****

# 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** | **[10/24/24]** | **Brandon Bond** |  |

## 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

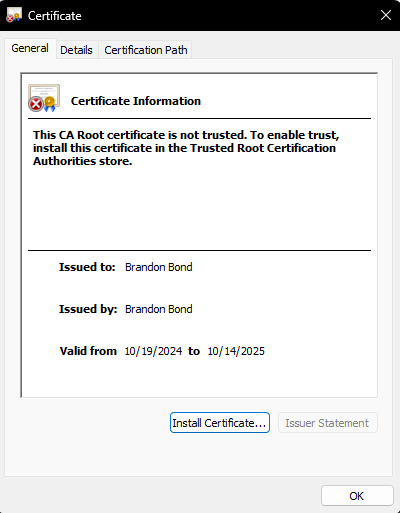
Brandon Bond

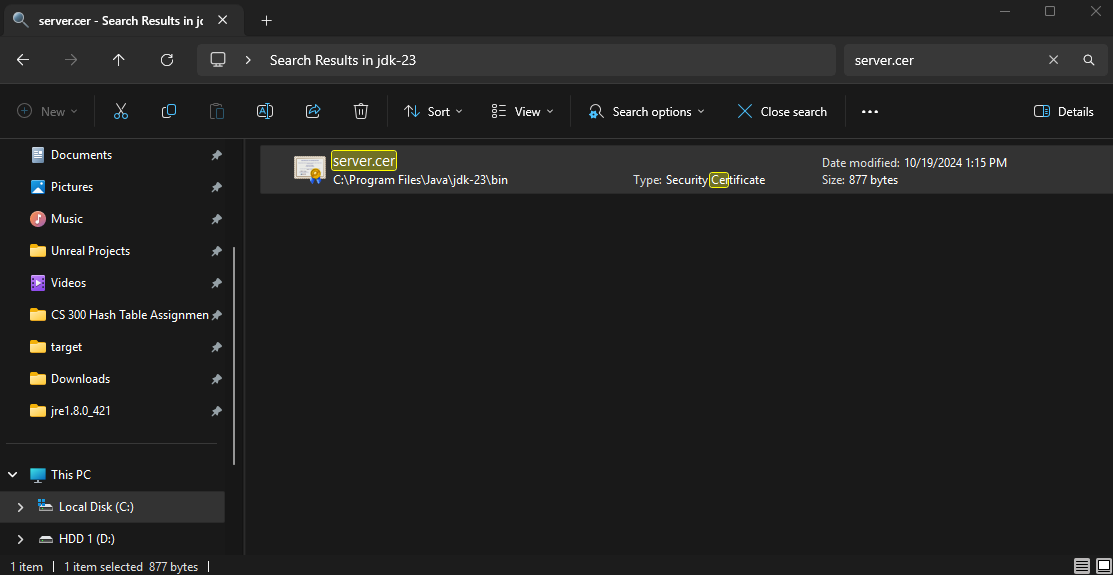
## Algorithm Cipher

For the use that Artemis Financial is looking for in a cipher I would suggest for them to use AES or Advanced Encryption Standard algorithm cipher. This is a good cipher for long-term archive file encryption and is known as a good algorithm. AES operates with a 128-bit encryption while supporting bit keys of 128, 192, and 256 bits, the higher number bits the stronger the encryption is. Random numbers in AES are used to generate keys and to initialize vectors so the encryption is unique. AES was created from its predecessor DES or Data Encryption Standard. DES was well known for being safe but people were starting to crack it, the first time was in 1997, today DES could be cracked within 5 minutes. After this AES was created and is currently being used in the government.

