****

# 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** | **4/20/24** | **James Melancon** |  |

## 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

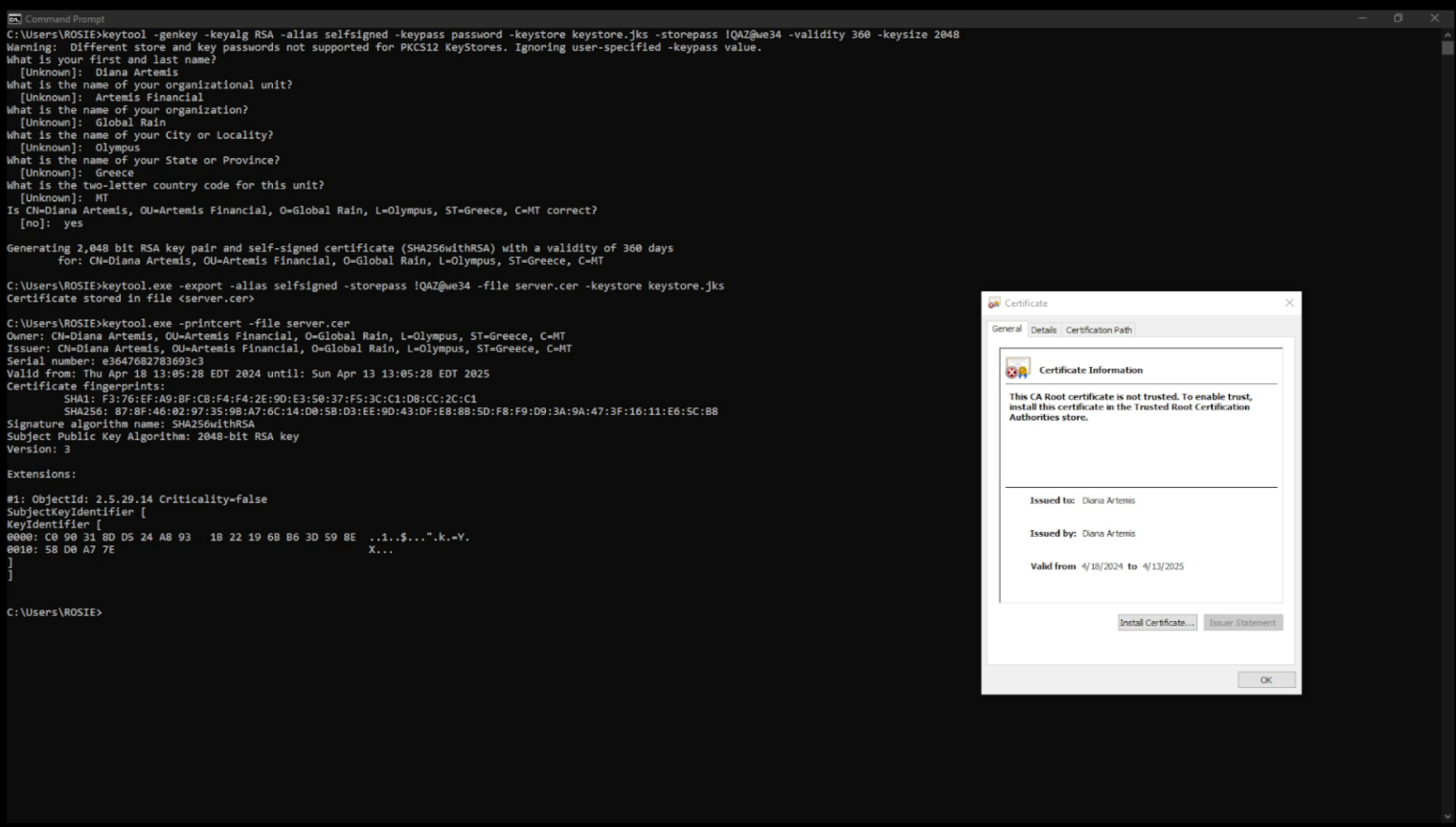
James Melancon

## Algorithm Cipher

My previous submission for the topic of Ciphers advocated on behalf of AES, but for this assignment, I decided it would be best to use SHA-256. It is just about as renowned for its strength and reliability in securing sensitive data. It generates a fixed-size hash value of 256 bits, making it ‘computationally infeasible’ to reverse-engineer the original input message from the hash. This property ensures both data integrity and authenticity, crucial for financial applications.

