****

# 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 5](#_Toc102040759)

[3. Deploy Cipher 5](#_Toc102040760)

[4. Secure Communications 5](#_Toc102040761)

[5. Secondary Testing 6](#_Toc102040762)

[6. Functional Testing 7](#_Toc102040763)

[7. Summary 7](#_Toc102040764)

[8. Industry Standard Best Practices 8](#_Toc102040765)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **12/3/22** | **Douglas Bolden** |  |

## 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.

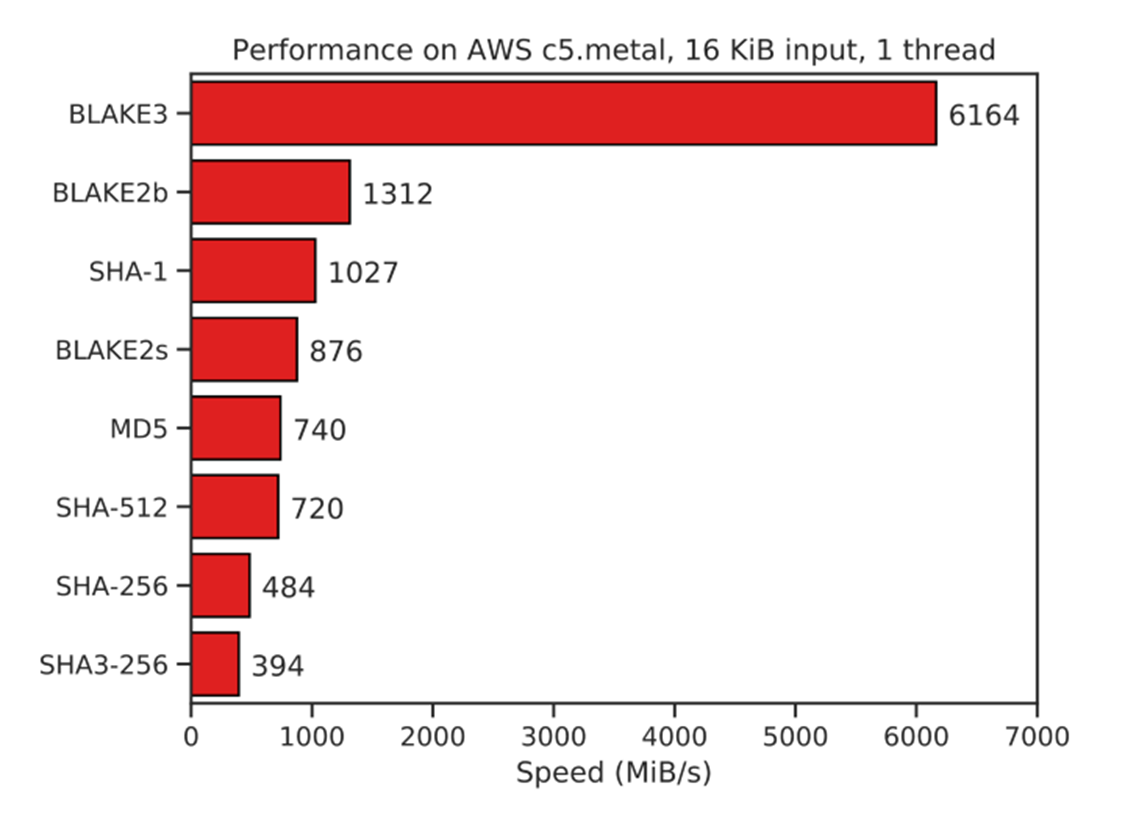
* Respond to the steps outlined below and include your findings.
* Respond using your own words. You may also choose to include images or supporting materials. If you include them, make certain to insert them in all the relevant locations in the document.
* Refer to the Project Two Guidelines and Rubric for more detailed instructions about each section of the template.

## Developer

Douglas Bolden

## Algorithm Cipher

BLAKE3 – This cipher is extremely secure, fast, and powerful.