## Certificate Generation

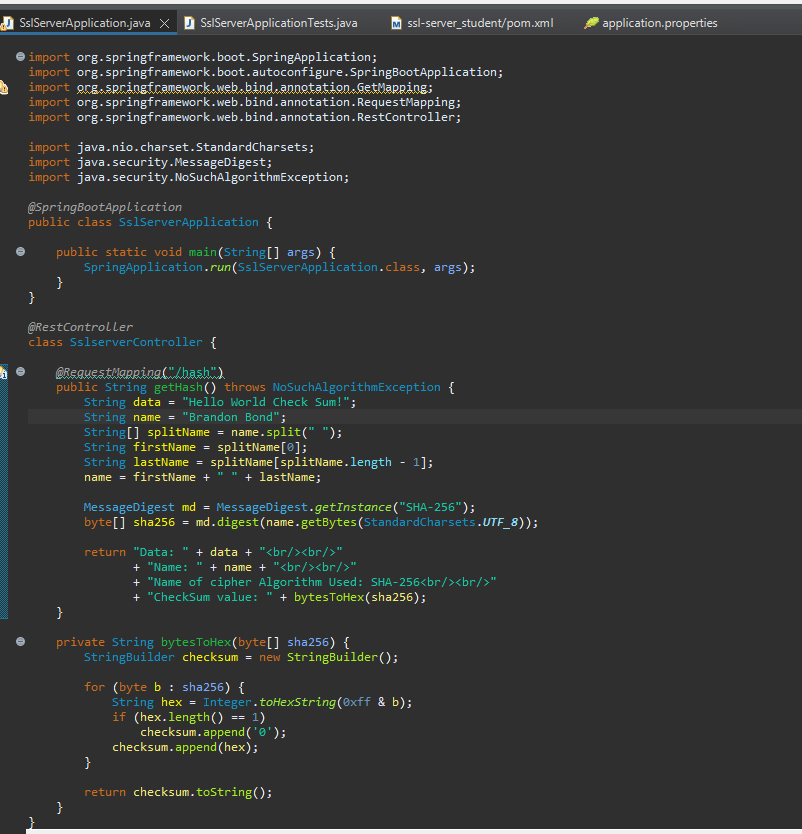
Insert a screenshot below of the CER file.





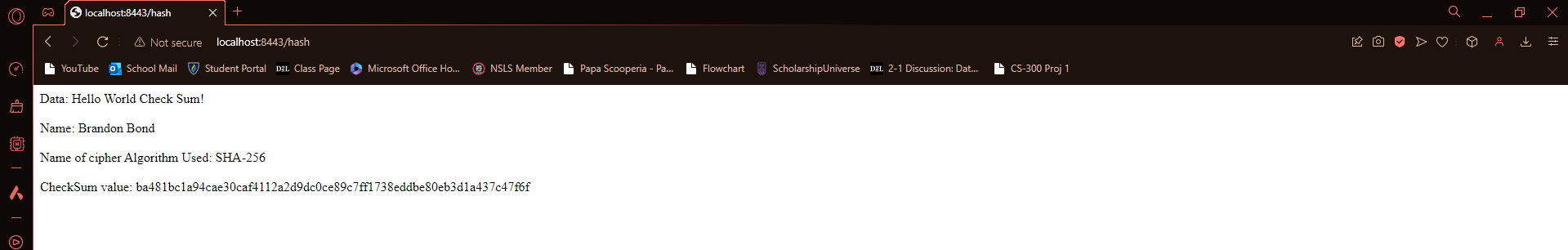
## Deploy Cipher

Insert a screenshot below of the checksum verification.