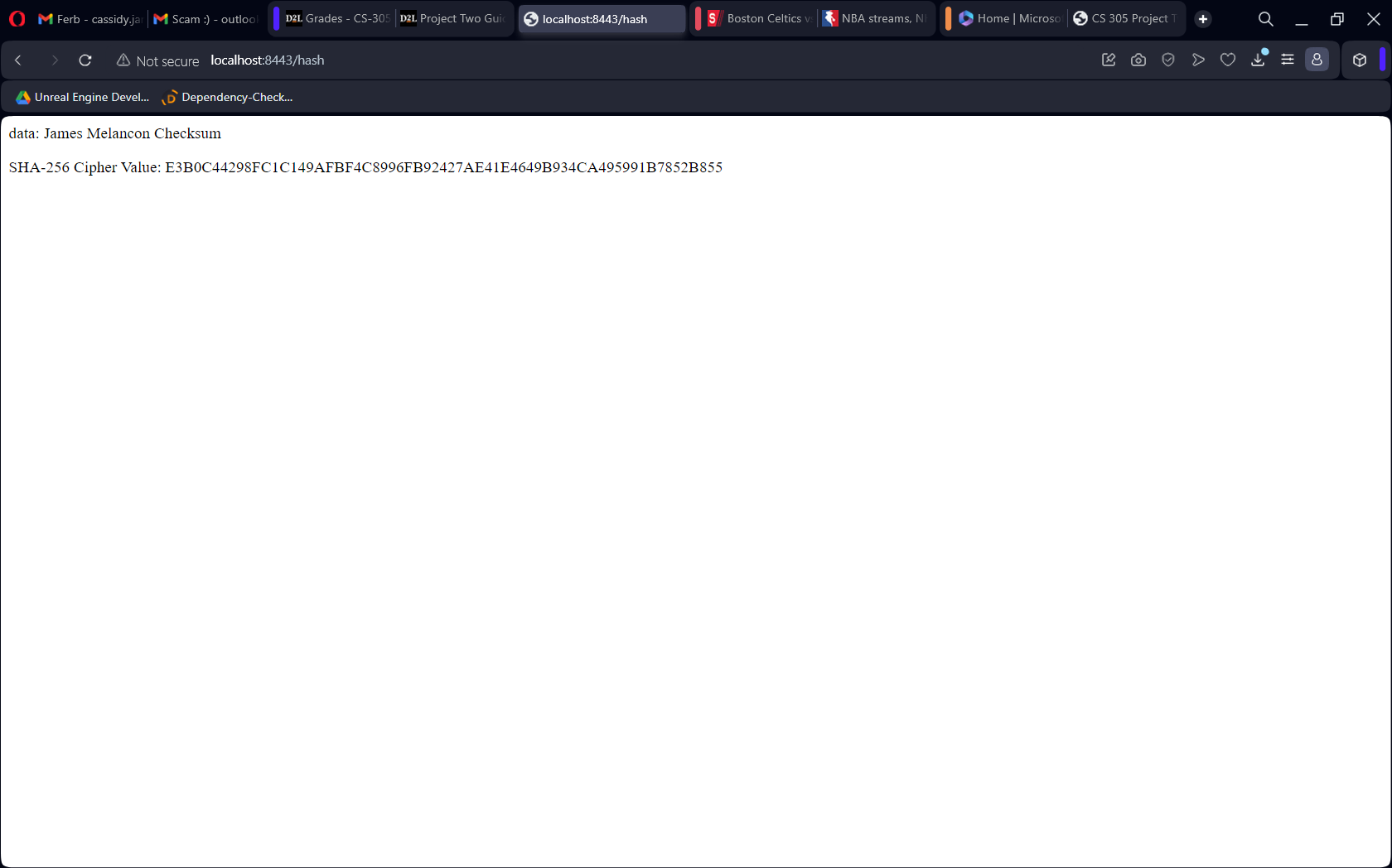
Unlike symmetric or asymmetric encryption algorithms (like AES), SHA-256 does not involve using keys for encryption or decryption. Instead focusing almost solely on generating a hash value for data verification/authentication. Perfect for checksum generation. It is NIST standardized, and its widespread use in finance and government help lend to its credibility.

