****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_prijxwsep8ou)

[**Client 3**](#_hv7yw0j2oy4w)

[**Instructions 3**](#_p5s50lp463jv)

[**Developer 4**](#_bt1bvvcpw5gn)

[**1. Algorithm Cipher 4**](#_mszlfg8i190w)

[**2. Certificate Generation 4**](#_rv1coq41ru3n)

[**3. Deploy Cipher 4**](#_nzhhsy3wigr)

[**4. Secure Communications 4**](#_t1l65wv9fhv0)

[**5. Secondary Testing 4**](#_htr81j31ld3)

[**6. Functional Testing 4**](#_e07729txys0y)

[**7. Summary 4**](#_24i3aia1ao2b)

[**8. Industry Standard Best Practices 4**](#_6ukzhfet1gsc)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **6/20/25** | **Kamirah Pritchard** |  |

## 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

Kamirah Pritchard

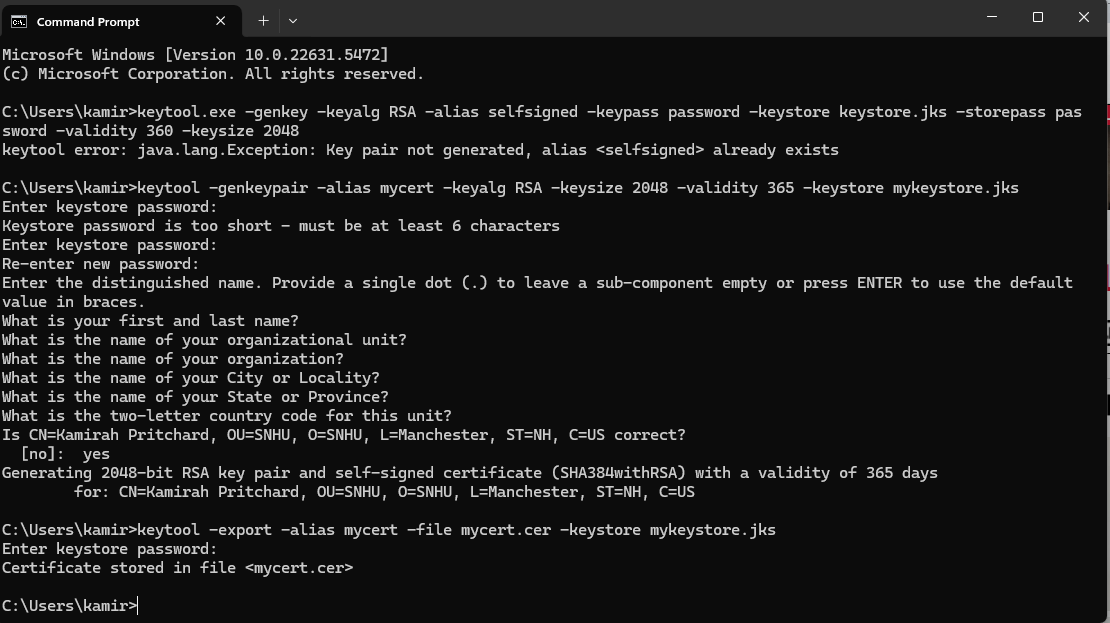
## Algorithm Cipher

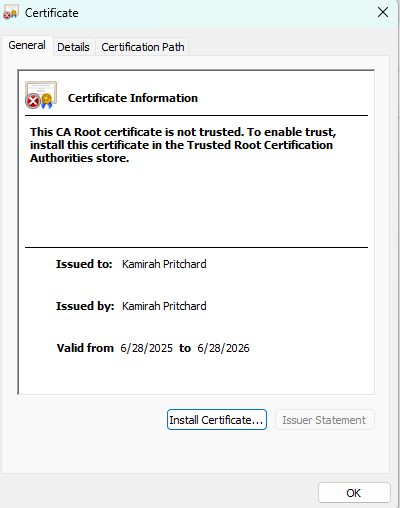
Encryption algorithms have come a long way developing to what we have now. Believe it or not, in ancient civilizations, humans actually always had some method of encrypting data, to break information down into what could be confusing to the public eye. However, with encryption in technology it started with IBM in 1970 where they created something called ‘Crypto Group’ that designed a block cipher to protect customer data. It later became the National Standard, renaming it to the Data Encryption Standard, DES. In 97, DES was cracked which led to the creation of public and private keys. In the 2000s, AES finally replaced DES.

