****

# 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** | **10/15/2023** | **Nadia Baamrani** |  |

## 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

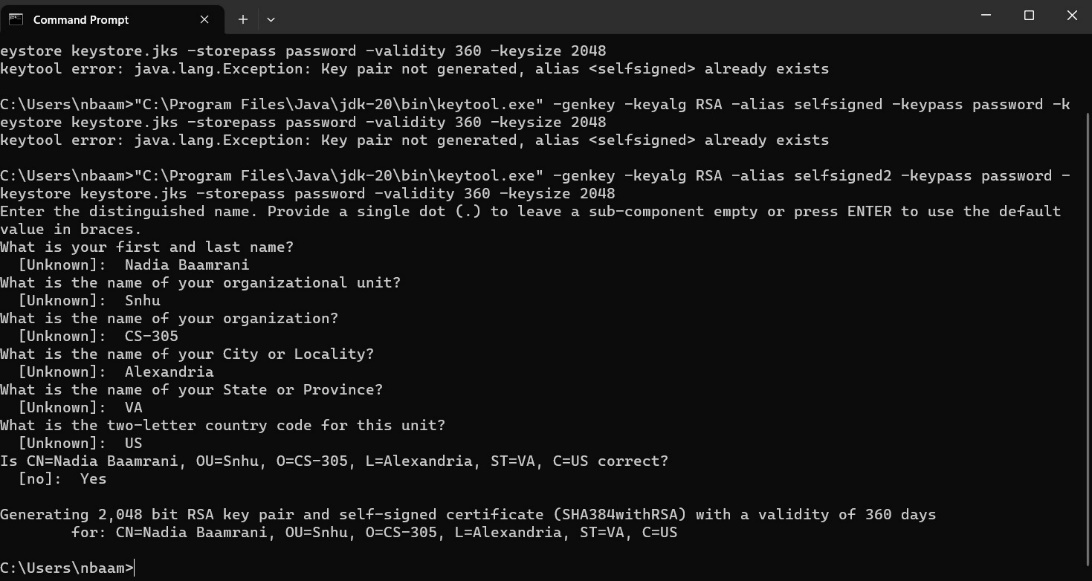
Nadia Baamrani

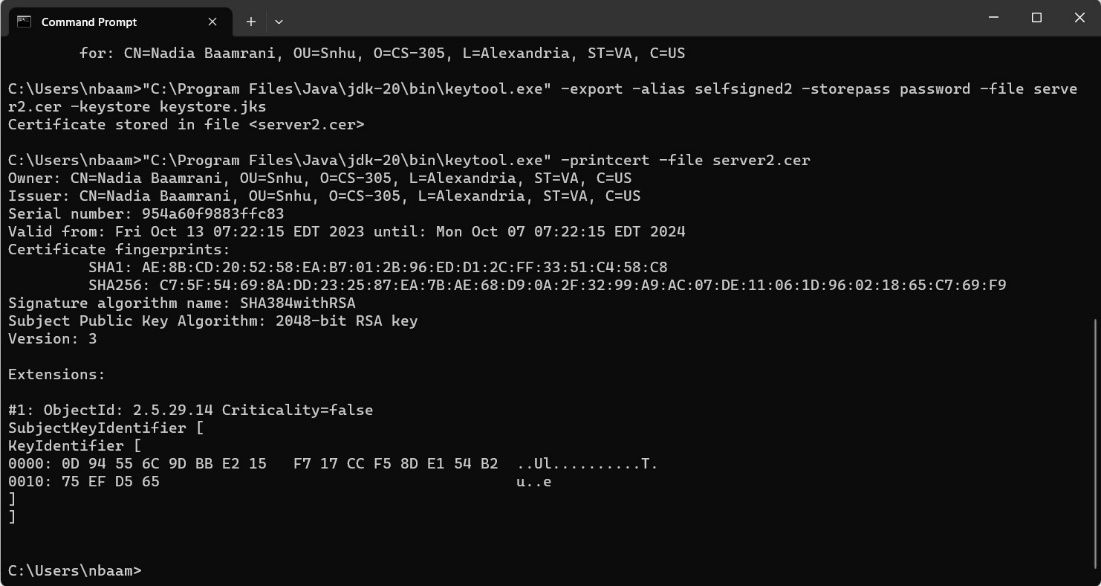
## Algorithm Cipher

For securing communications and ensuring data integrity, we can use the SHA-256 hashing algorithm as the encryption algorithm cipher. SHA-256 is widely used for generating checksums and ensuring data integrity. It produces a 256-bit (32-byte) hash value, which is considered secure.SHA-256 is a symmetric cryptographic algorithm, meaning it uses the same key (algorithm) for both hashing and verification. It does not involve random numbers or asymmetric keys.