## Certificate Generation



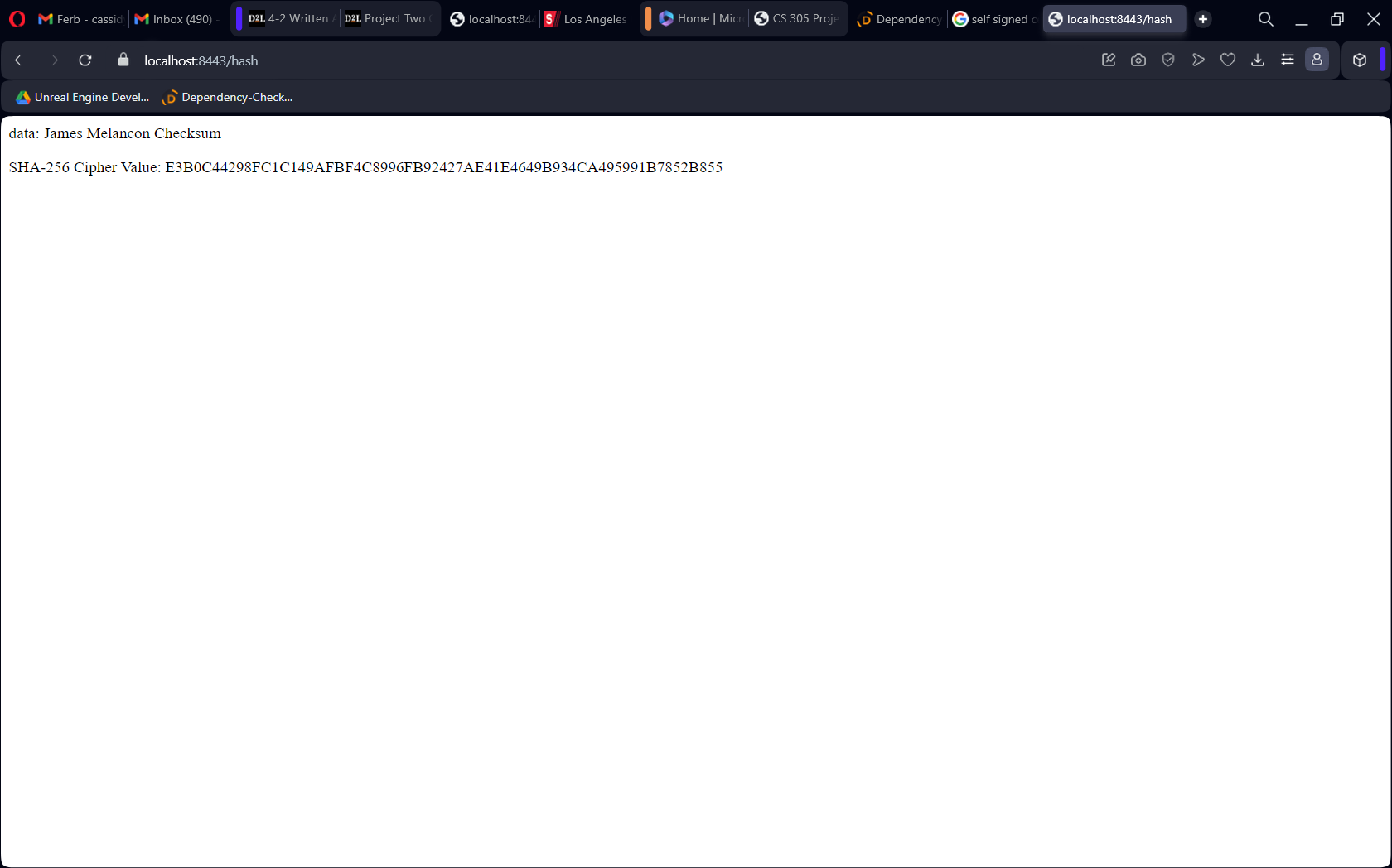
## Deploy Cipher

Insert a screenshot below of the checksum verification.



