****

# 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** | **4/23/25** | **Christopher Braman** |  |

## 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

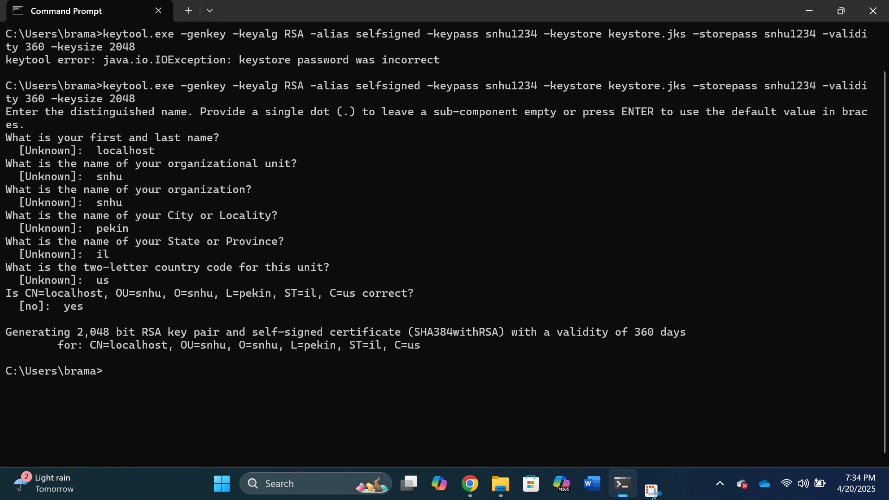
Christopher Braman

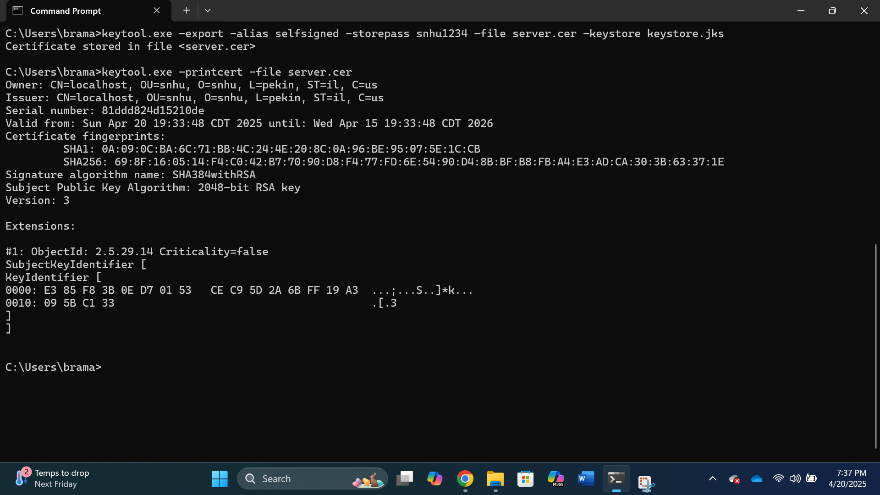
## Algorithm Cipher

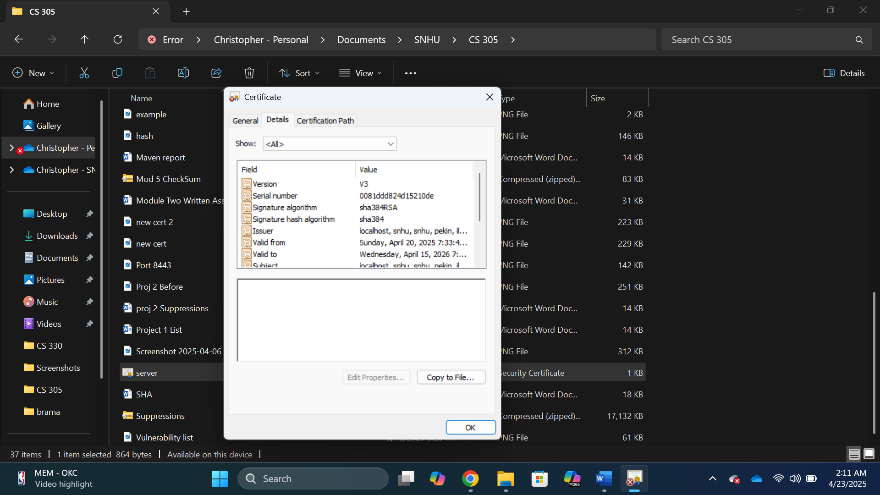
The algorithm cipher of choice is AES. Given that Artemis Financial is an institute that is looking to allow users to make deposits, invest, and obtain insurance they will need to have standards upheld by the United States (and potentially global) standards. With the AES algorithm cipher the information that will be transfer will be secured in two separate ways. It uses the standard AES (Advanced Encryption Standard) which encrypts the information with a specific key. This key can be many different forms of algorithms itself, I specifically used SHA-256 for the encryption. The only way for this encryption to fail is if the key is discovered and then applied to the specific information in transport that may have used that key. The odds of that are astronomically low. AES in maintained by NIST, and it is approved by the head of the US Commerce Department. This ensure that the standards for the US, as well as national standards are met.