Certificate Generation

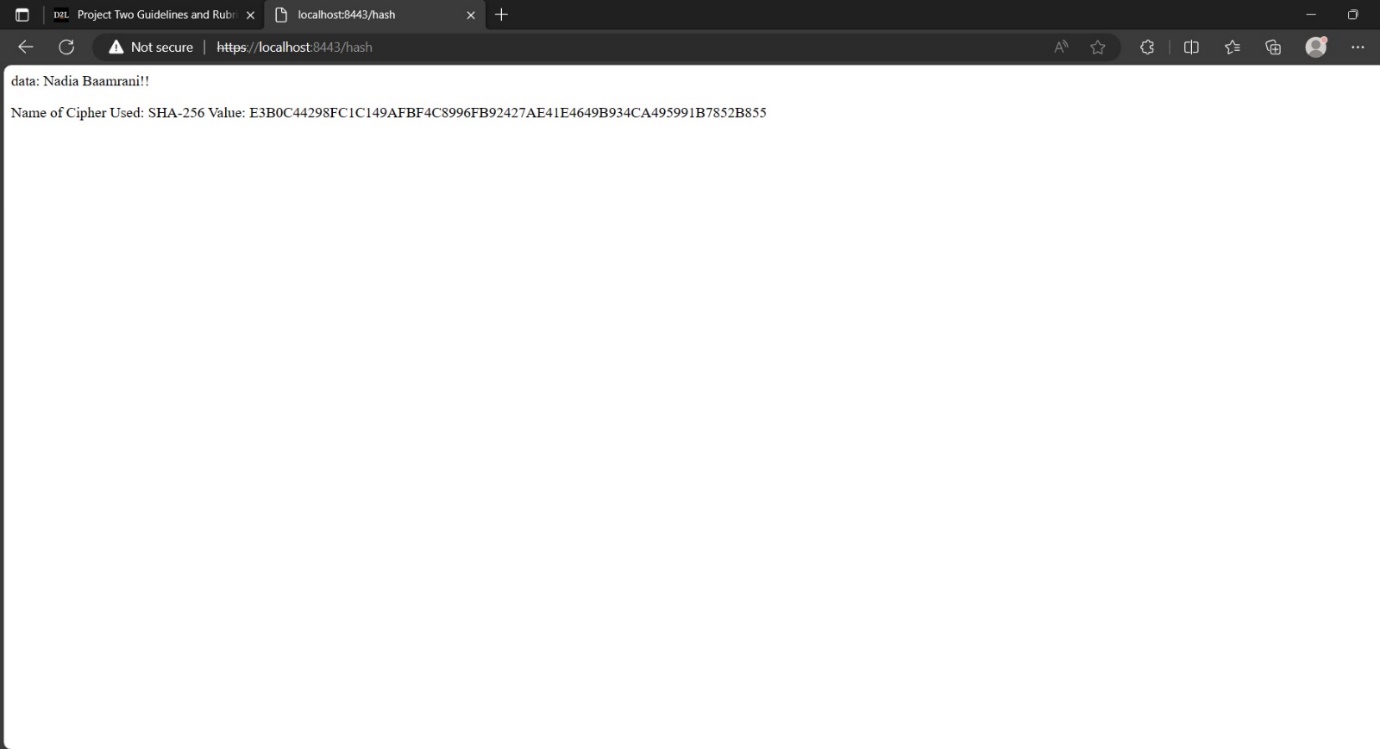
Insert a screenshot below of the CER file.





