****

# 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** | **February 24,2024** | **Jeffrey Gaspardino** |  |

## 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

Jeffrey Gaspardino

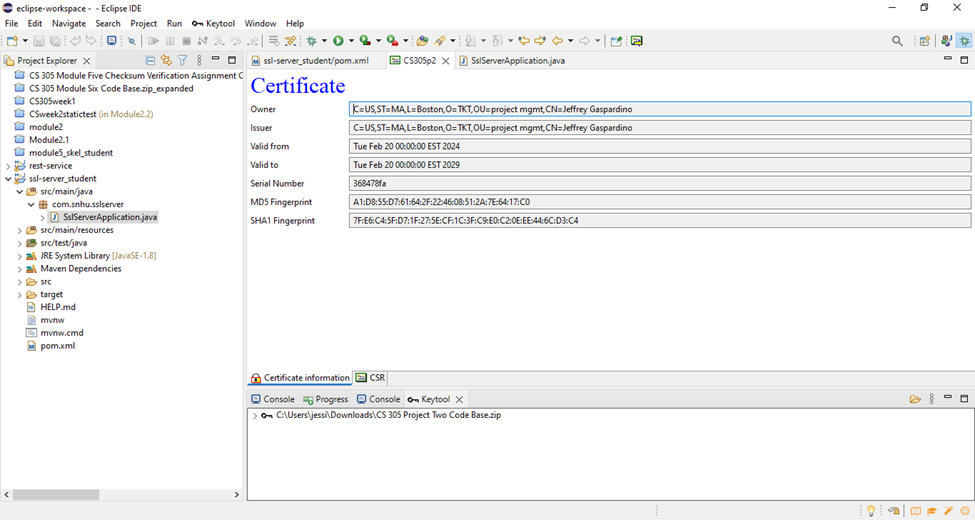
## Algorithm Cipher

The main goal for Artemis Financial is to create a website that is efficient, safe and able to transfer client data securely. I think the best course of action for Artemis would be to work with Advanced Encryption Standard (AES) algorithm to encrypt their files. AES encrypts data in 128,192 and 256-bit blocks. I would strongly encourage Artemis to employ SHA-256 as the encryption algorithm cipher. This cipher is widely used due to it being impossible to penetrate or crack. It would take outside forces years to break SHA-256 cipher. The SHA-256 hash function and bit levels are made from random letters and numbers. The hash value is the name for the compressed data. The length of the encryption is determined by the bit levels.

Symmetric Keys is said to be the simplest and best-known encryption technique. It uses one key for both encryption and decryption. Symmetric is less complex but does execute faster and typically the preferred usage when sending data in bulk. The first known evidence of the use of cryptography (in some form) was found in an inscription carved around 1900 BC, in the main chamber of the tomb of the nobleman Khnumhotep II, in Egypt. (Sidhpurwala,H ., 2023). The current/future state of encryption algorithms is not completely safe. Experts think that if quantum computing becomes powerful enough, the algorithms used today could be easily cracked. Software developers will need to update their products accordingly before these quantum computers become commonplace and readily available.

## Certificate Generation

Insert a screenshot below of the CER file.

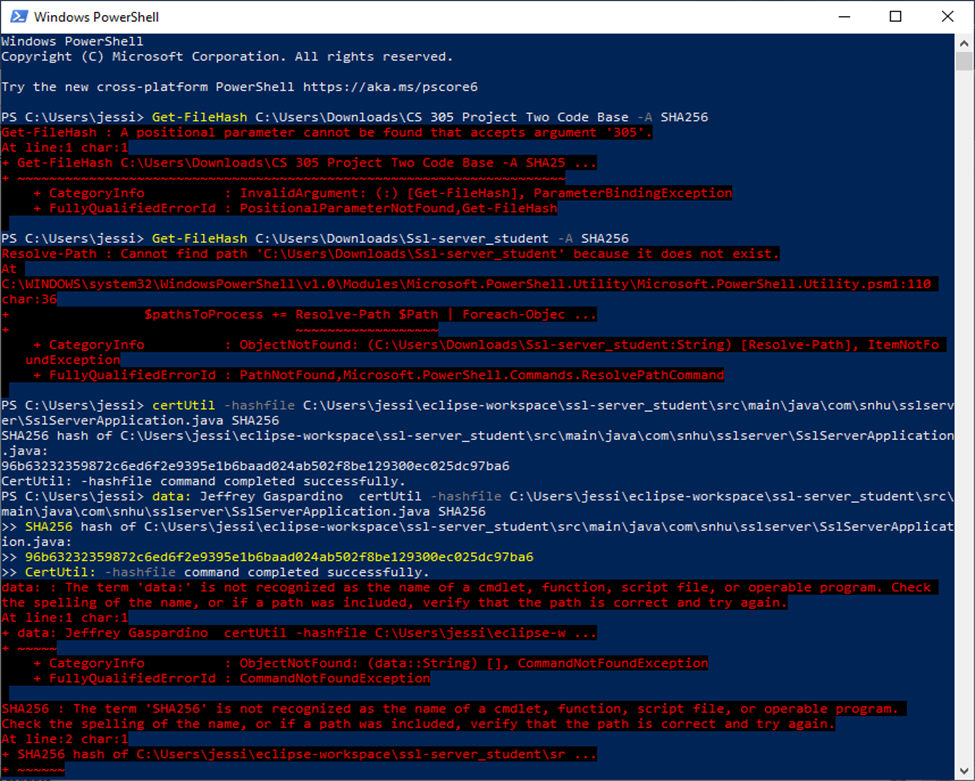


A screenshot of a computer

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.



