****

# 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** | **11/12/2025** | **Evan Nagy** |  |

## 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

Evan Nagy

## Algorithm Cipher

There are several types of algorithms available to us. However, the major contenders would be the

AESalgorithm and SHA-256. AES is a symmetric encryption where the same key used to encrypt is used

to decrypt a message. Without this key a message is unviewable to anyone who does not have this key.

AES is the standard for the government and banking across the world and is one of the safest

encryption methods available for confidential data.SHA-256 is an algorithm that that produces a

hash function to store the data instead of encryption. A hash function are primarily used to verify data

integrity and store passwords. This in summary will create a, “digital fingerprint” for our messages.

AES was created 1997 by the National Institute of Standard Technology “NIST”. AES was created with

the intent for creating stronger and more versatile encryption standards than previous Data Encryption

Standard “DES”. In 2001 it was officially adopted as this new standard and has been widely adopted

since.

SHA-256 is part of a family of SHA algorithms. It was developed in 2001 to be an easier algorithm to

use and a stronger algorthim than previous algorithms. Today, since it can create a digital fingerprint, it

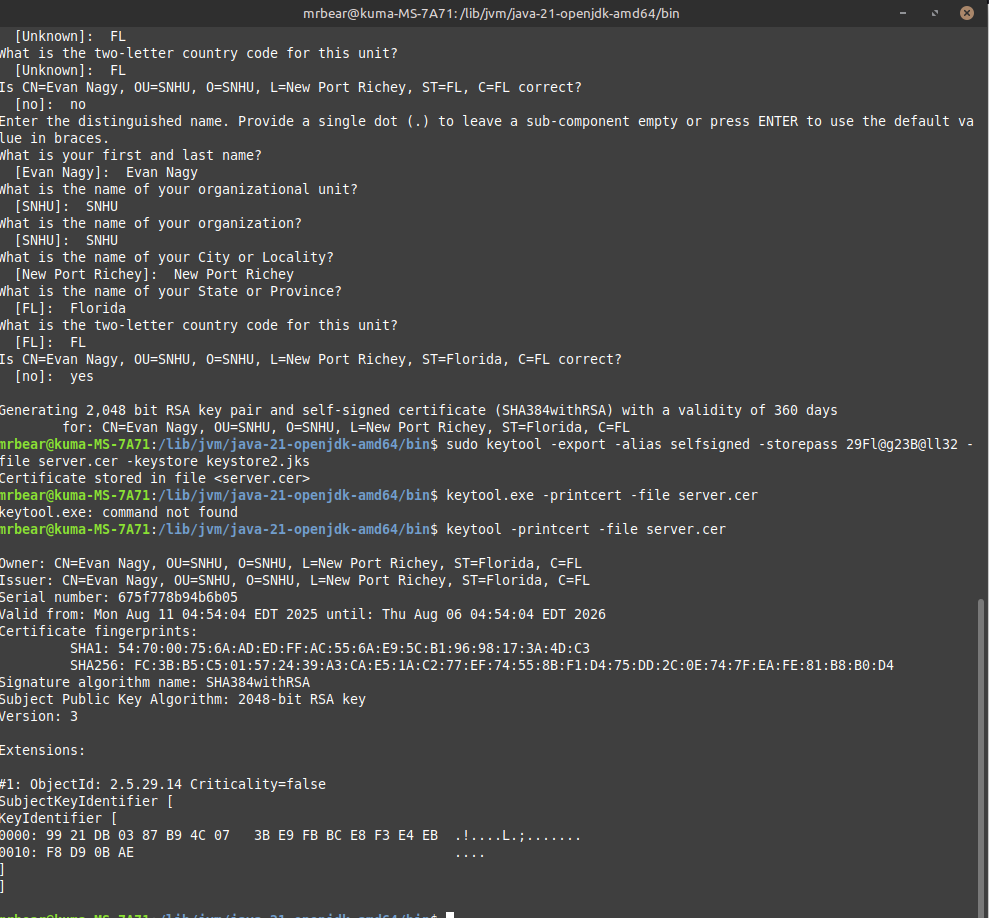
is used for creating digital certificates , cryptocurrency mining and password hashing.

In my opinion, since we are dealing with sensitive financial information, we should be implementing

AES due to its ability to encrypt.