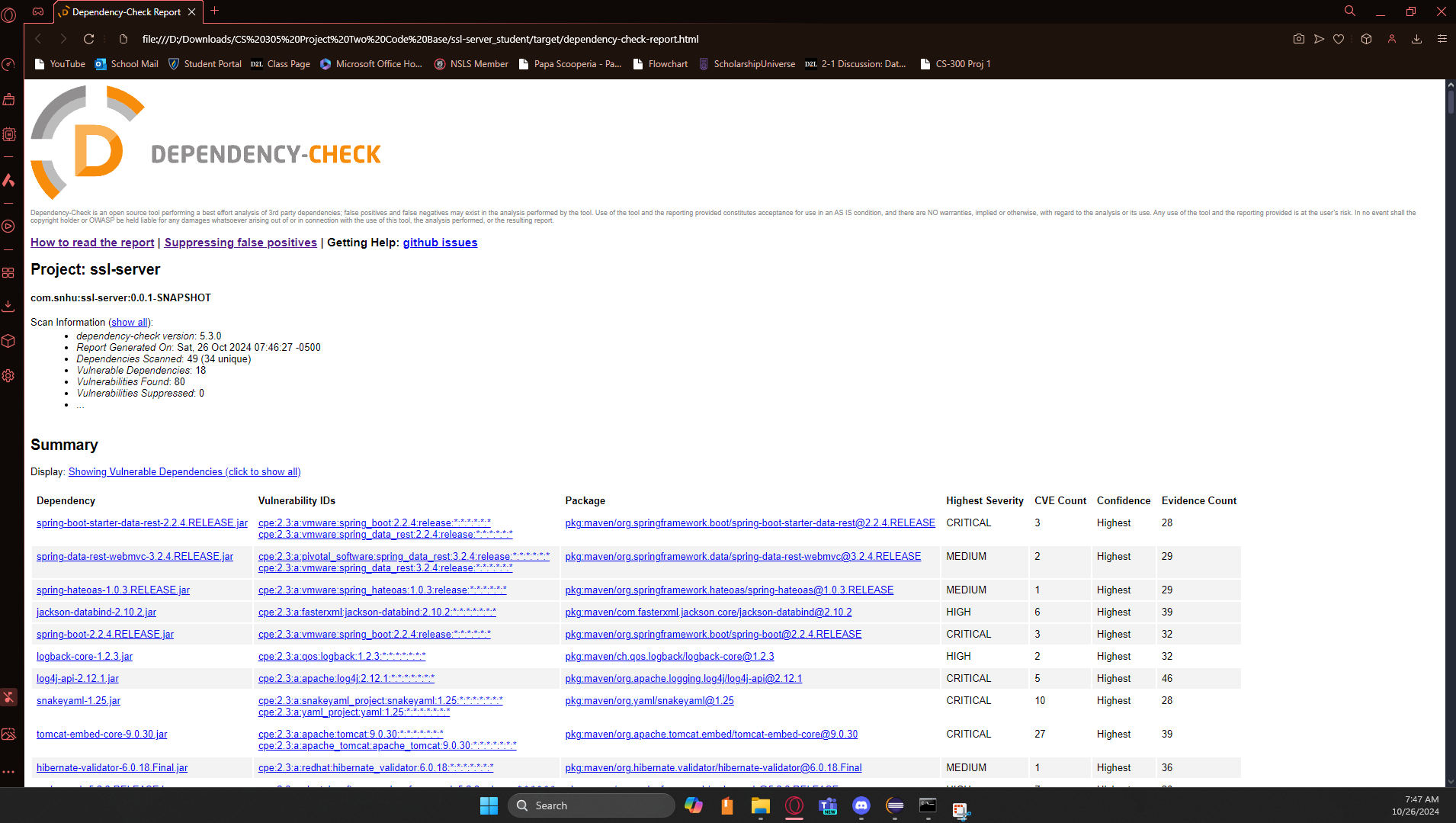