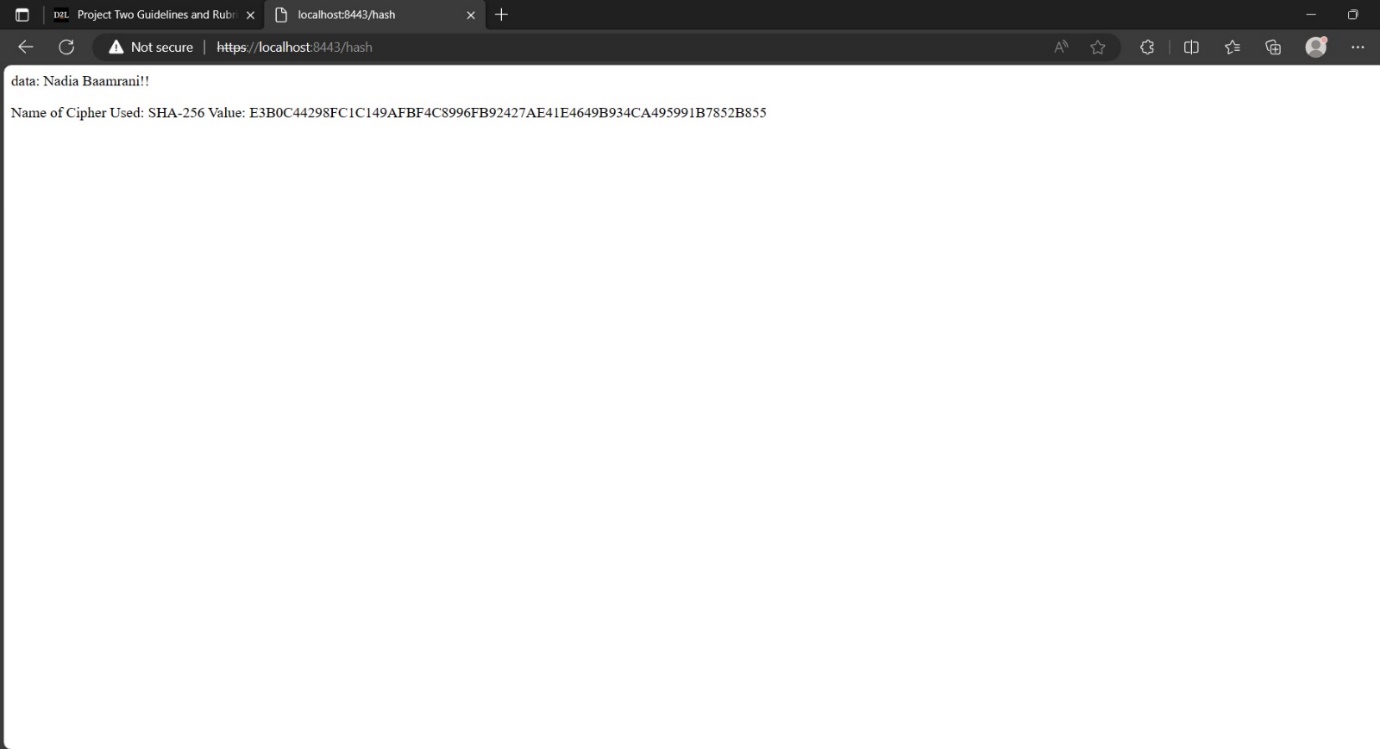
## Deploy Cipher

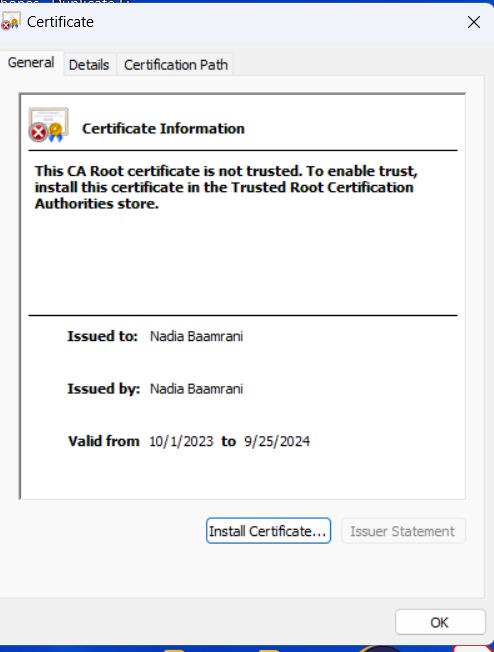
Insert a screenshot below of the checksum verification.



