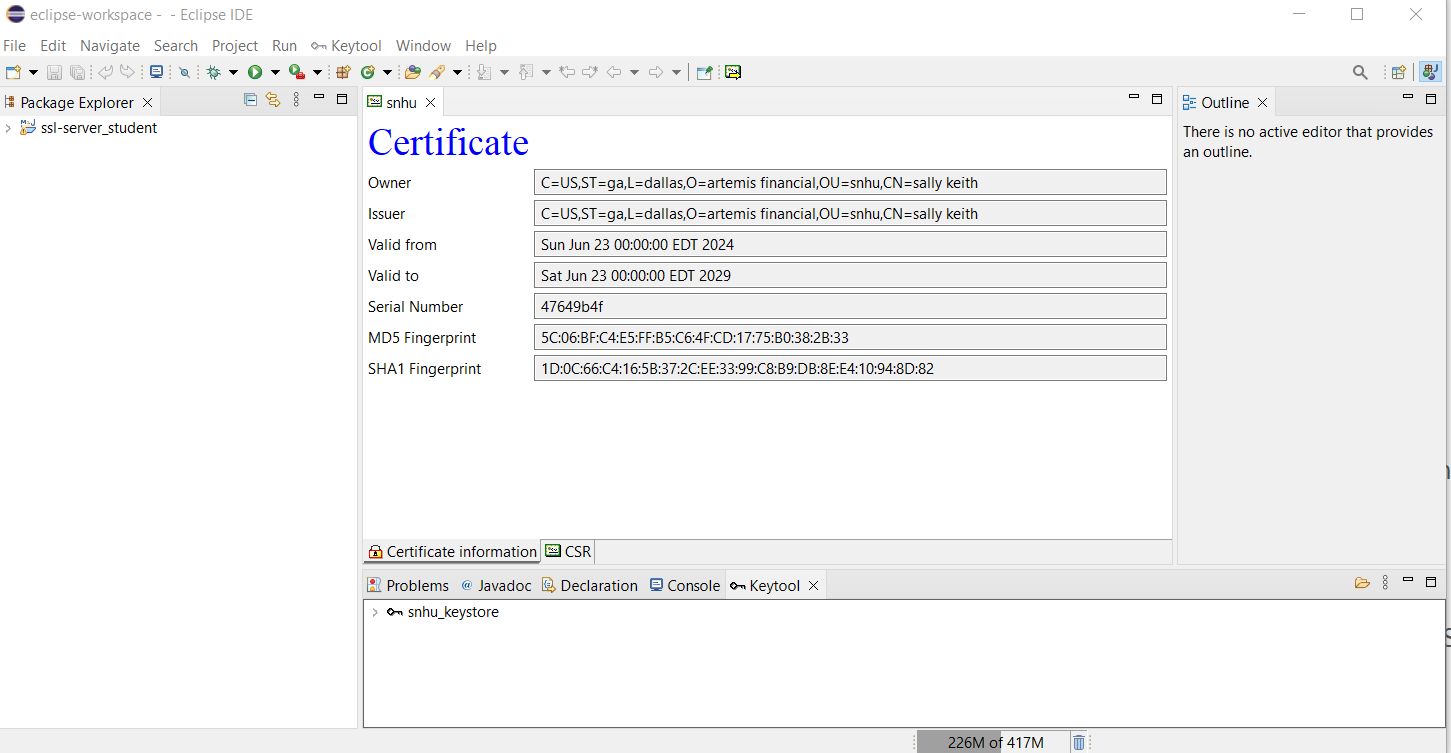
Artemis Financial wants to encrypt it’s archive files and for this the Algorithm Cipher I recommend is AES. There are security attacks such as DDoS (denial-of-service) and attacks where attackers can crack the password files. Attackers may even be able to steal entire files or databases containing important financial information. AES is incredibly secure and virtually impossible to crack when set up properly. (Kiteworks) AES is approved by the Federal Information Processing Standards Publications and the Secretary of Commerce.

The algorithm cipher will be used to protect financial information and data such as passwords and usernames, and other information such as account balances, addresses, names, etc. AES is the best cipher because it has been around for quite some time and has proven to be one of the most secure algorithm ciphers, and it is approved by government regulations. When it comes to something as sensitive as financial information you definitely want the most secure algorithm cipher possible. You would only choose something else if you had a less secure project that you were handling.