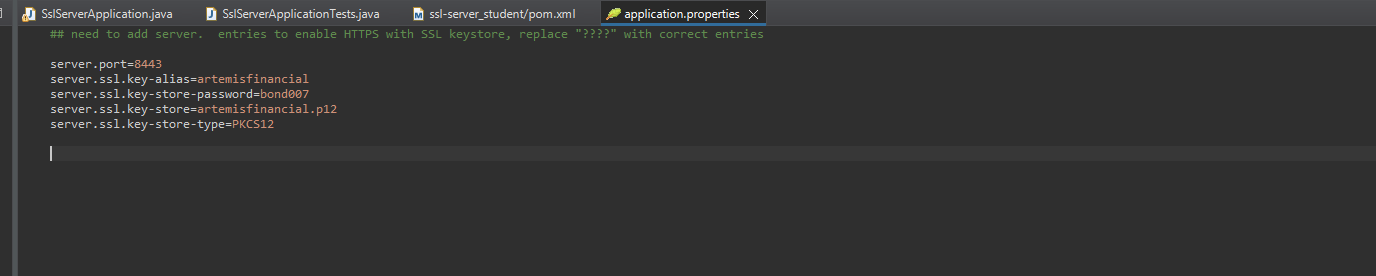
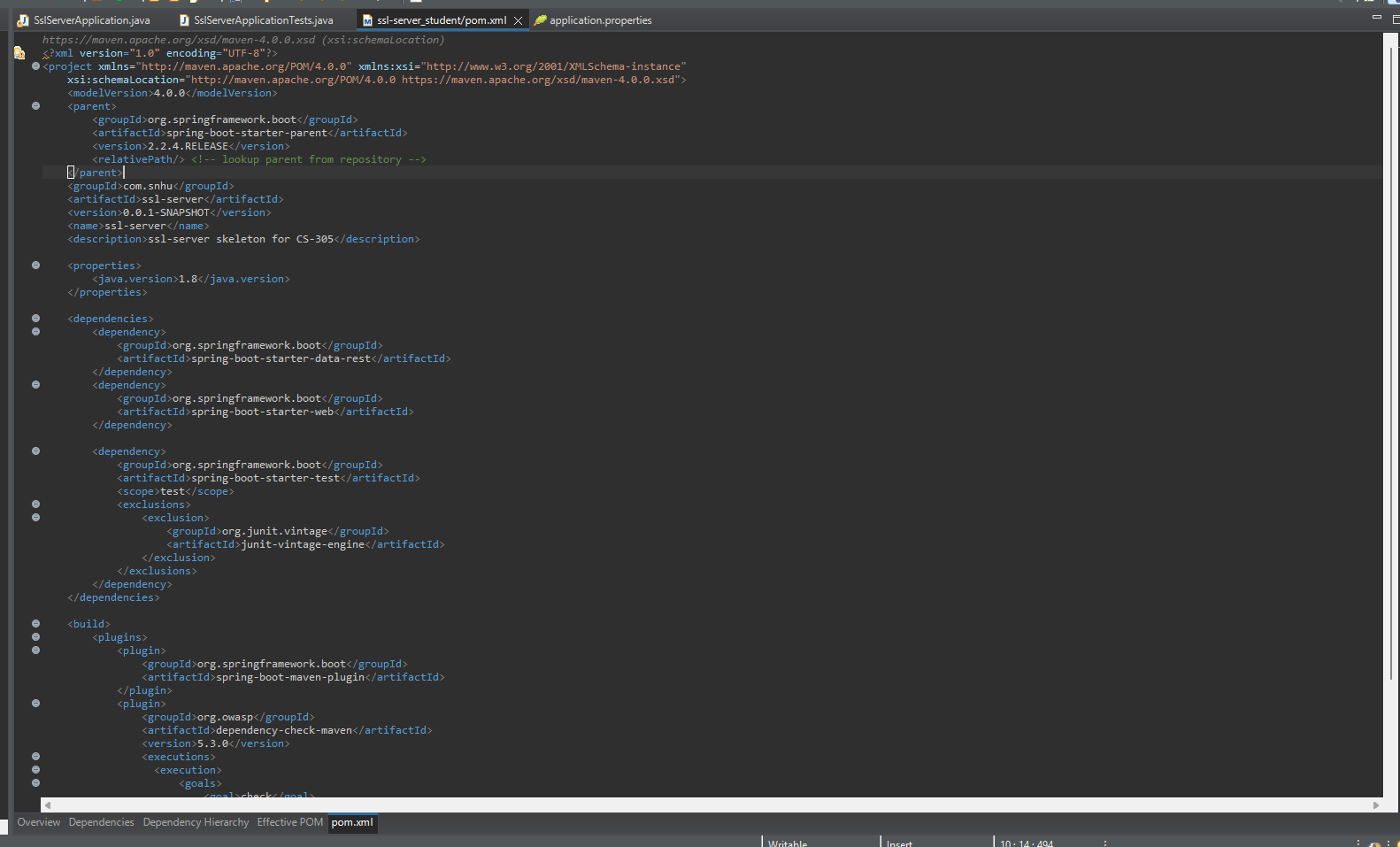