## Secure Communications

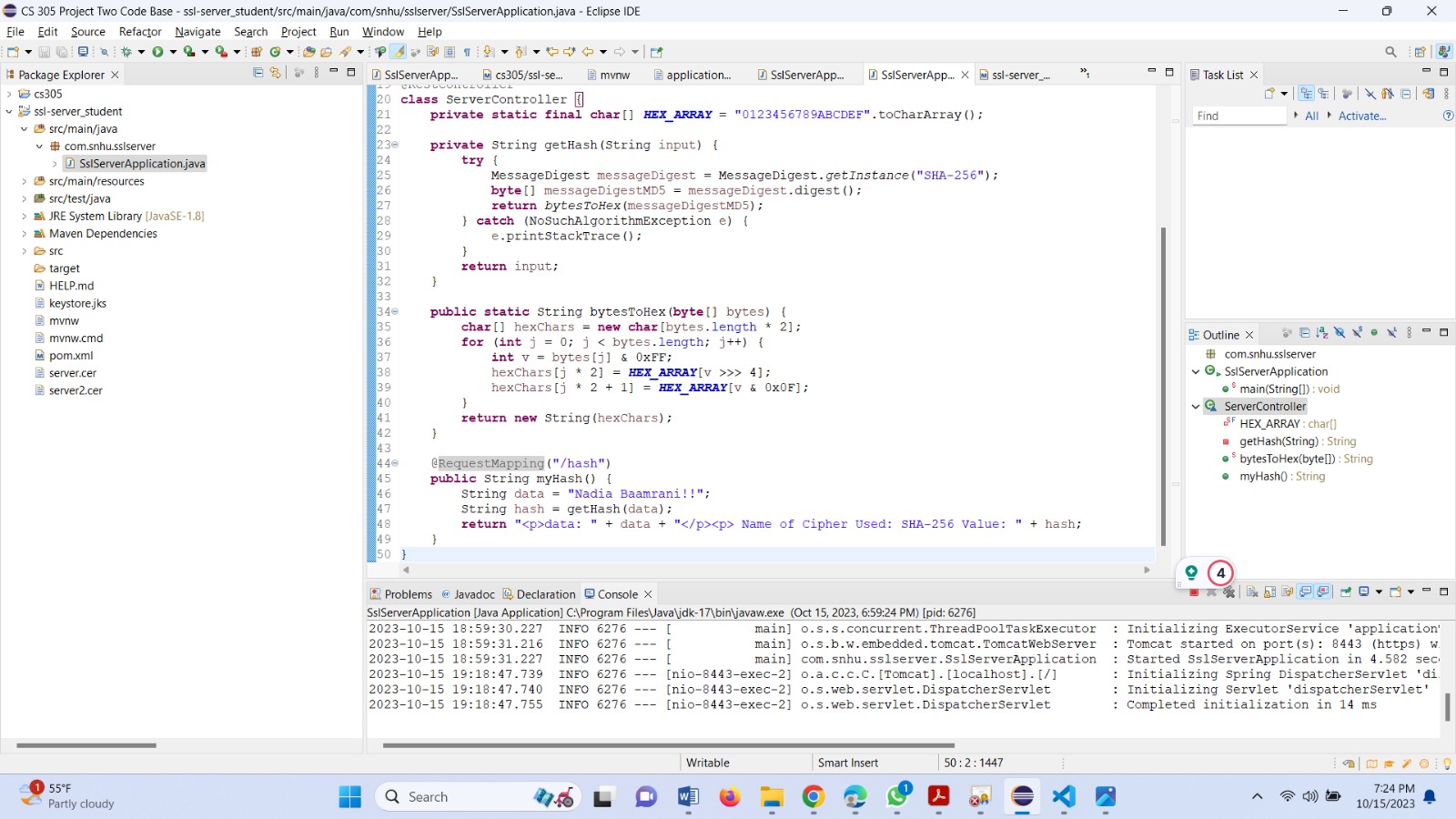
Insert a screenshot below of the web browser that shows a secure webpage.