The purpose of the cipher’s has functions and bit levels is to confuse any potential attackers from decoding what the actual information is. Random numbers and symmetric keys are also used to prevent attackers from decoding what the information is. Algorithms have a long history of protecting information and with attackers on the rise ciphers have evolved to keep up with the demand of securing sensitive information. There are now trusted and true algorithm cipher’s such as AES that protect sensitive information.

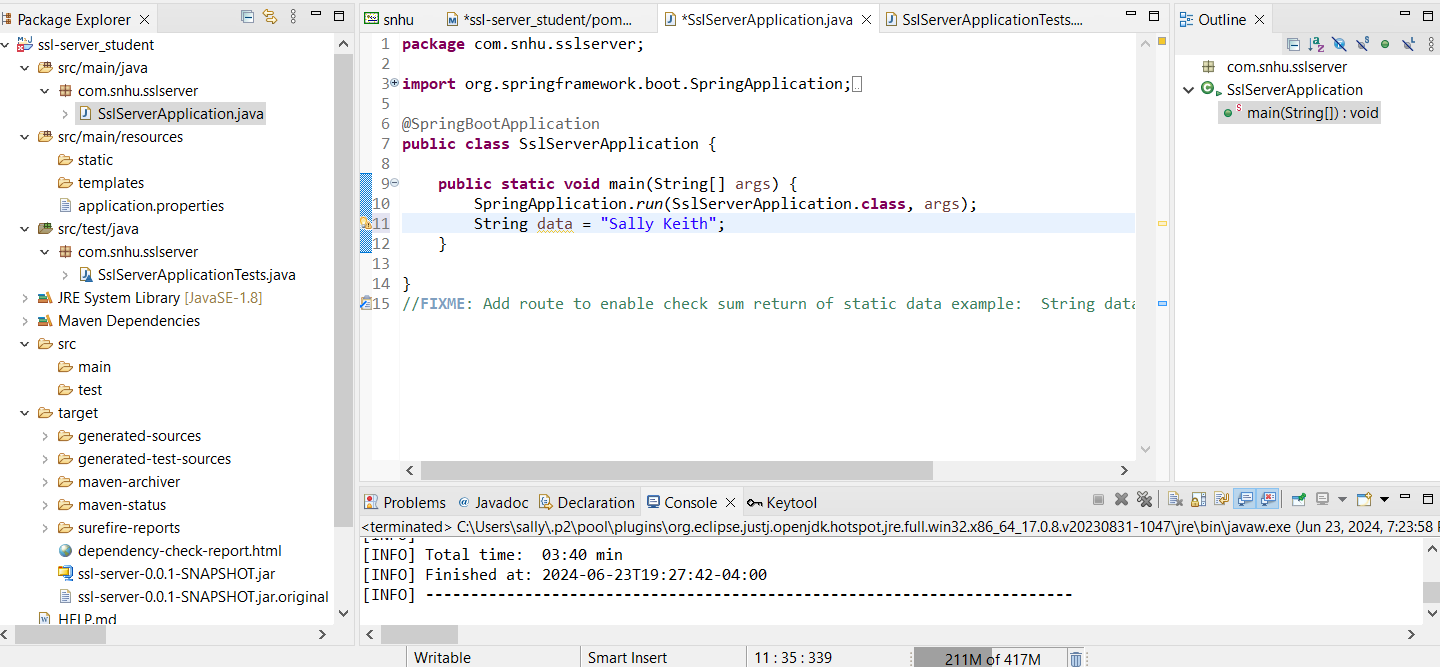
## Certificate Generation

Insert a screenshot below of the CER file.