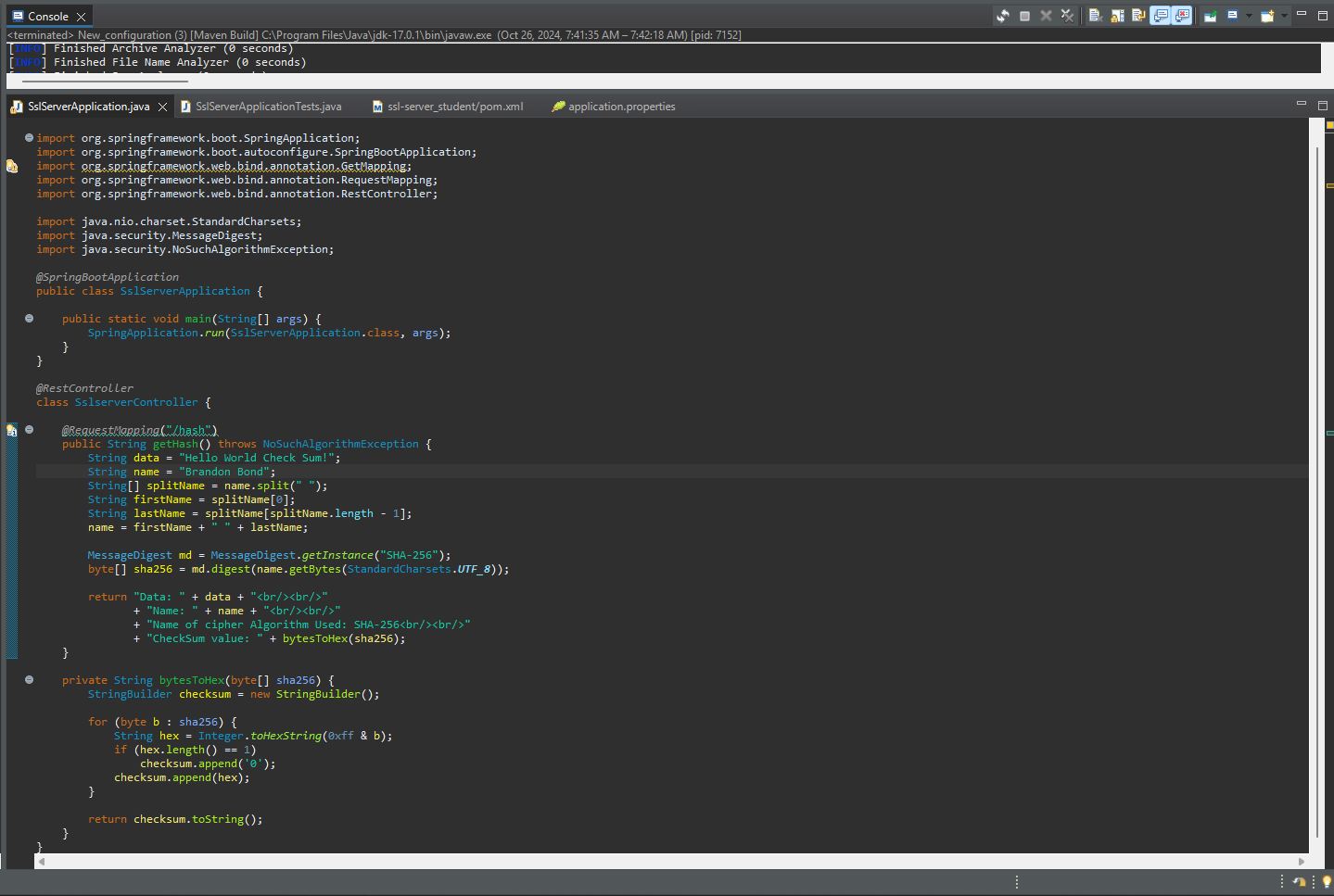
