****

# 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** | **10/22/2022** | **Tam Phan** |  |

## 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.

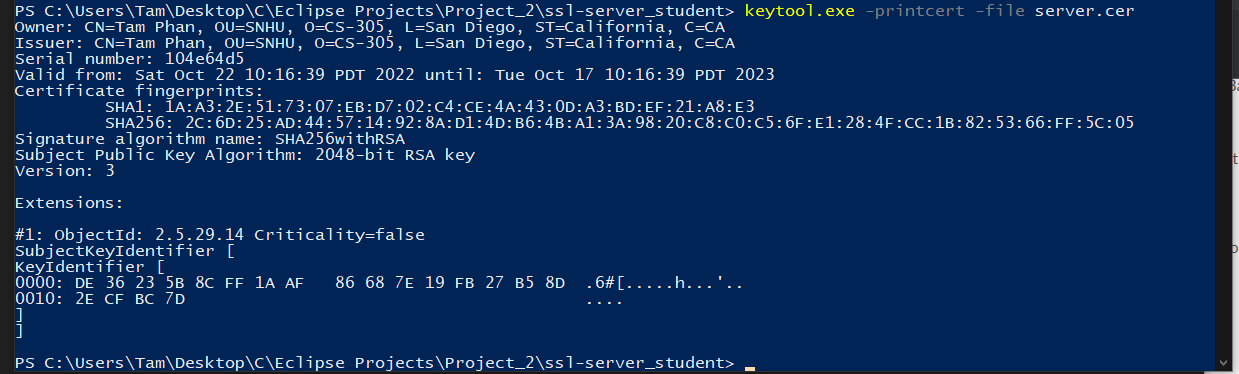
## Developer

Tam Phan

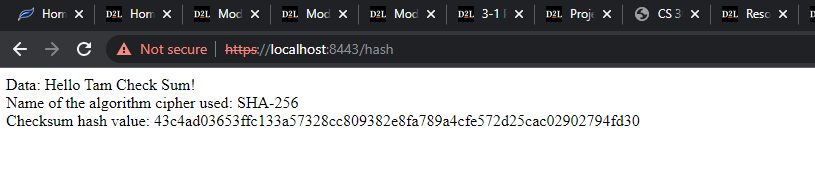
## Algorithm Cipher

SHA-256 is the most popular cipher to use, backed by the U.S. government since it’s known for no vulnerabilities has been found. The hash will produce a 256 bits long value and will be decrypt with a matched keystore. The purpose of this cipher is to verify data integrity, and prevent certain alteration to the original data.