After the summary of what the encryption algorithms are, the algorithm cipher that I would recommend to this company is AES. I recommend the AES (Advanced Encryption Standard) algorithm for best protection regarding encrypting archive files. It doesn’t specify if the archive files will be at rest but if so, data that is at rest needs security that is able to be unwrappable when it needs to be used…which is where encryption comes in. In my opinion, with encryption algorithms AES is the most proficient one. It is Trusted by the US government, and supports key sizes of 128, 192, and 256 bit sizes. This is very important because it gives clients flexibility for different security purposes and has a high speed processing to quickly encrypt data safely. Regarding attacks, AES is brute force resistant. With algorithm ciphers, Hash functions are extremely important to software security because it prevents collisions. They are cryptographic algorithms that take a sequence of large numbers or strings and computes them into small integer values. In addition, the use of symmetric and asymmetric keys are also important to mention. Symmetric keys are used in AES (or Encryption algorithms) this is when there is a secret key that is used to scramble private information that is impossible to reveal unless you have that specific key. With symmetric keys there is only one is used for the encrypting and decrypting. While Asymmetric keys there is one key that is a private key and kept secret and the public key is made available to anyone. However, there is no way to derive the private key from the public one.

## Certificate Generation

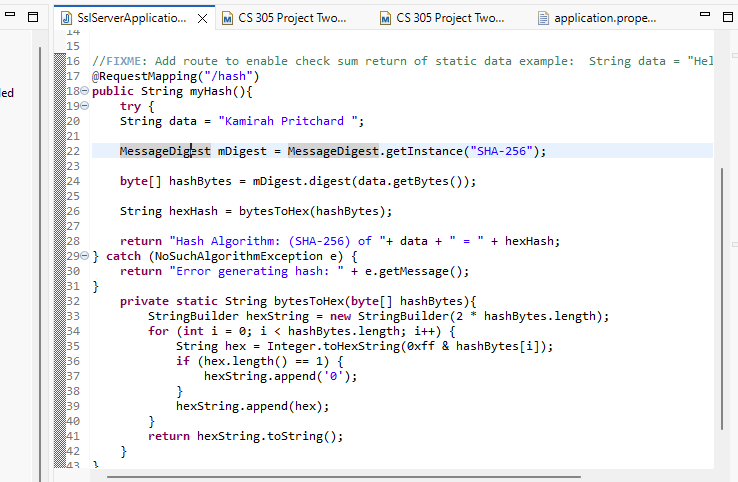
Insert a screenshot below of the CER file.