As can be seen by the preceding graph, the speed of BLAKE3 completely wipes the floor with the current speed of any hashing algorithm. It also uses 256 bits. BLAKE3 is extremely fast and secure. Ultimately, this makes it collision free:

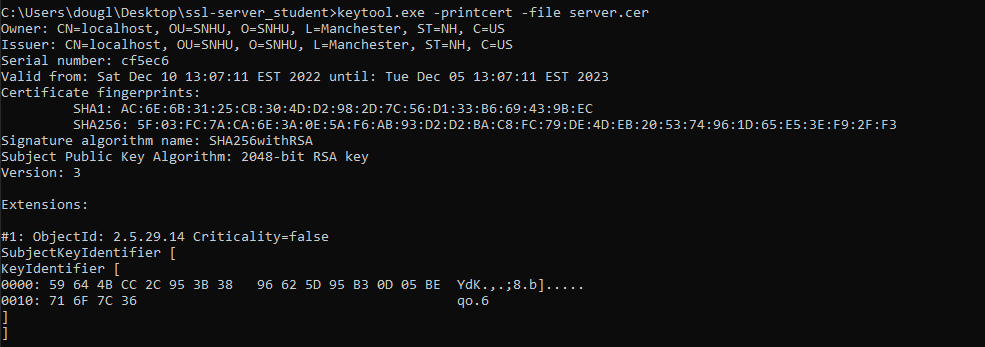
256-bit encryption is refers to the length of the encryption key used to encrypt a data stream or file. A hacker or cracker will require 2256 different combinations to break a 256-bit encrypted message, which is virtually impossible to be broken by even the fastest computers.

Typically, 256-bit encryption is used for data in transit, or data traveling over a network or Internet connection. However, it is also implemented for sensitive and important data such as financial, military or government-owned data. The U.S. government requires that all sensitive and important data be encrypted using 192- or 256-bit encryption methods. (256-Bit Encryption)

Symmetrical keys are useful, but asymmetrical keys are more secure. The biggest problem with asymmetrical keys is how slow the process is. Other than that, asymmetrical is the best choice. It is harder to break the algorithms. Random numbers make it harder for people who want to steal your information. Some encryption algorithms have been broken, but most algorithms are still intact today, as they use absurdly strong encryption (military grade), some of which can’t even be broken by a super-computer (at least not yet).

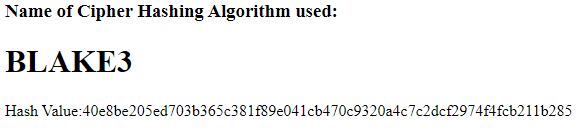
## Certificate Generation

Insert a screenshot below of the CER file.



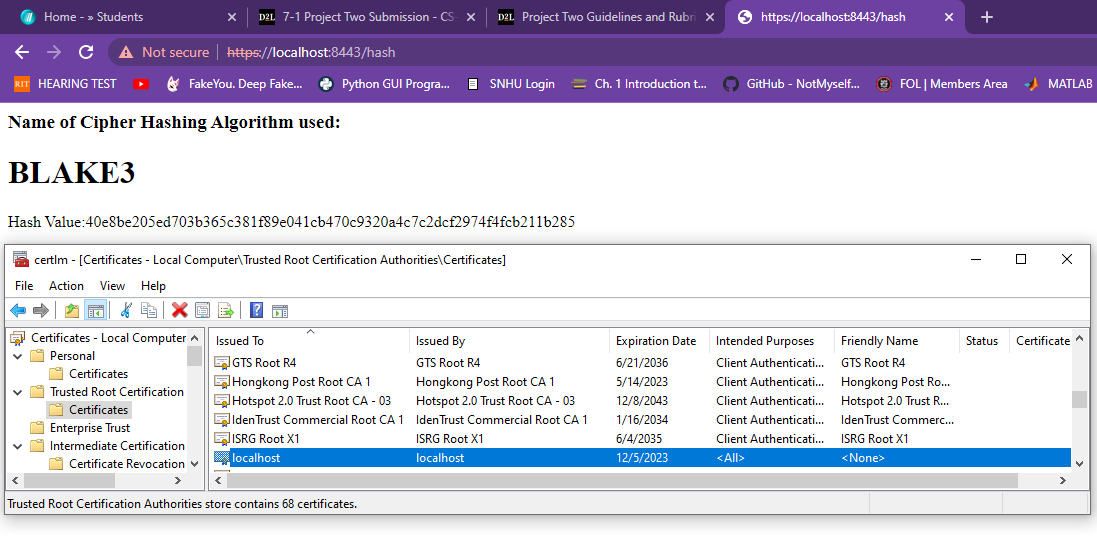
## Deploy Cipher

Insert a screenshot below of the checksum verification.