PS C:\Users\jessi> data: Jeffrey Gaspardino certUtil -hashfile C:\Users\jessi\eclipse-workspace\ssl-server\_student\src\main\java\com\snhu\sslserver\SslServerApplication.java SHA256

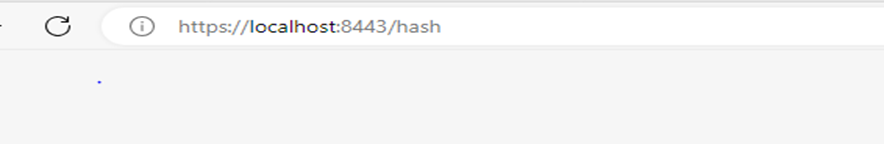
>> SHA256 hash of C:\Users\jessi\eclipse-workspace\ssl-server\_student\src\main\java\com\snhu\sslserver\SslServerApplication.java:

>> 96b63232359872c6ed6f2e9395e1b6baad024ab502f8be129300ec025dc97ba6

>> CertUtil: -hashfile command completed successfully.

## Secure Communications

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



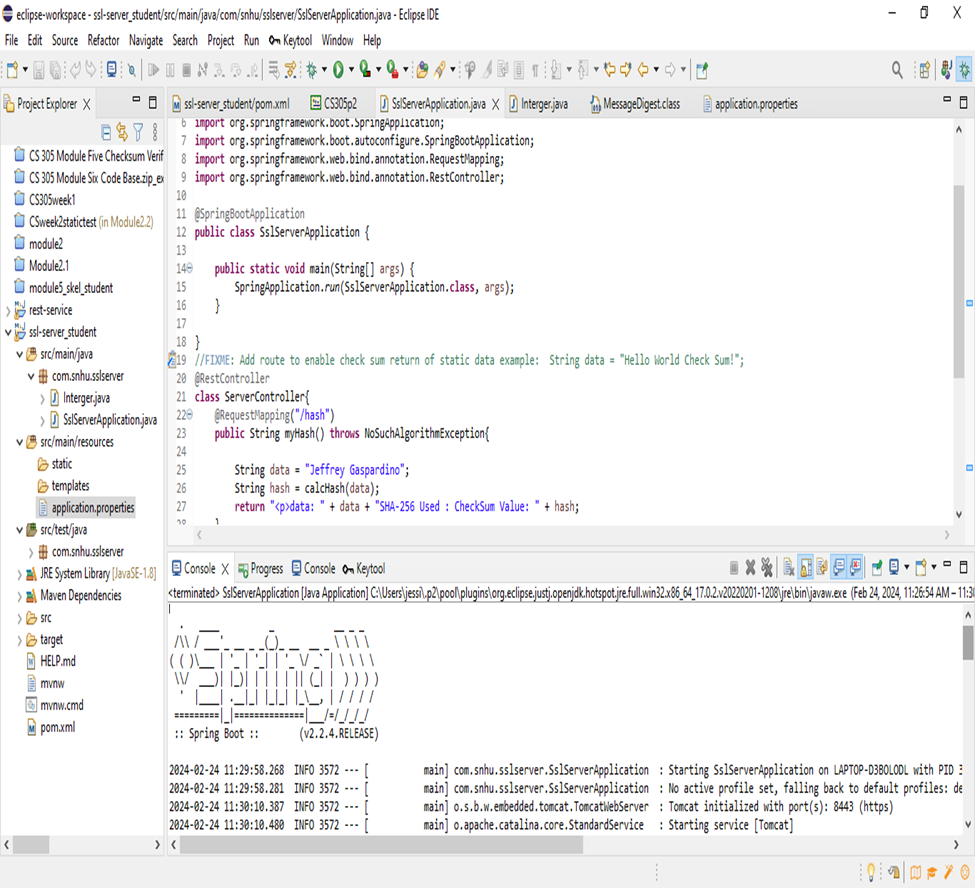
A screenshot of a computer error

Description automatically generated

I was having trouble with Microsoft 365 but this the screenshot I got.