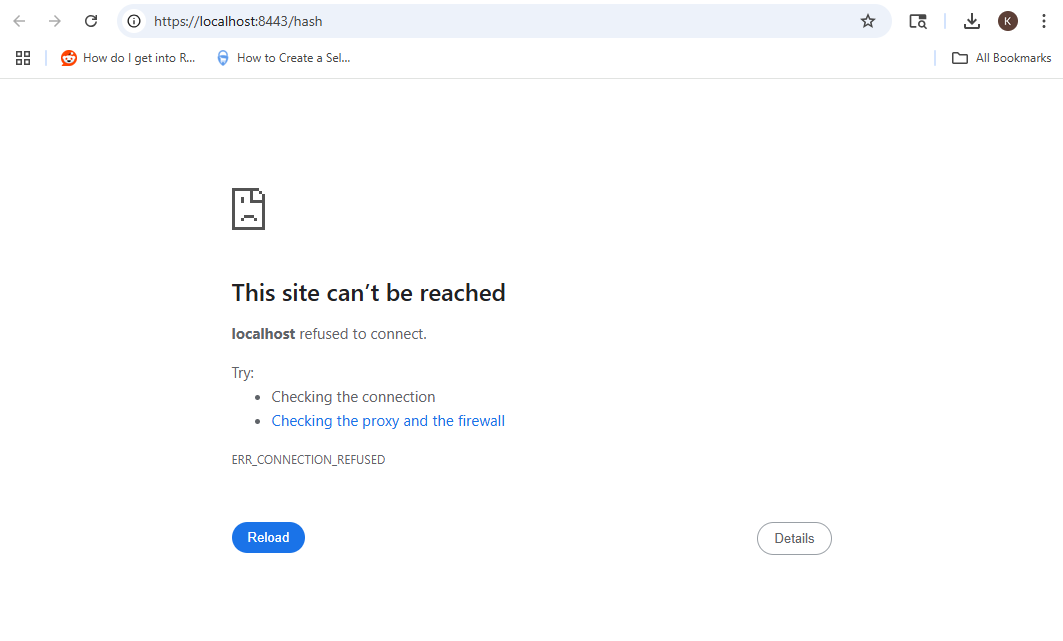
## Deploy Cipher

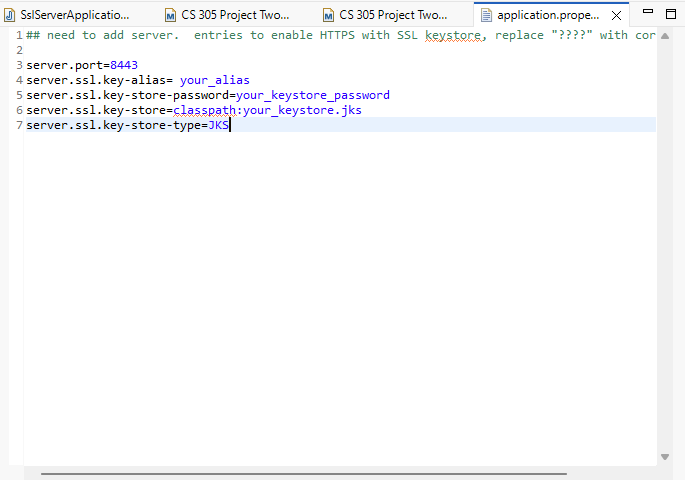
Insert a screenshot below of the checksum verification.



## Secure Communications

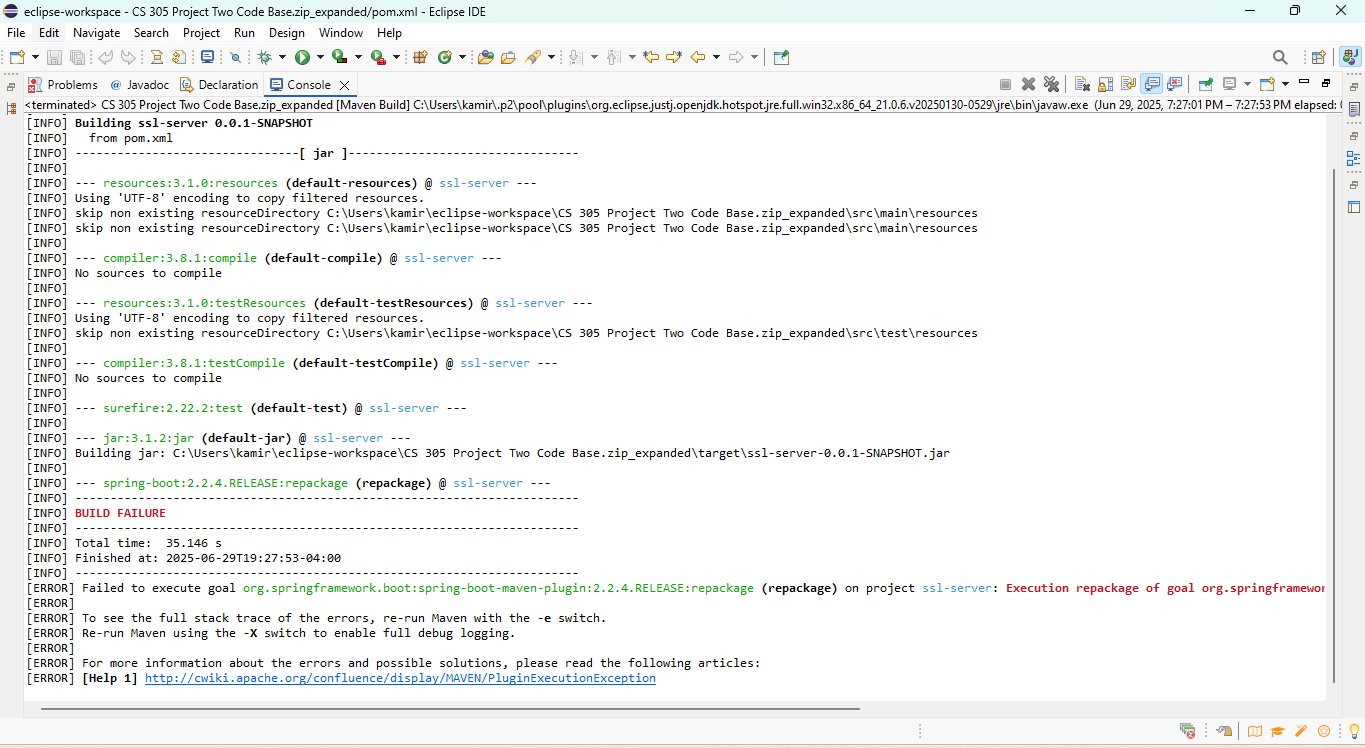
Insert a screenshot below of the web browser that shows a secure webpage.