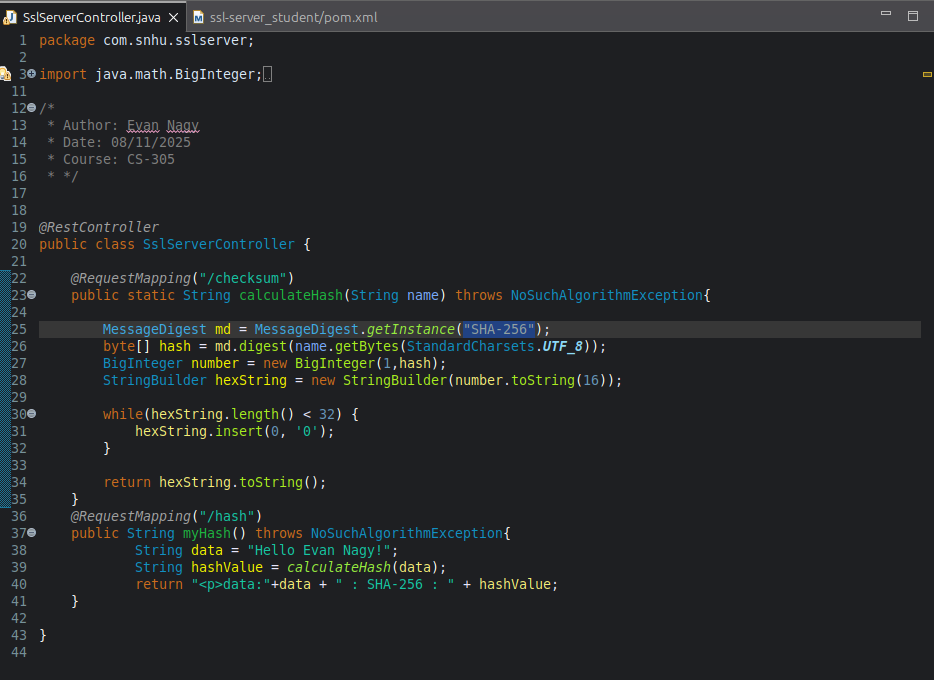
## Certificate Generation

Insert a screenshot below of the CER file.



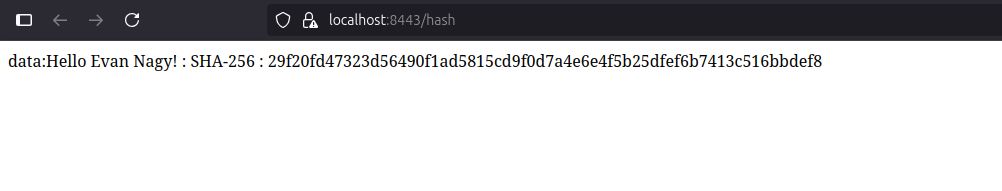
## Deploy Cipher

Insert a screenshot below of the checksum verification.