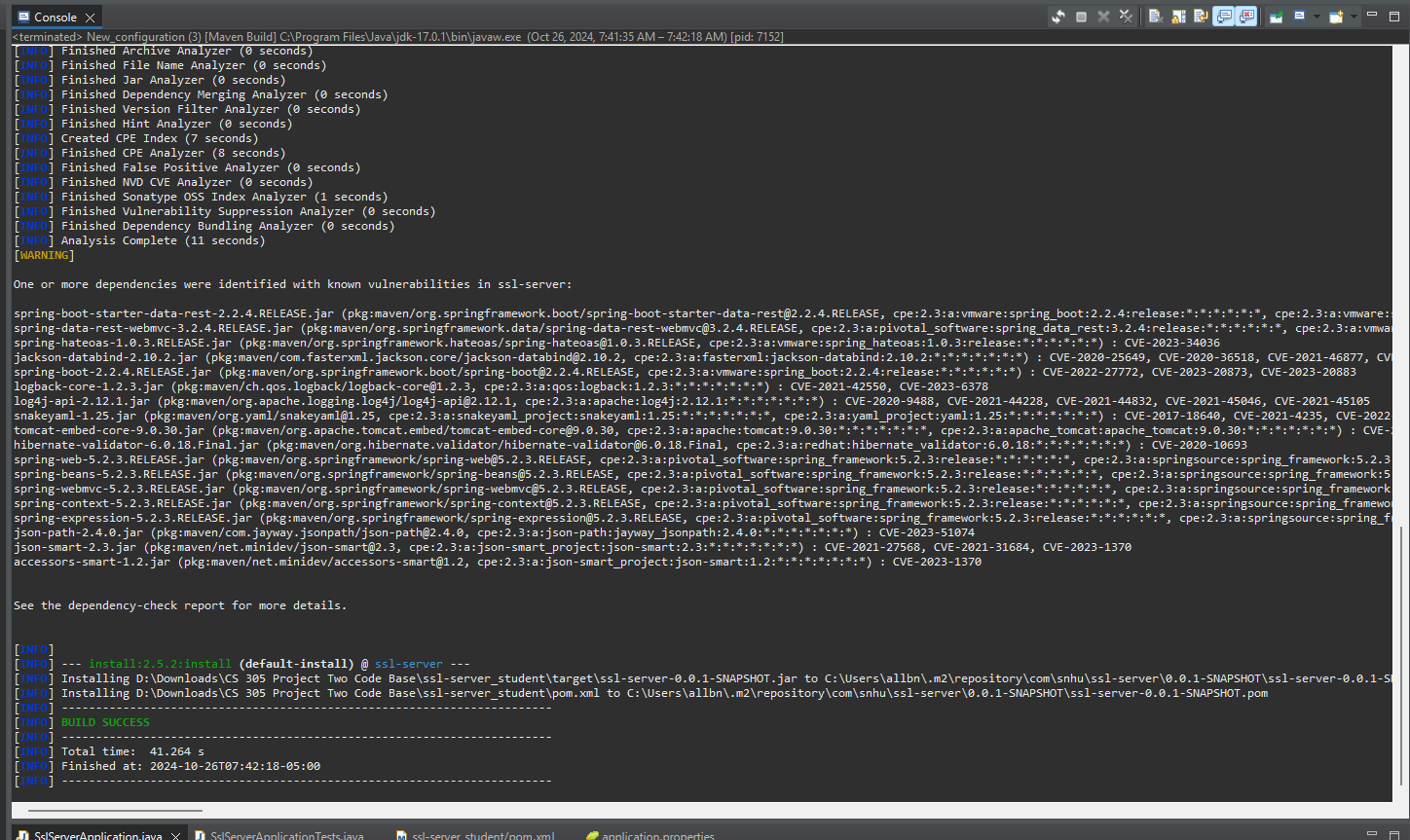
## Secure Communications