## Certificate Generation

Insert a screenshot below of the CER file.

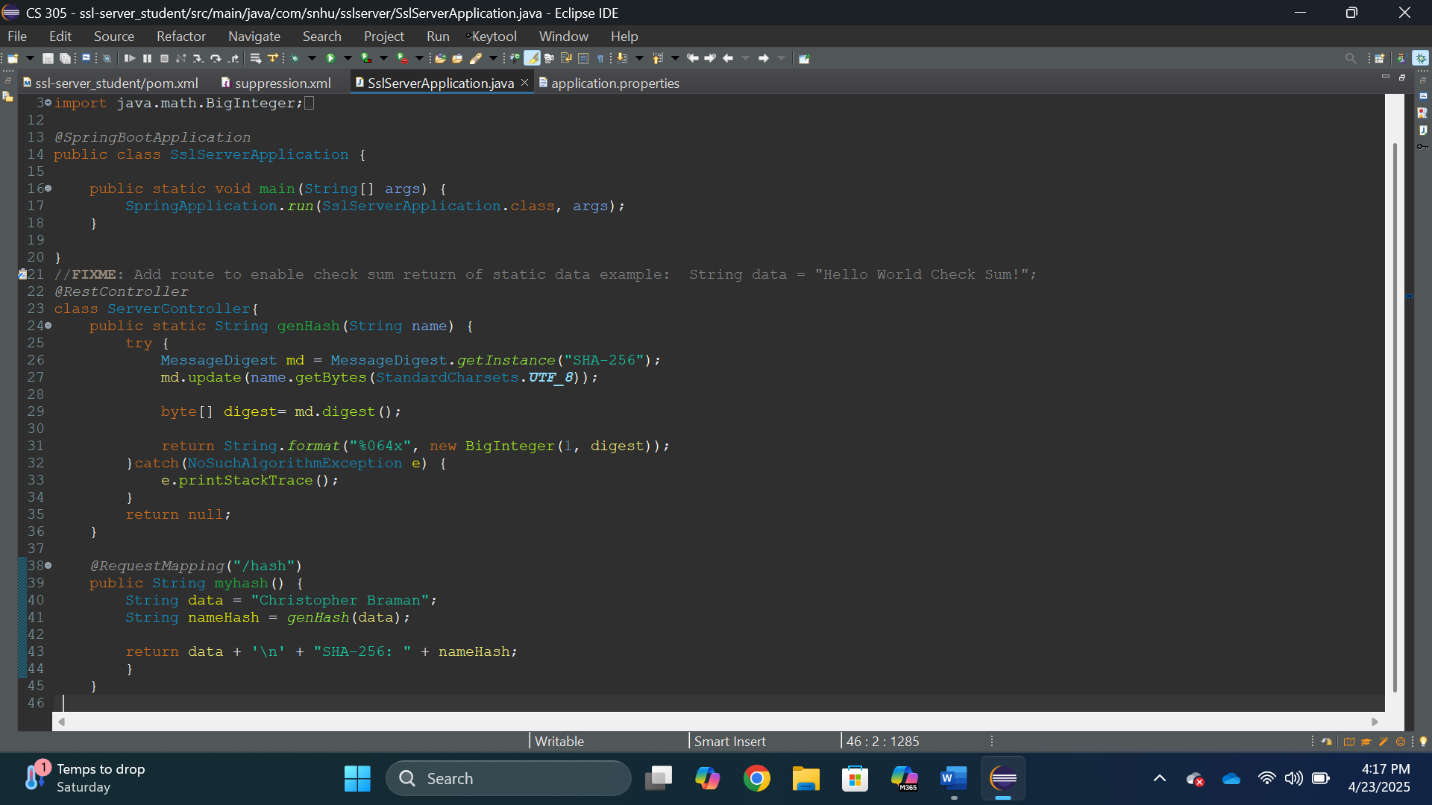






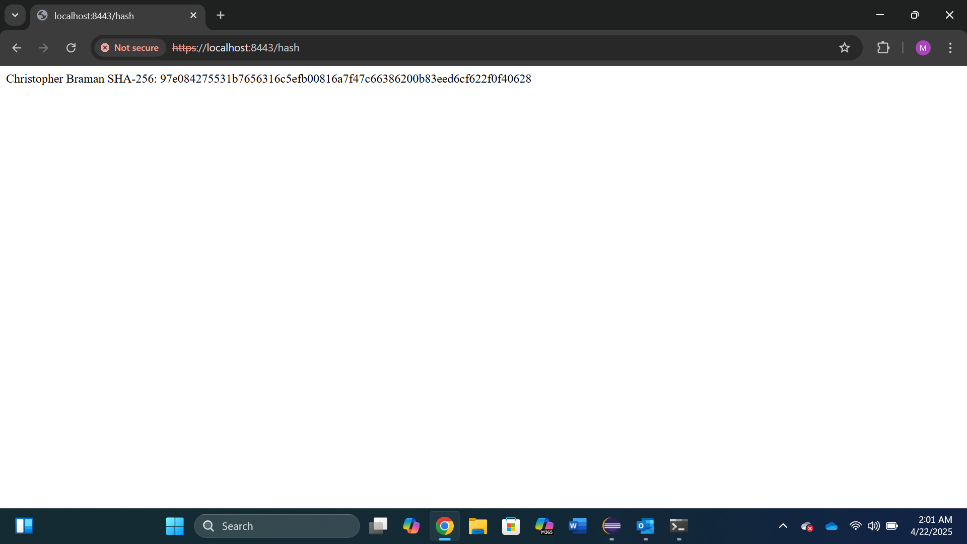
## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

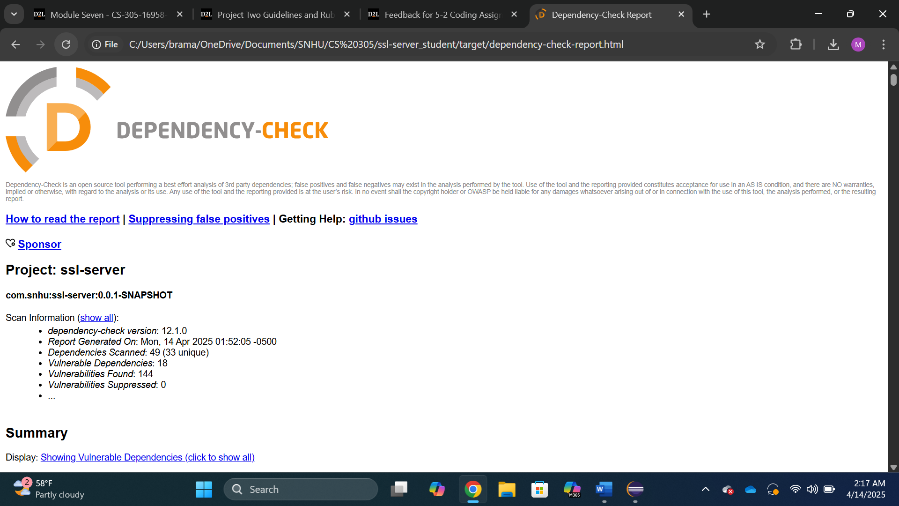
Insert a screenshot below of the web browser that shows a secure webpage.