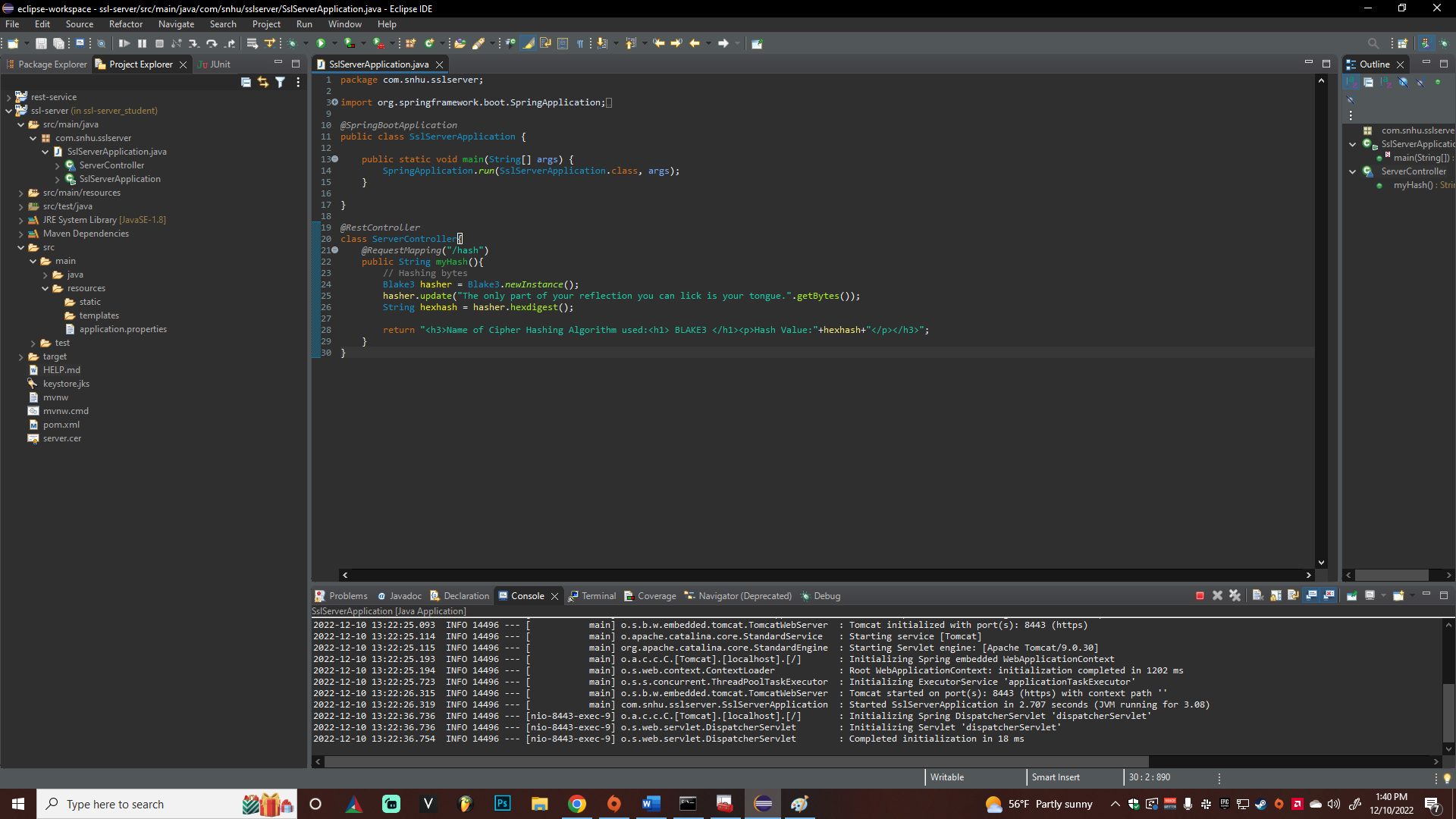
## Secure Communications

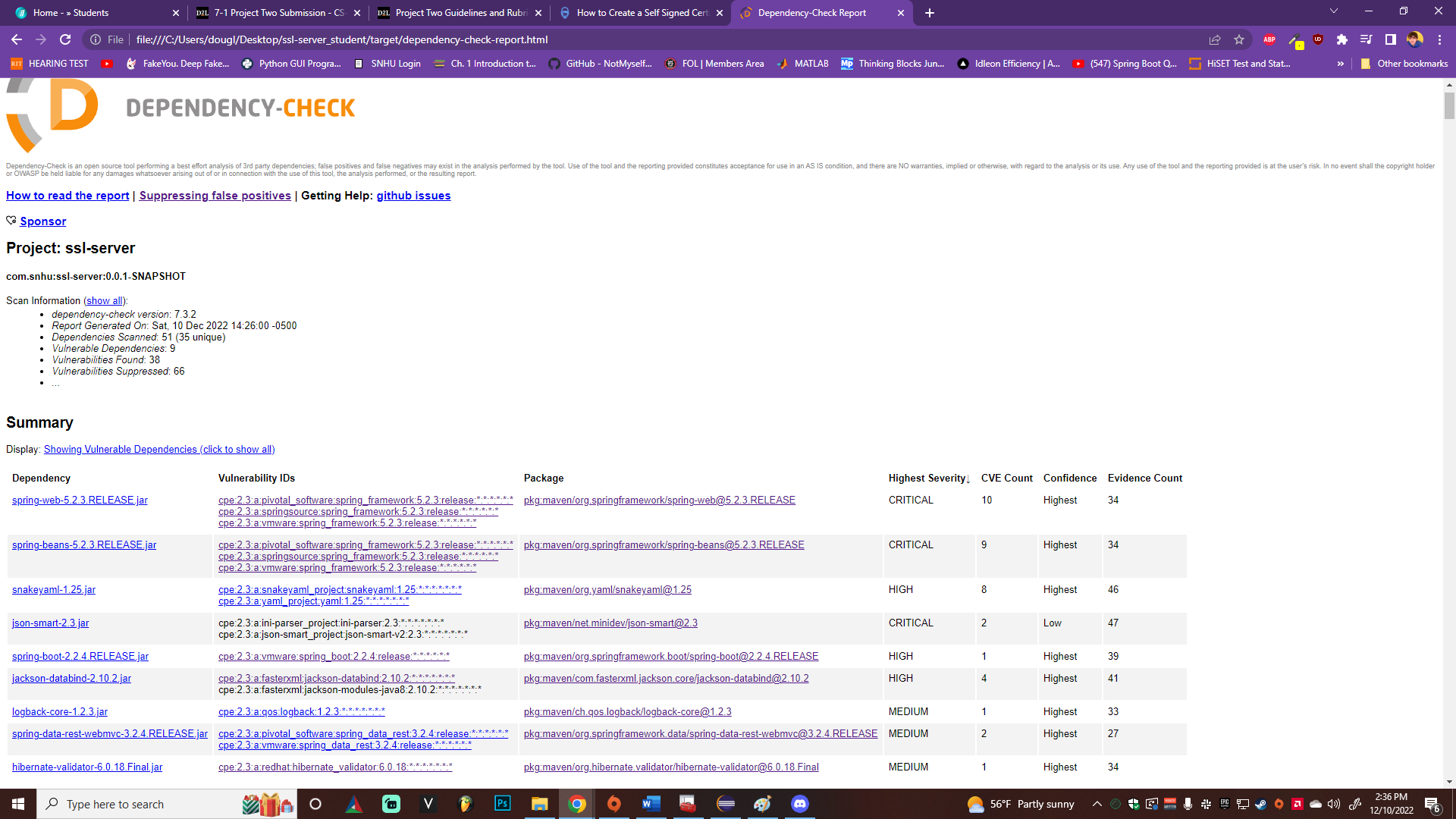
Insert a screenshot below of the web browser that shows a secure webpage.