## Secondary Testing

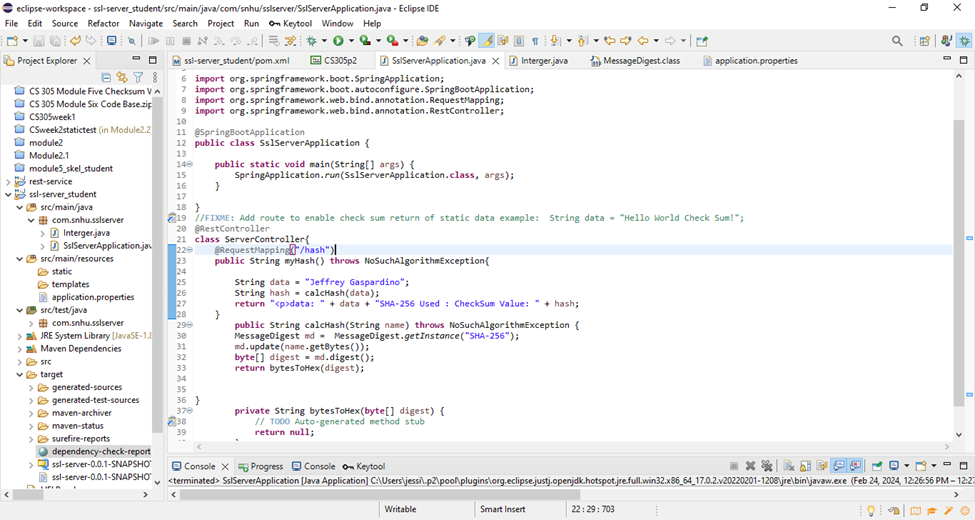
Insert screenshots below of the refactored code executed without errors and the dependency-check report.

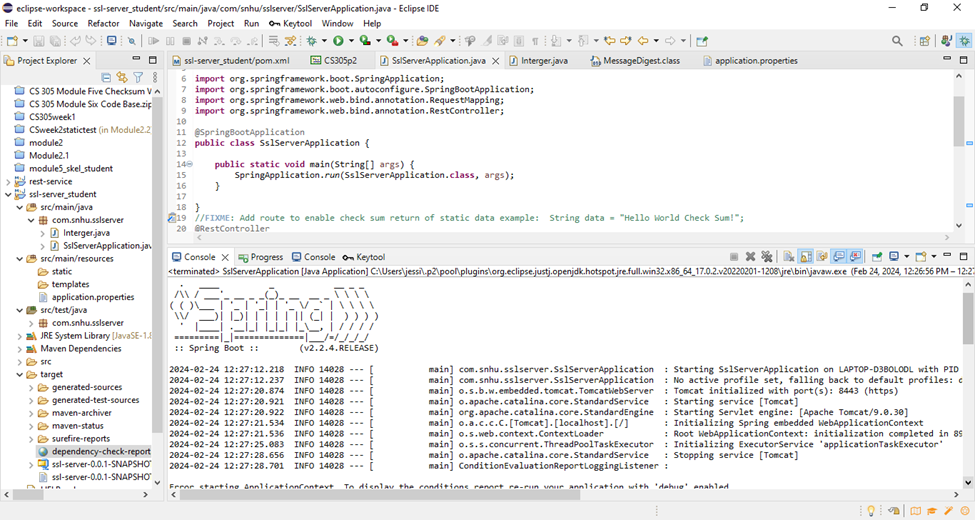




## Functional Testing

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





## Summary

By investigating and then using the Vulnerability Assessment Process Flow Diagram, the code was updated and added with the use of a hash function for the checksum verification. In addition, the site was installed with the certification generation and keystore use. By implementing a hash function for data integrity, Artemis will be notified if any outside party tries to gain access to their site. Another area of security was using an HTTPS instead of an HTTP. These updates will aide Artemis so that its customers won’t face security problems.

## Industry Standard Best Practices

To maintain the current security of a software application, I followed industry standard best practices for secure coding. These practices include:

1. Input validation: Ensuring that all user inputs are properly validated and sanitized to prevent common vulnerabilities.
2. Secure authentication and authorization: Implementing strong authentication mechanisms, such as multi-factor authentication, and proper authorization controls to ensure that only authorized users can access sensitive data or perform specific actions.
3. Secure communication: Using secure protocols like HTTPS to encrypt data transmitted between the application and users, preventing eavesdropping or tampering.
4. Secure configuration: Ensuring that the application is properly configured with secure settings, such as disabling unnecessary services and using strong encryption algorithms.
5. Regular updates and patches: Keeping the software application up to date with the latest security patches and fixes to address any known vulnerabilities.

Applying industry standard best practices for secure coding is crucial for a company's overall wellbeing. Here are some reasons why:

1. Protection against data breaches: By following secure coding practices, companies can reduce the risk of data breaches and unauthorized access to sensitive information, protecting their customers' data and their own reputation.
2. Compliance with regulations: Many industries have specific regulations and standards related to data security. Adhering to industry best practices helps companies meet these requirements and avoid legal consequences.
3. Cost savings: Addressing security vulnerabilities early in the development process is generally more cost-effective than fixing them later. By following best practices, companies can reduce the likelihood of security incidents and the associated financial impact.
4. Customer trust and loyalty: Demonstrating a commitment to security by following industry best practices can enhance customer trust and loyalty. Customers are more likely to choose and remain loyal to companies that prioritize the security of their data.