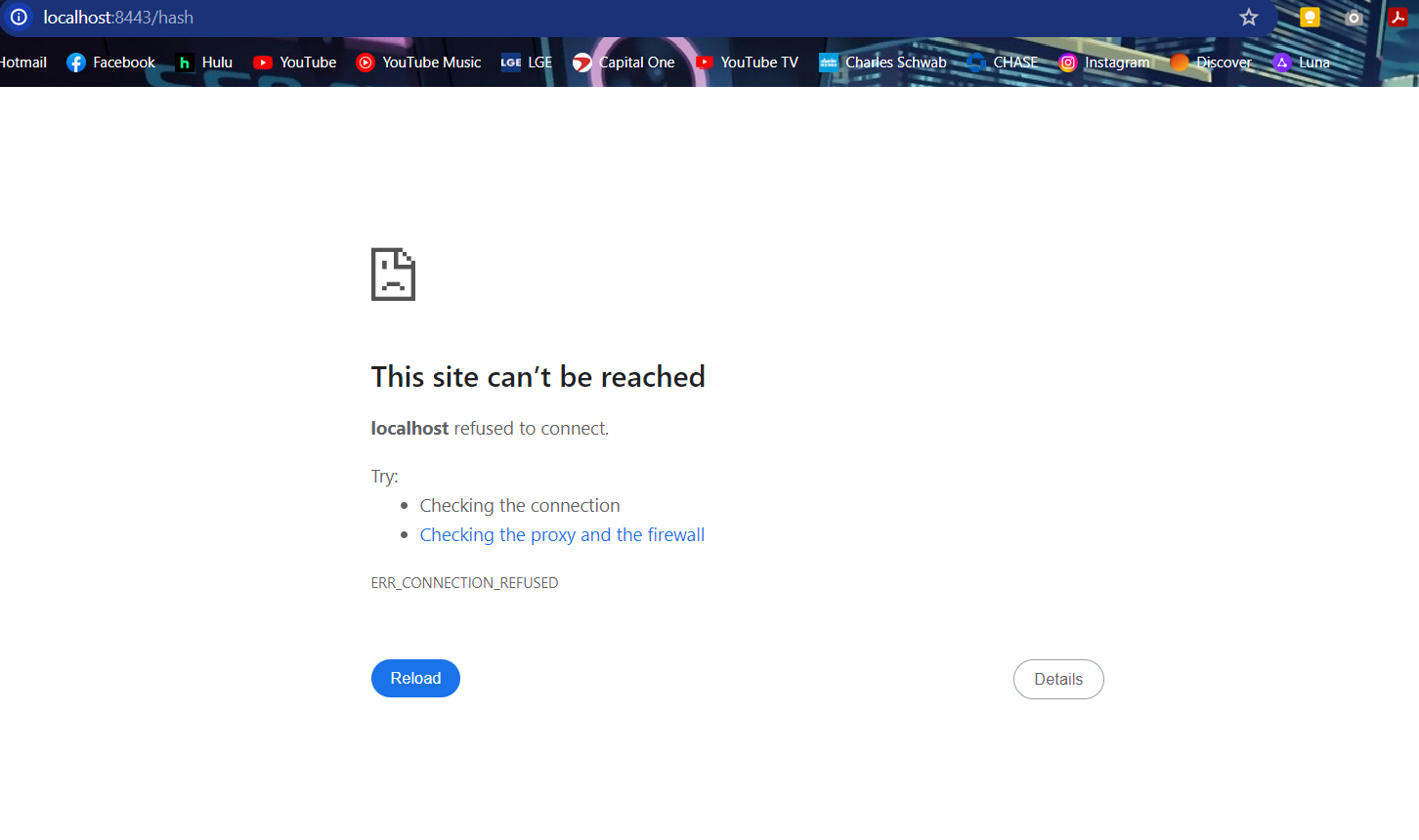
## Deploy Cipher

Insert a screenshot below of the checksum verification.