## Secondary Testing

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

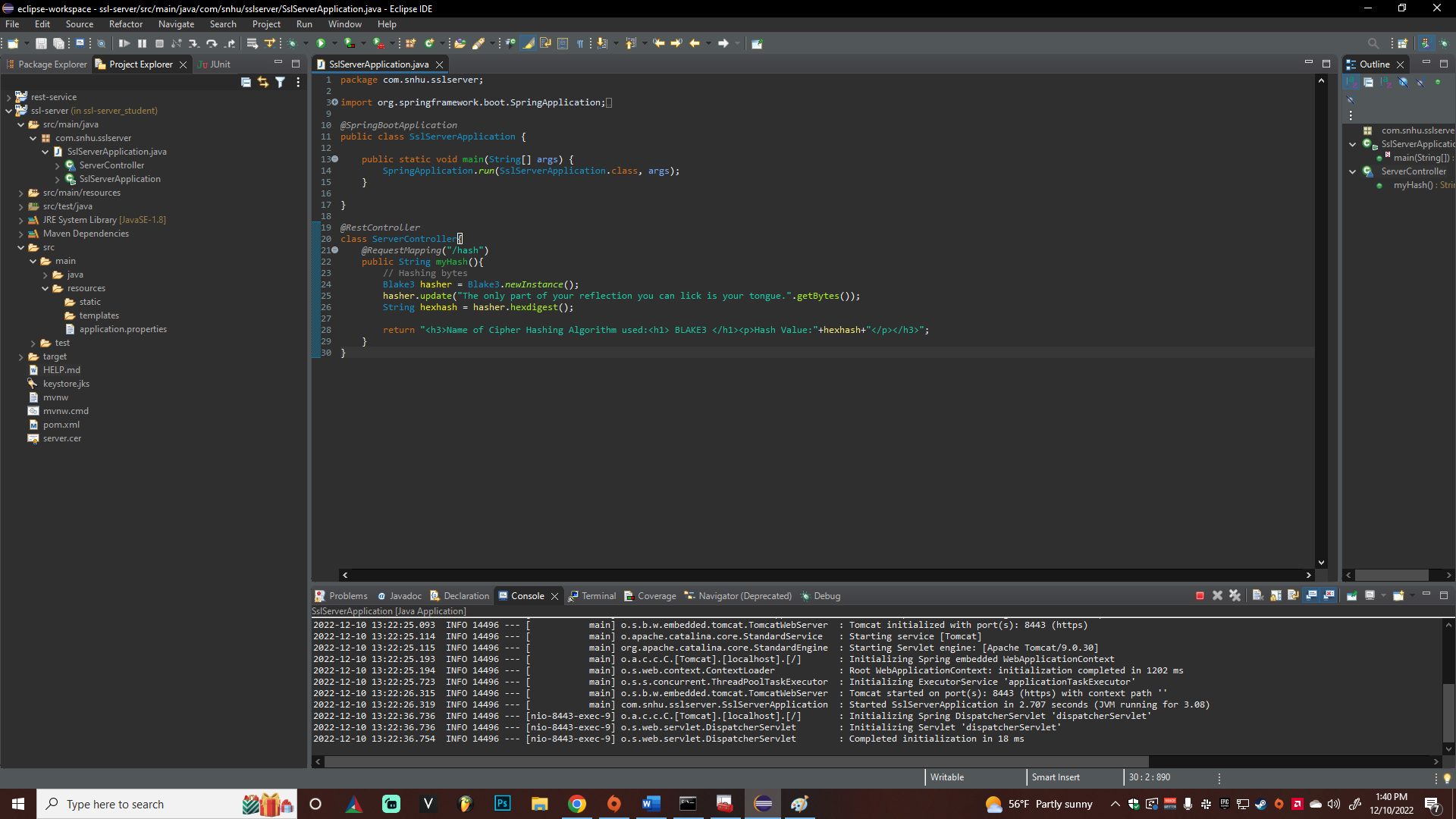




No new dependencies arise.

## Functional Testing

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



## Summary

* Areas of Security addressed:
  + Cryptography
  + Client / Server
  + Code Quality
* Added a Rest Controller
* Added BLAKE3 encryption to a test string
* Output the hexhash of the checksum

## Industry Standard Best Practices

Using the application of industry standard best practices, I used the BLAKE3 Algorithm Cypher to encrypt information that was transferred to html. In doing so, I made sure that all best practices were followed, and ensured that the company’s current security was strictly followed. I also implemented a dependency suppression file to alter the current dependencies to hide all the false positive dependencies in the dependency report. Software security is crucial in society as most of the information on the internet is credentials. These credentials contain personal identification, and this information is what hackers want. When I used the encryption cypher, I made sure that it was well fortified by using a cipher with a high encryption level that hasn’t been cracked. This makes it impossible for hackers to steal this information. The security of the company is of the utmost importance. I hope this information serves you well. Thank You.

**References**

*256-Bit Encryption*. Techopedia.com. (n.d.). Retrieved November 21, 2022, from <https://www.techopedia.com/definition/29703/256-bit-encryption>