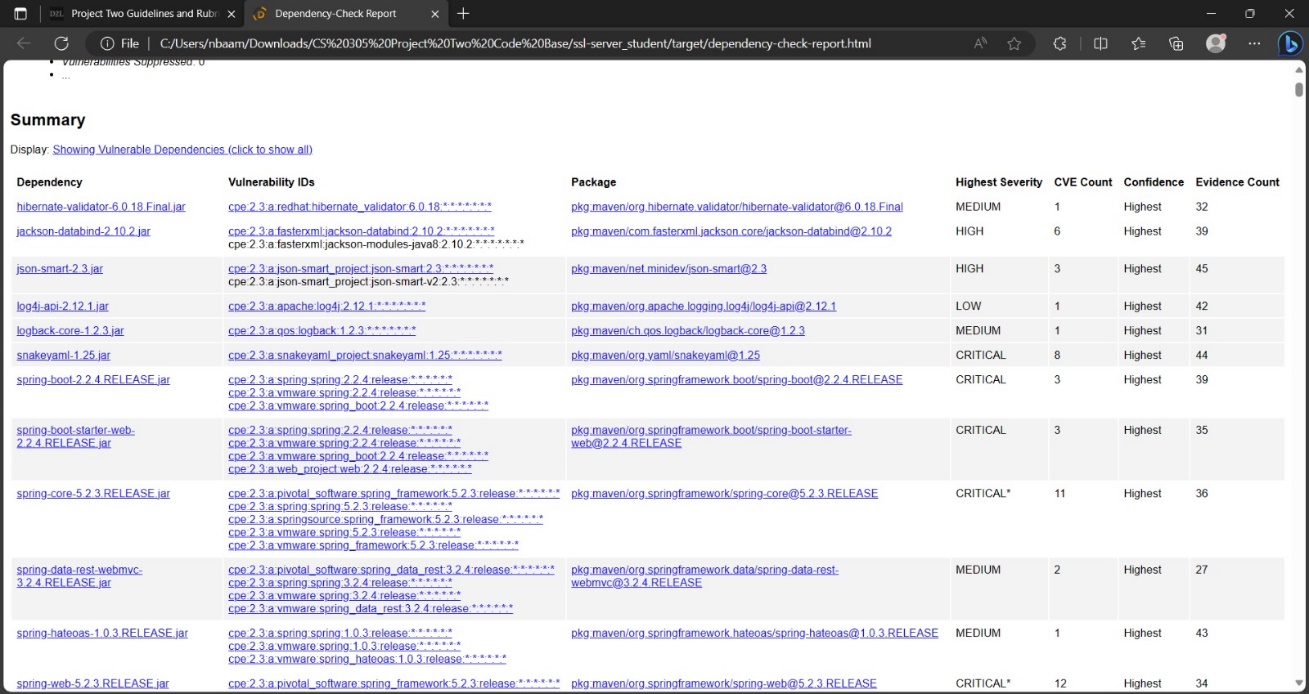


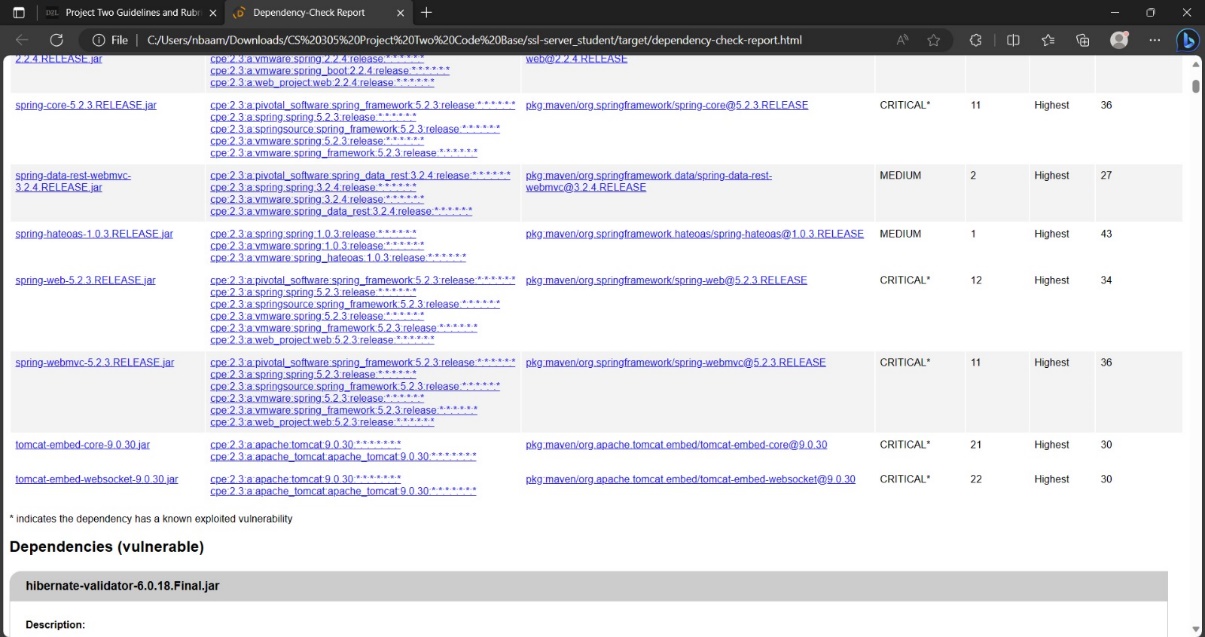


## Secondary Testing

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.