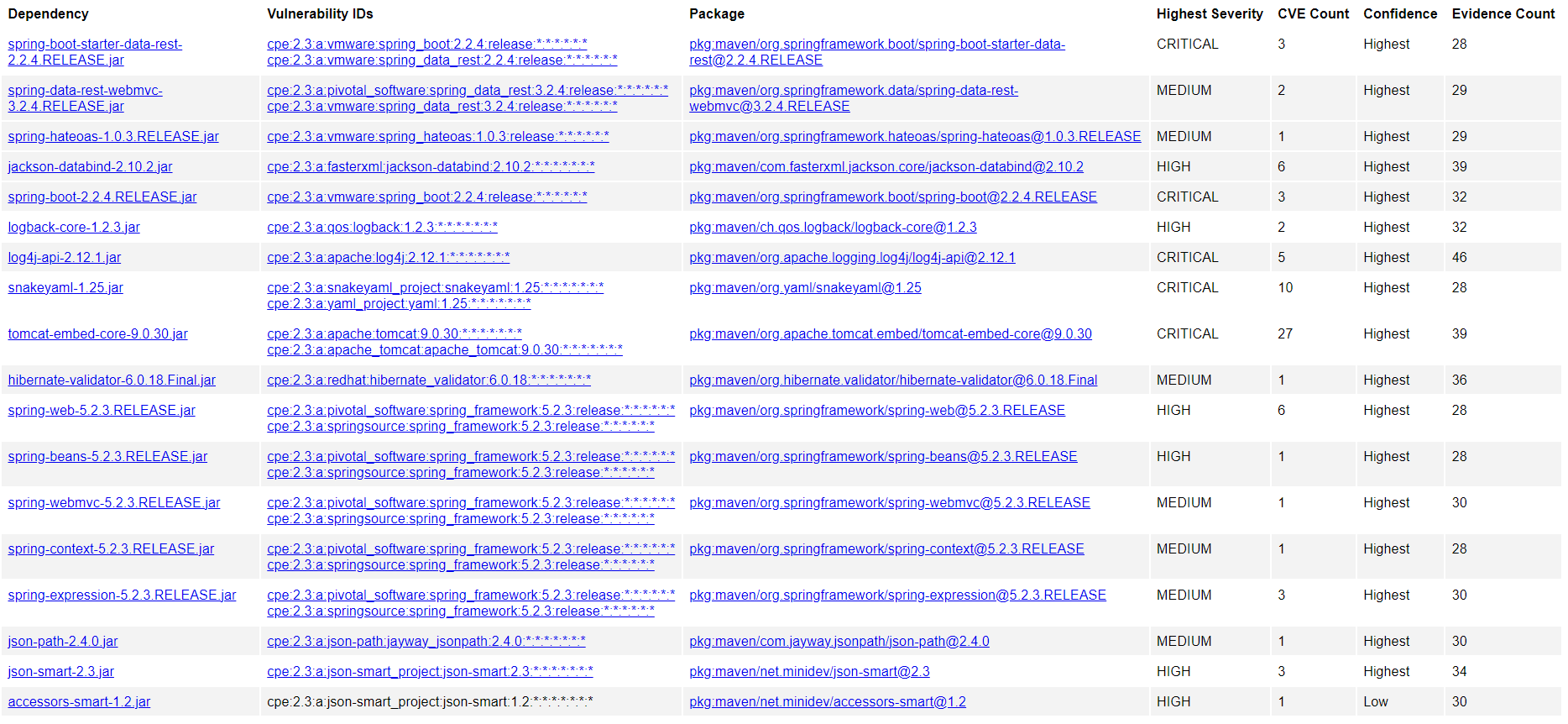
## Secure Communications

Insert a screenshot below of the web browser that shows a secure webpage.



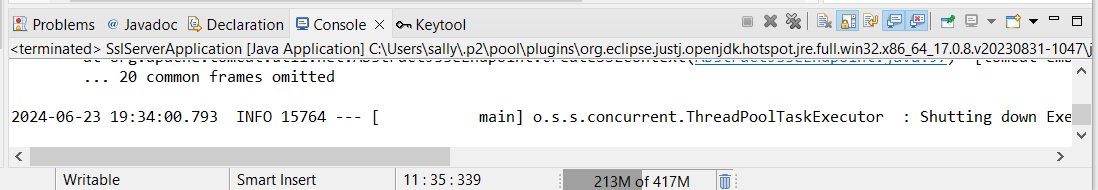
## Secondary Testing

Insert screenshots below of the refactored code executed without errors and the dependency-check report.



## Functional Testing

Insert a screenshot below of the refactored code executed without errors.



## Summary

The code has been refactored and complies with security testing protocols because after running the dependency check I created a new file called suppression.xml and within that file I added 1000 lines of code for suppressing all of the security vulnerabilities. Refactoring the code addresses Cryptography by discovering vulnerabilities, Input validation for secure input and representation, code quality by using secure coding practices and encapsulation by having secure data structures. The application has the security vulnerabilities suppressed and a key certificate.

## Industry Standard Best Practices

I applied industry best practices for secure coding to mitigate known security vulnerabilities by using the maven dependency check for static testing. Applying industry best practices for secure coding is best for the company’s well being because it prevents having security risks in the future which could cause legal and financial loss or problems.

**References**

Java Security Standard Algorithm Names 2017   
<https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names>

Iron-Clad Java: Building Secure Web Applications, Manico, Jim, Detlefsen, August, 2015

Everything You Need to Know About AES-256 Encryption   
<https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/>