****

# 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** | **04/19/2024** | **Michael Fortugno** |  |

## 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

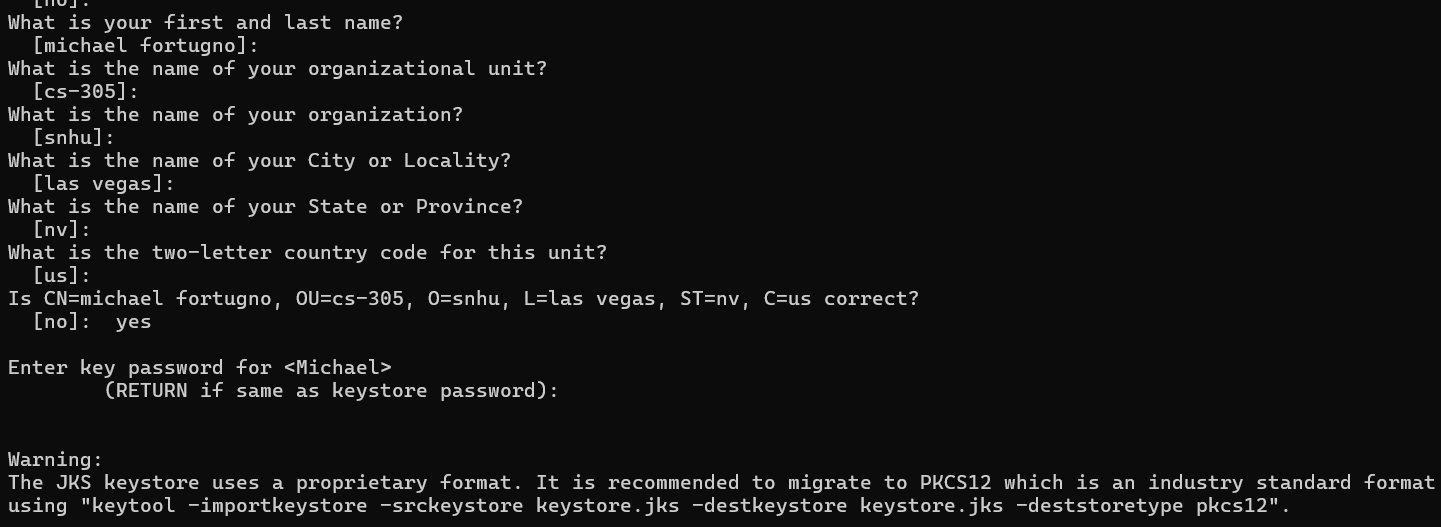
Michael Fortugno

## Algorithm Cipher

The best encryption algorithm for Artemis Financial would be Advanced Encryption standard (AES), utilizing SHA (256) hash functions. This cipher provides excellent security to any potential attackers, AES is an industry standard used by many businesses and government. The sensitive information that Artemis financial will be dealing with this cipher will provide best security possible. The bit count size of the has function can be 128, 192, or 256 bits. The encryption uses different rounds to generate the keys for the encryption depending on the but size count for example 128 bits would have 10 rounds 192 bits 12 rounds and 256 14 rounds. The decryption process is the same just in reverse of the encryption process.

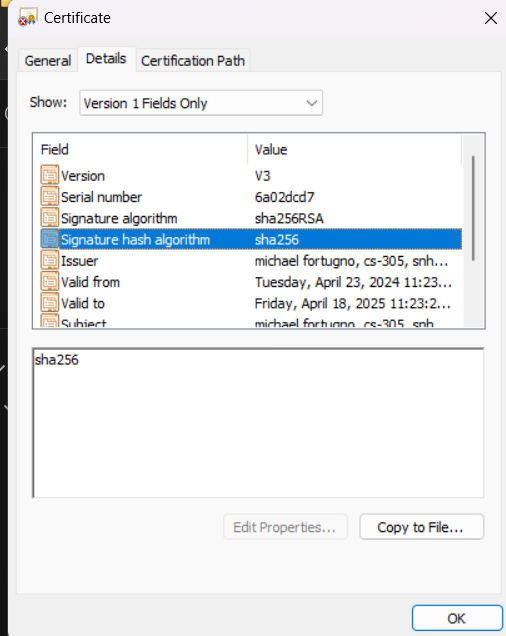
Encryption methods date back to ancient times with simple methods such as replacing a letter to be another letter and create a cipher so messages could be encrypted and decrypted. During World War 2 the enigma machine was for the time an advanced encryption method the Germans used to encrypt messages. With the inventions of computers simple encryption methods are no longer good enough as a computer can go through all possible combinations extremely fast, so better methods such as hash functions need to exist to attempt to create keys that that brute force attacks are not realistic.