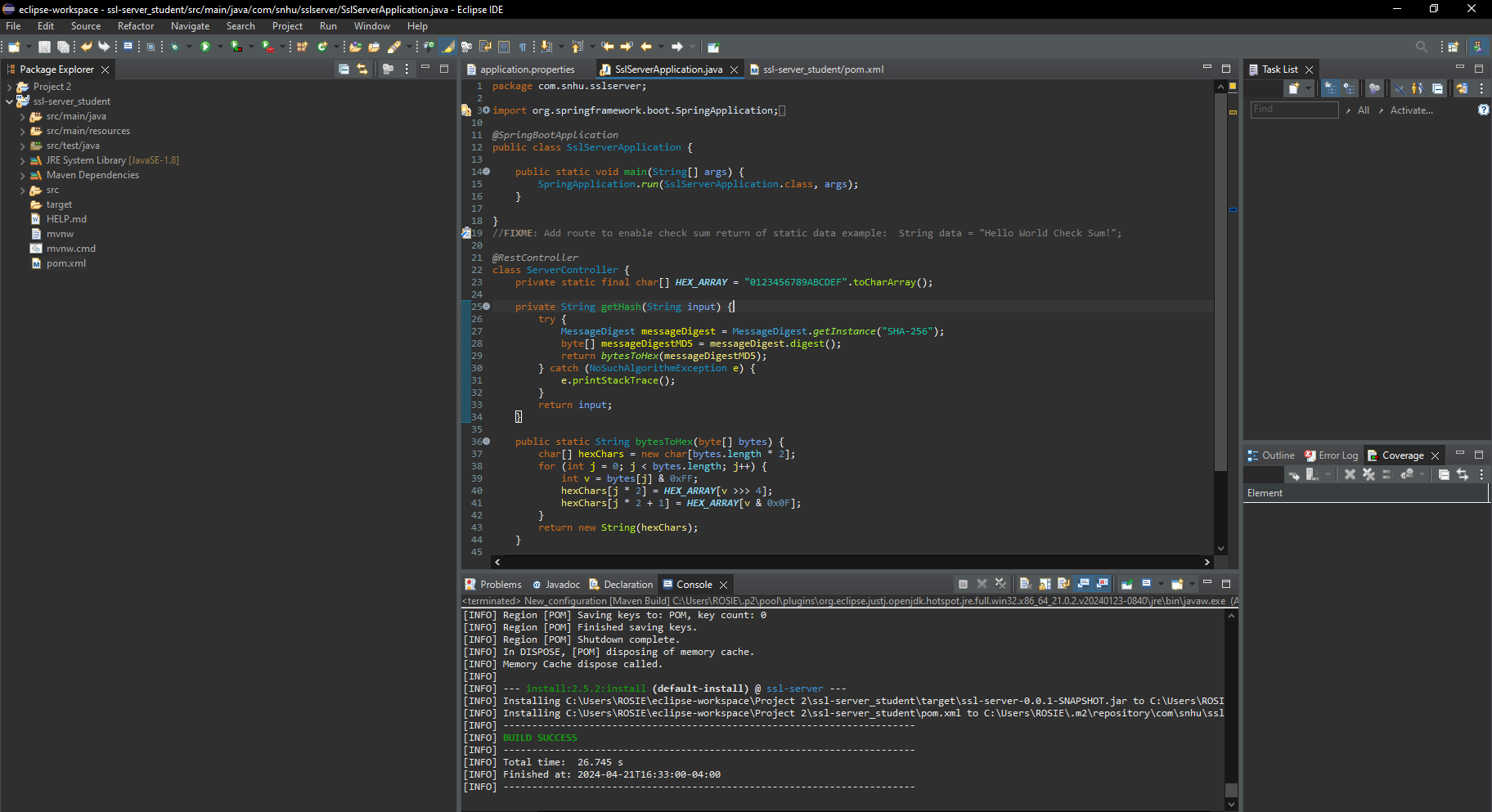
## Secure Communications

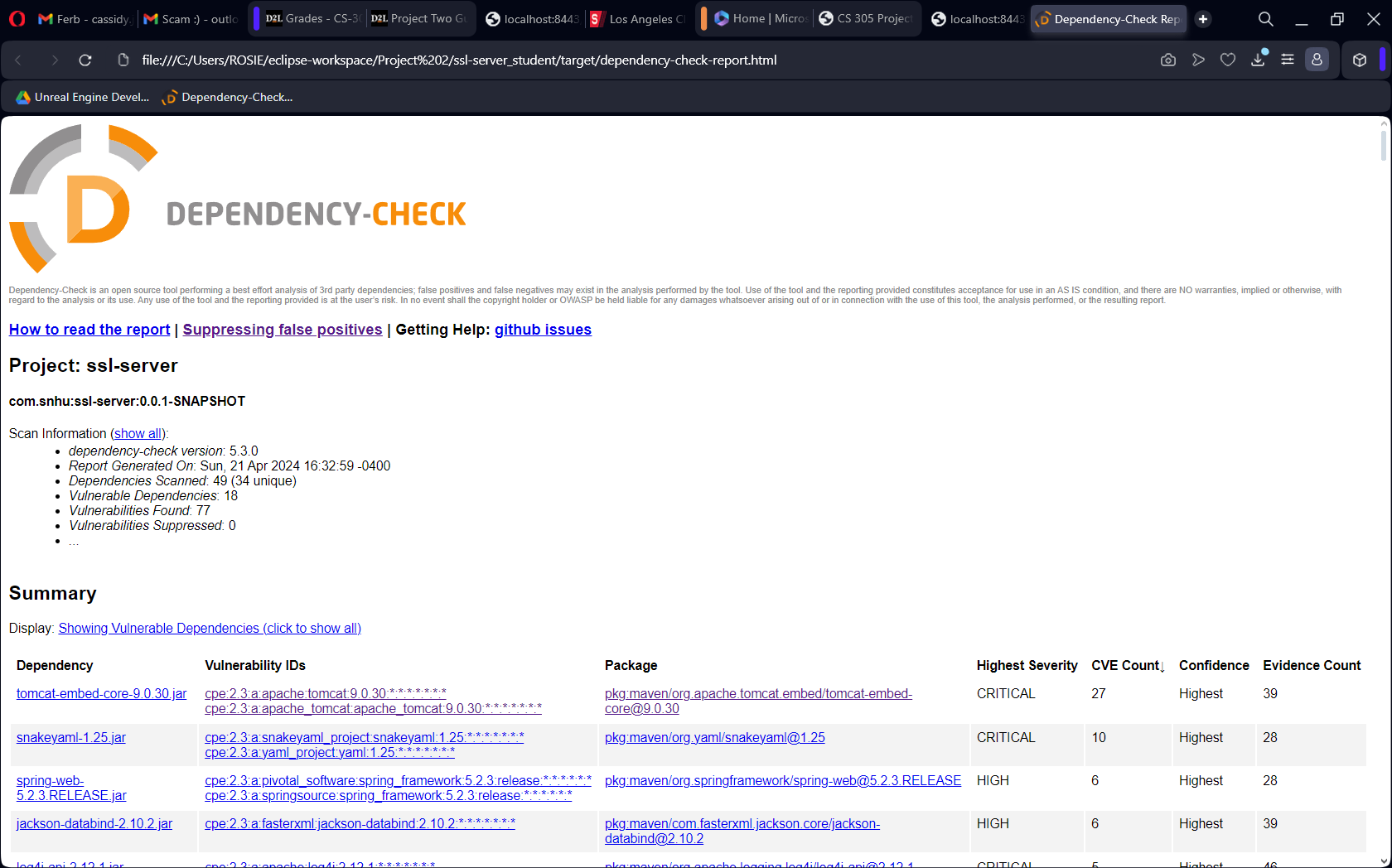
Insert a screenshot below of the web browser that shows a secure webpage.