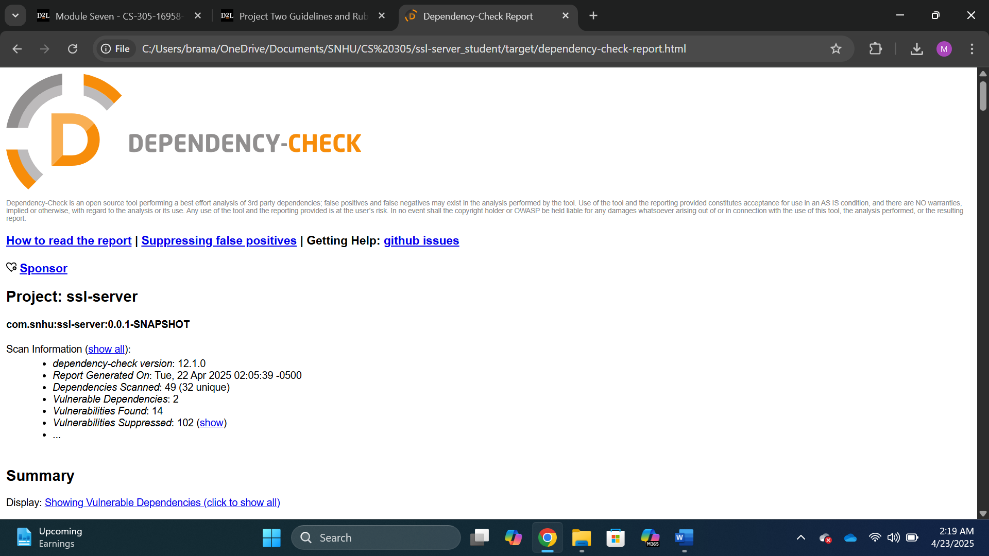
## Secondary Testing

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

Dependency Before:

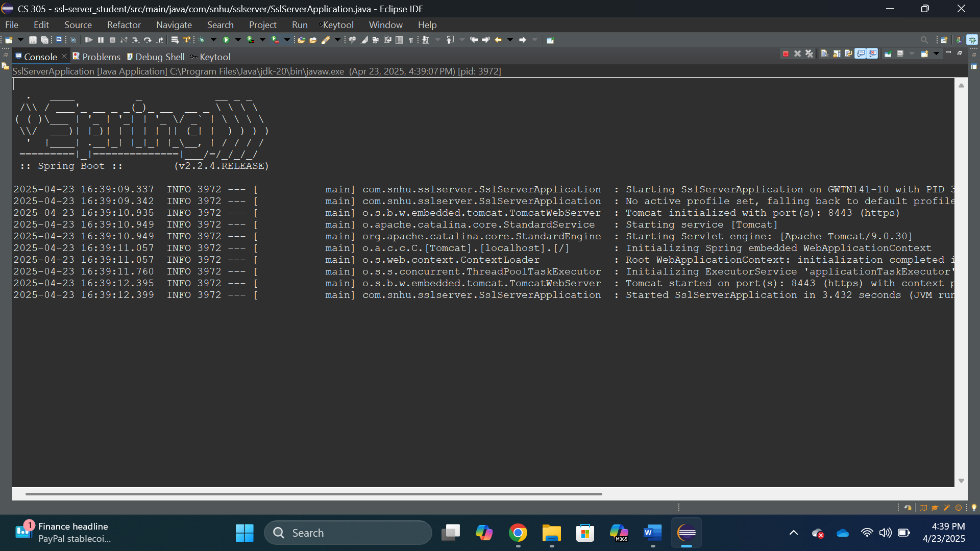


Dependency After Suppressions and Testing:



## Functional Testing

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



A screenshot of a computer

AI-generated content may be incorrect.

## Summary

Given the goals of Artemis Financial the areas of safety include: Cryptography, Client/Servers, and Error Handling. Due to the fact that Artemis Financial is handling with highly sensitive data, cryptography should be their highest priority. To help ensure that cryptography was handled properly the deployment of an algorithmic cipher is best used. SHA-256 a cipher that has been used within the US Department of Commerce so it is a well known and trusted cipher. It is also maintained by a reputable source, the National Institute of Standards and Technology (NIST). This helps alleviate the stress of meeting standards because the company will be using code that is upheld by those who set the standard.

The second point of interest is the Client/Servers. Ensuring there is a secure connection between the client and the server helps with security as well as reputation with the client. Establishing a secure connection with the use of certificates gives the ease of mind to anyone who maybe be using your services.

The final concern that was sent with the code that was sent is error handling. The was no error handling (try/catch) within the code. Making sure errors are handled properly, makes sure that hackers are not able to manipulate how/what the error would actually do. A simple try/catch statement prevents this.

Adding multiple layers for security is better than not having security at all. Imagine being in a situation where you have a firework going off in a firework factory. If the firework enters the factory it could cause some real problems. There are ways to safeguard this from happening through the use of layers of protection. Safe handling practices, ensuring that certain items are not permitted, making sure that the factory works and packs accordingly because if one thing goes wrong it could be catastrophic.

## Industry Standard Best Practices

Best practices were used in the code with proper naming conventions of the files (Ex: Suppression, pom, keystore), proper file placements (keystore file), generating a certificate, and through the use of try/catch clauses. Applying these best practices helps maintain security through ease of maintenance, error handling, and secure connections.

References

National Institute of Standards and Technology. (November 26, 2001). *Announcing the ADVANCED ENCRYPTION STANDARD (AES).* NIST. <https://csrc.nist.gov/files/pubs/fips/197/final/docs/fips-197.pdf>