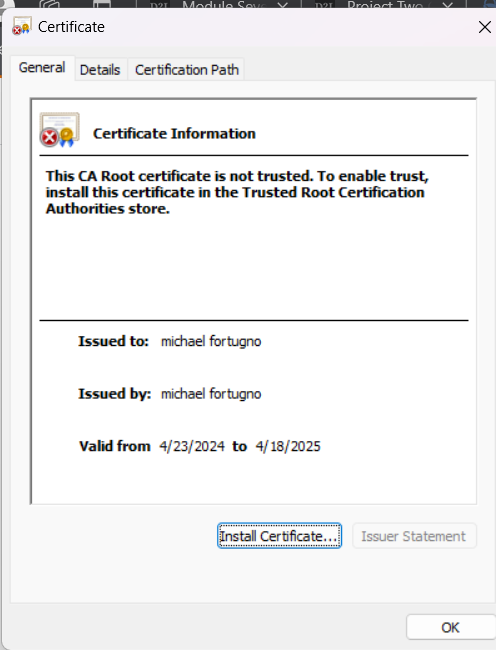
## Certificate Generation



A screen shot of a computer

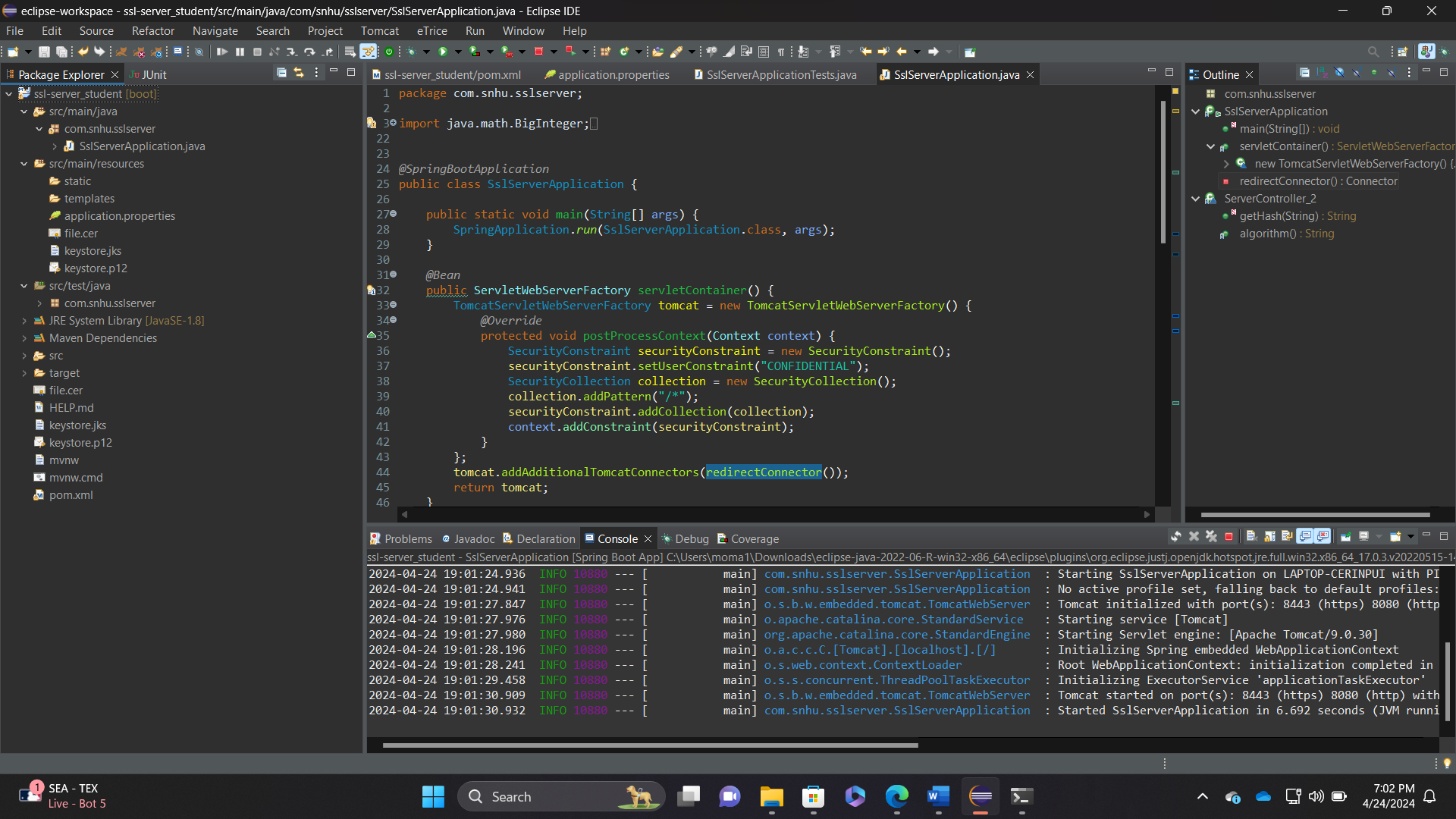
Description automatically generated





## Deploy Cipher

Insert a screenshot below of the checksum verification.