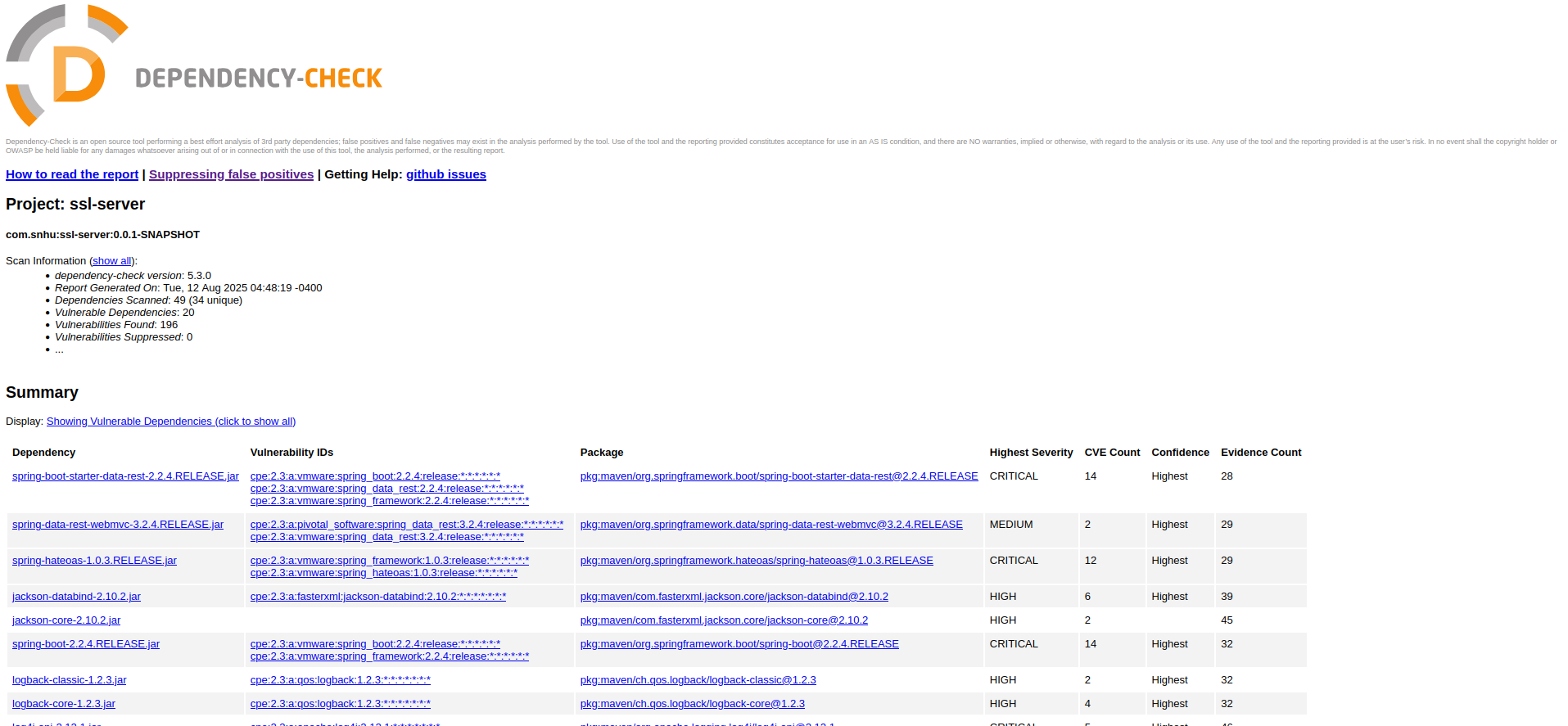
## Secure Communications

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



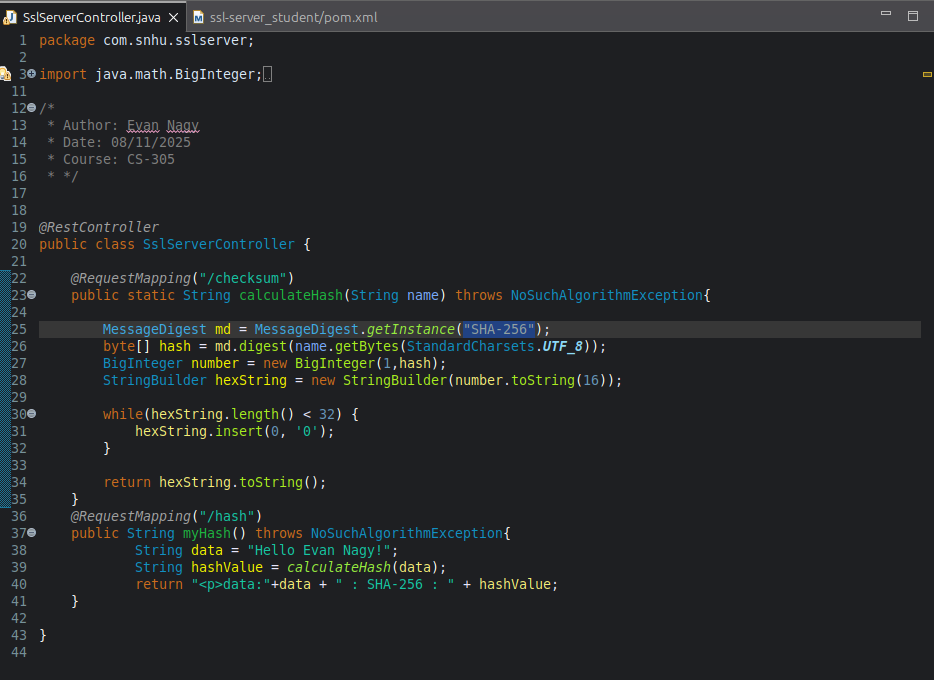
## Secondary Testing

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

Considering the Vulnerability Assessment Process Flow Diagram, “VAPFD”. I created a class called

sslServerController in order to keep my code organized. This is where I placed my @RestController and

@RequestMapping so that the program will refer to these bits of code when looking for my hash and

checksum. Since we have 2 options for our algorithm is used SHA-256 as a place holder until Artemis

Finacial tells me which standard they want to work with. My personal recommendation is AES for its

key encryption ability.

## Industry Standard Best Practices

Software Security is imperative when considering best practices. There will always be malicious

agents out in the world trying to make a quick buck off of other people's misery. When making sure

that your code is secure, you make sure your company is secure. With this security, you will save time,

effort and manpower in the long run. Whenever a company has been breached, lives can be ruined,

money can be lost and a permanent scar on your company's reputation can occur. These reasons and

more are why Security should be top priority whenever you create an application.