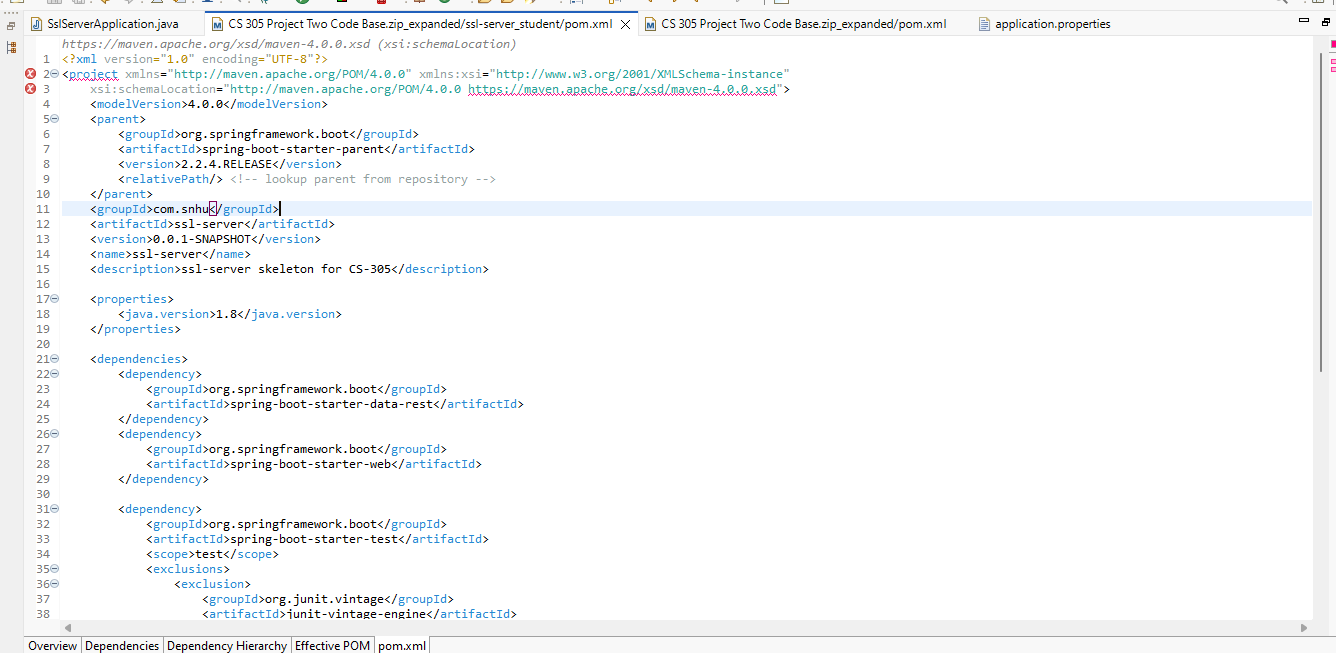
## Secondary Testing

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

Looking at the vulnerability assessment, we addressed Input Validation by using the certification and asking for a password . In addition, securing APIs and data protection by using Encryption with validating the HTTPS request and also we addressed the secure distributed companies with the self signed certification that would be able to secure information from sender to receiver.

## Industry Standard Best Practices

Industry Standard Best Practices that I have implemented in this project are Vulnerability scanning which we used the Maven dependency check to determine if there were any new vulnerabilities. In addition, Authentication and Authorization was implemented by using the JDK signing certification.