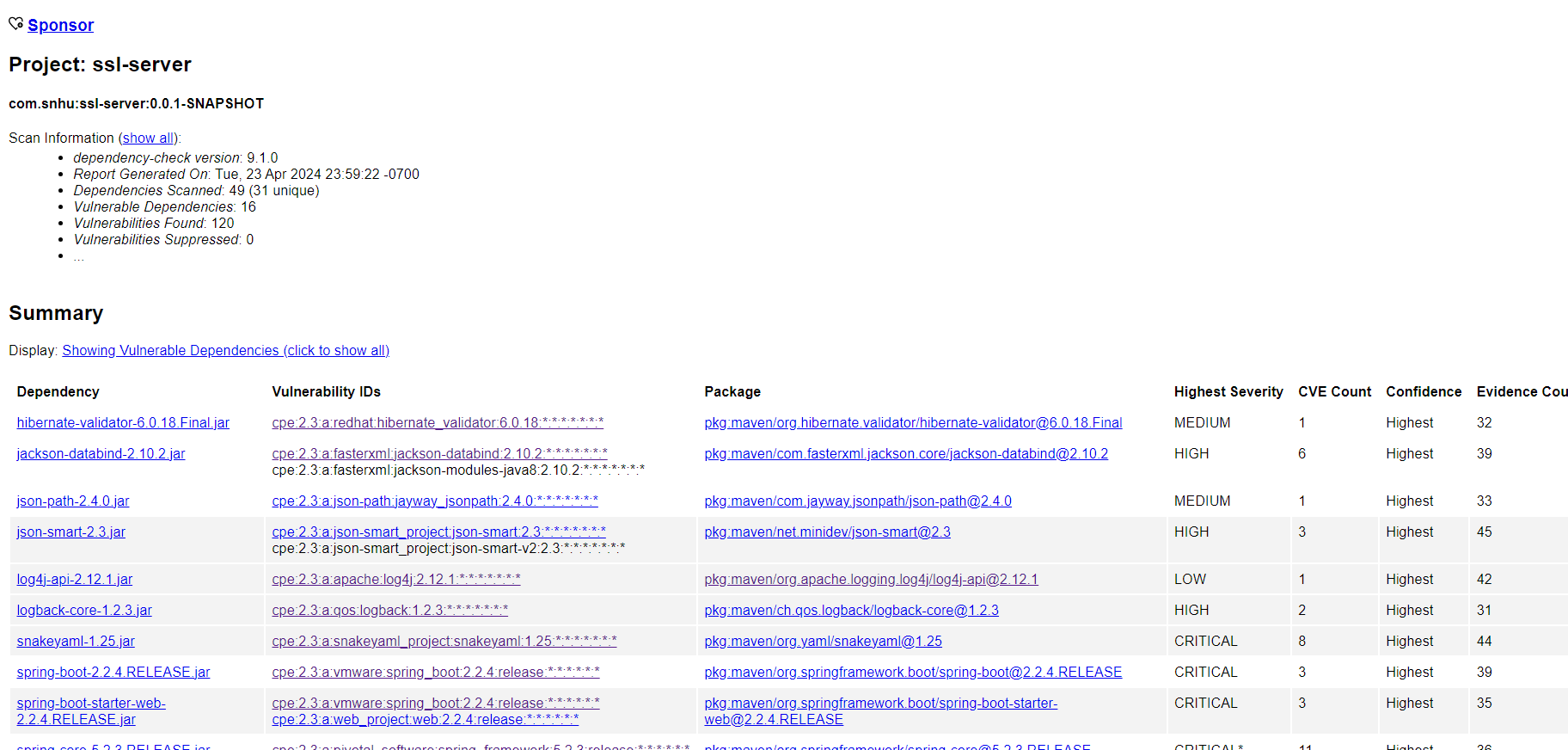
## Secure Communications

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

[Insert screenshots here.]

## 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.

[Insert screenshots here.]

## Summary

I was unable to get code to run properly when it would connect to server code would just freeze in place but would never continue to completion, there were no error codes given and trying to research this problem I have been unable to resolve this issue, so I could not complete the check sum verification process and thus not complete assignment to completion.

## Industry Standard Best Practices

Ensuring you are using most up-to-date versions of software that has been protected from any vulnerabilities that present security issues earlier versions.

Make sure to suppress any false positives so time is not wasted working on vulnerabilities that are not relative to your code or is not a vulnerability at all.

Ensuring methods and members are protected by using proper private members and methods that restrict access to these which could be an attack vector.