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



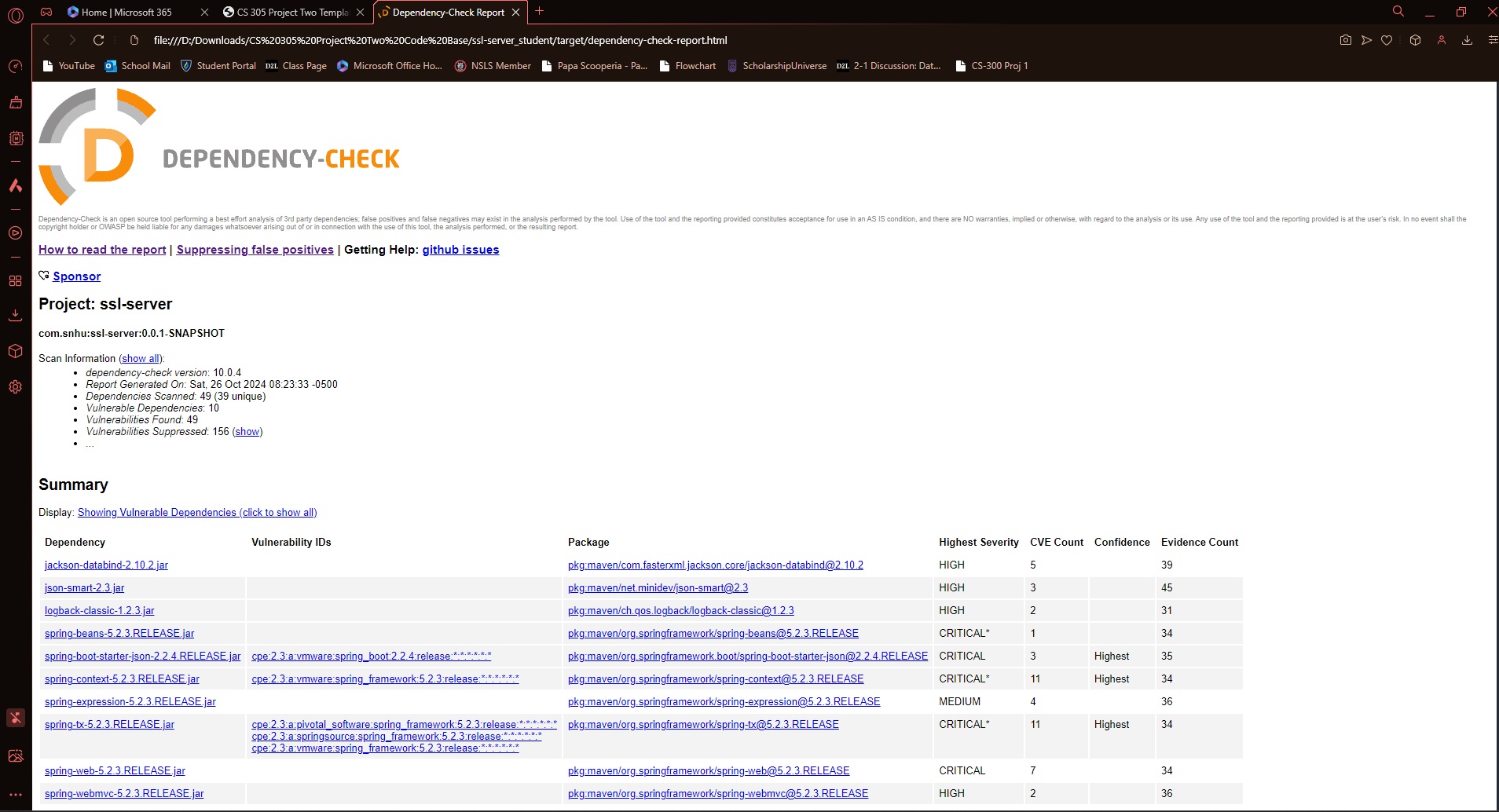
## Secondary Testing

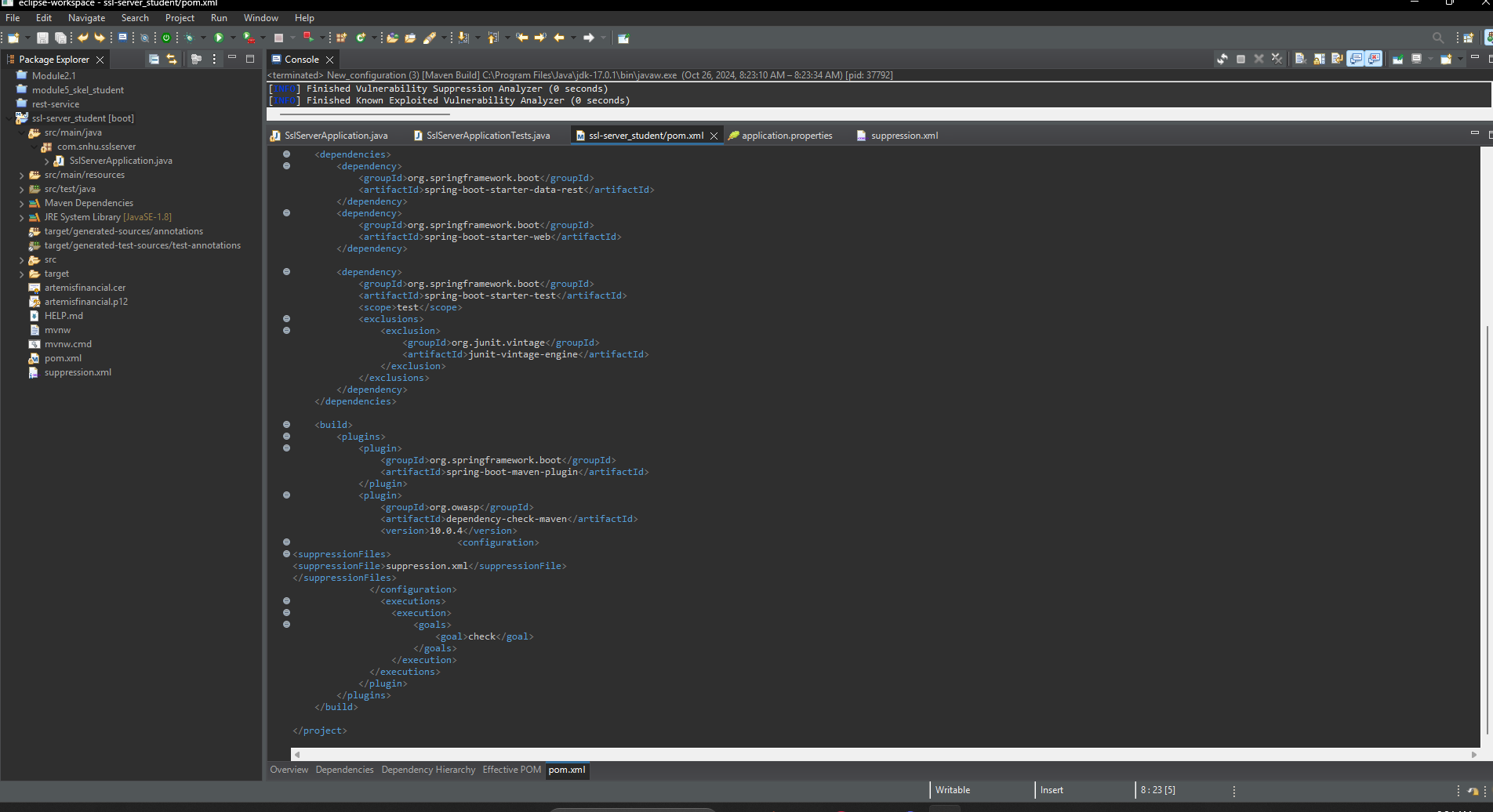
Insert screenshots below of the refactored code executed without errors and the dependency-check report.



## Functional Testing

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





## Summary

When refactoring the code most of the vulnerabilities came from outdated versions of the processes, so changing the versions to newer ones helped maintain security. Suppressing false positives helps filter out vulnerabilities and make the process more secure. Changes made to the codebase add encryption and certificate management, added security layers such as encryptions and secure communications.

## Industry Standard Best Practices

Industry standard best practices are important to follow for secure software. I followed this by creating input validation, adding a layer of encryption, making sure that the code runs without error, and following a quality code structure. The program is encrypted through AES and a certificate key, allowing encapsulation. The value of following these practices for a company like Artemis Financial is to protect their users while being able to transfer data globally. Artemis Financial has access to highly sensitive information about their clients and to transfer this information it must be protected, or they will no longer be able to retain their client base. This would make the company fail overall. In general, it is in the best interests of all companies to protect their information whether it be the companies or their clients, so the information does not become public or given to people that intend to do harm.