## Secondary Testing

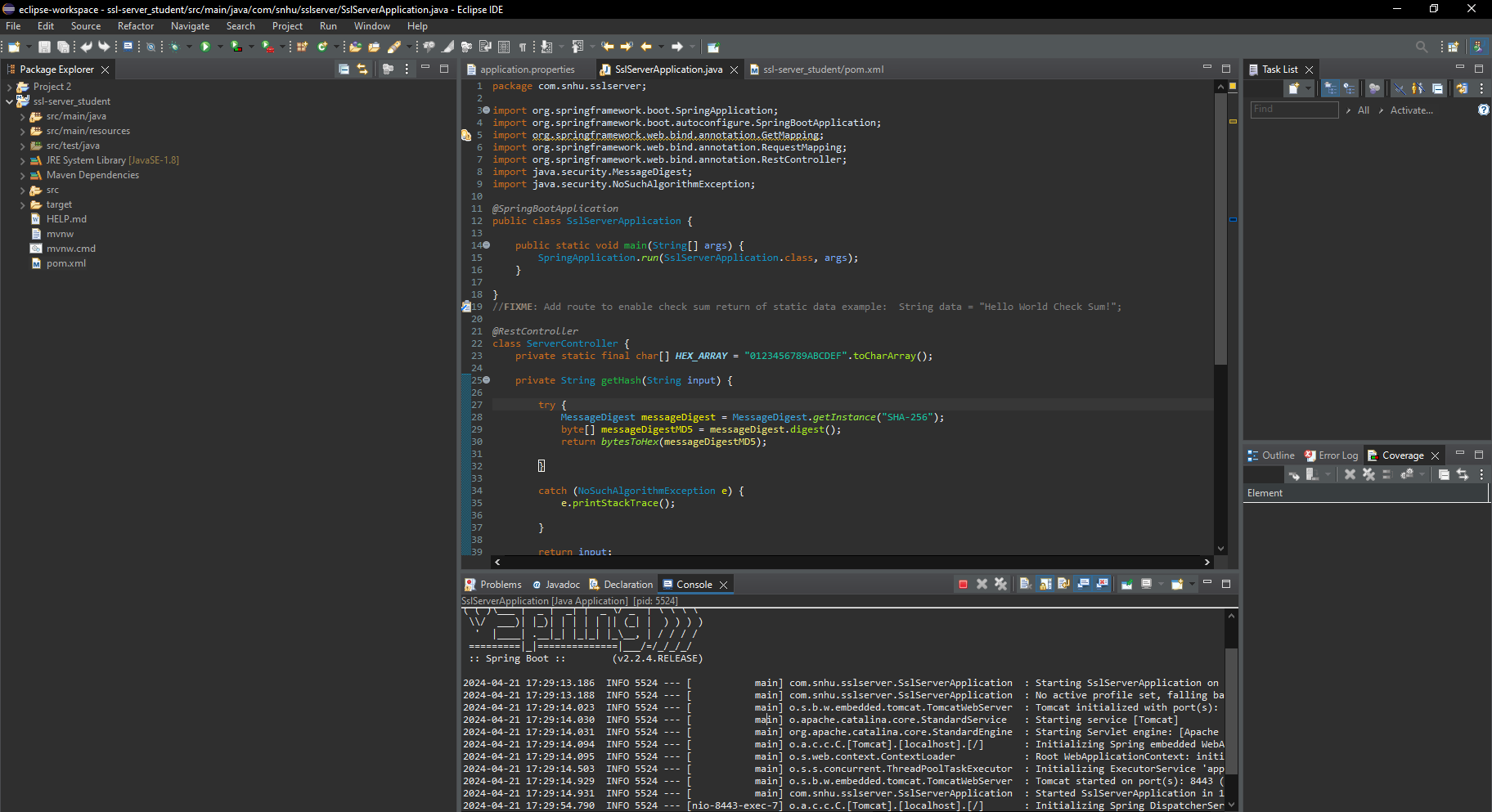
Insert screenshots below of the refactored code executed without errors and the dependency-check report.





## Functional Testing

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



## Summary

After the Architecture was Reviewed, several security measures were taken. The first of which was an introduction of a Cryptograph hash function(SHA-256), which allowed for checksums to be generated, as well as help establish secure communications to and from clients and servers. Client/Server Security is then addressed specifically by that communication then being secured via self-signed certification and conversion of HTTP to the HTTPS protocol. Secondary static testing of the code occurs, using Dependency Check Maven to ensure software security standards are met. Functional testing finalizes the Code Quality with a manual review. Any syntactical, logical, or security vulnerability is addressed. A production quality integrated application that includes secure coding protocols is delivered.

## Industry Standard Best Practices

For the benefit of Artemis Financial, meeting the industry standard displays both a professional security posture and brand. Besides the appearances, actually maintaining competent security standards and meeting regulations lend to enhancements in the overall production of the company. Security exists in software to ensure that things run as smoothly and efficiently as they are designed to do. A good system in place will mitigate security risks and can proactively prevent ill intending files and users from compromising the integrity of either Artemis Financial’s data or reputation.