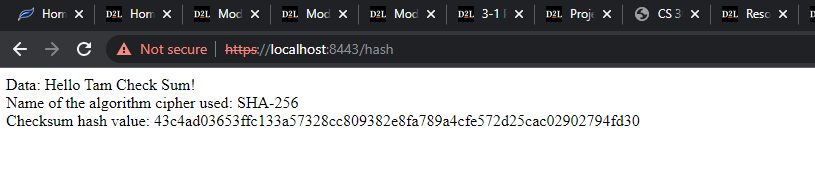
## Certificate Generation

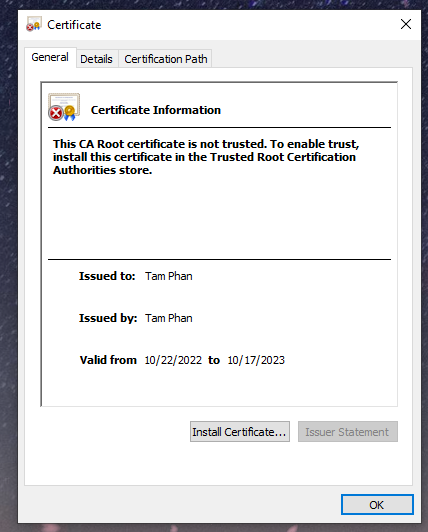


## Deploy Cipher

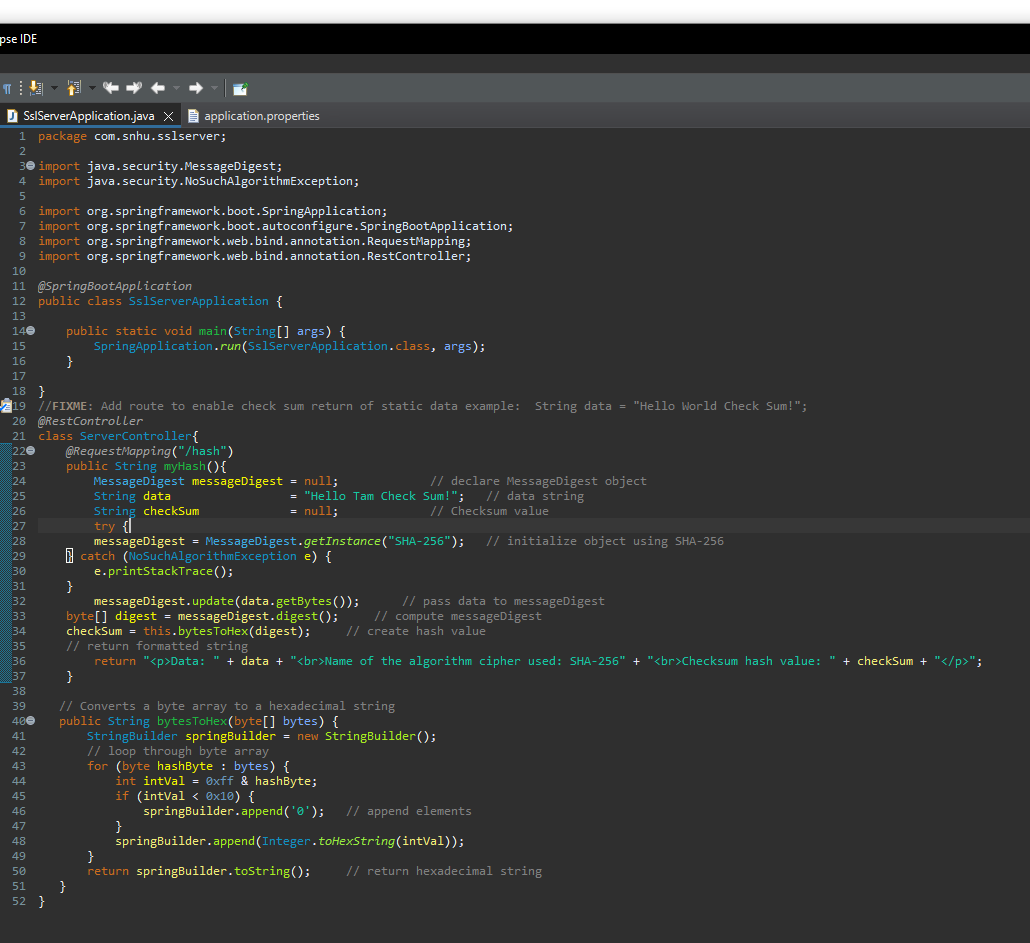


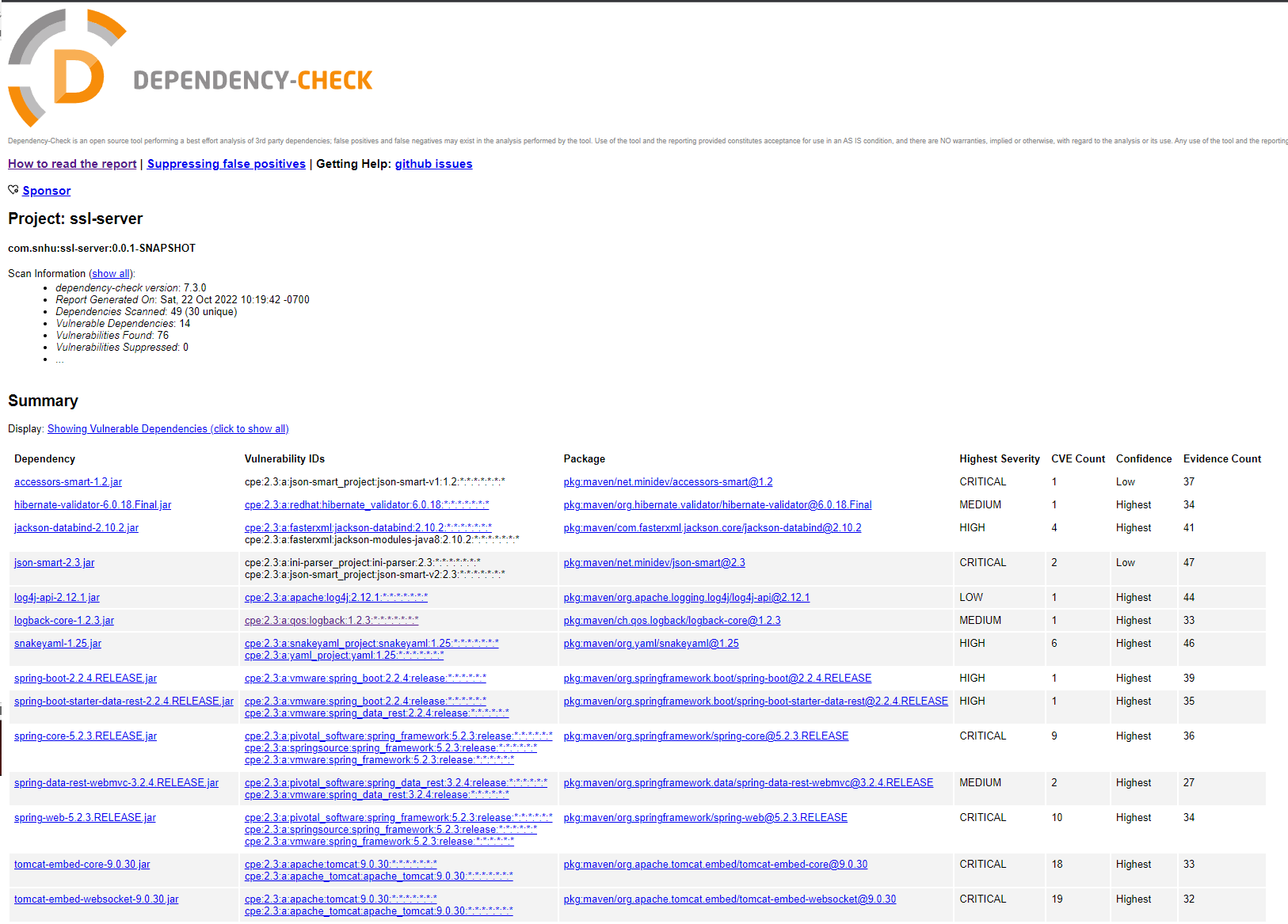
## Secure Communications



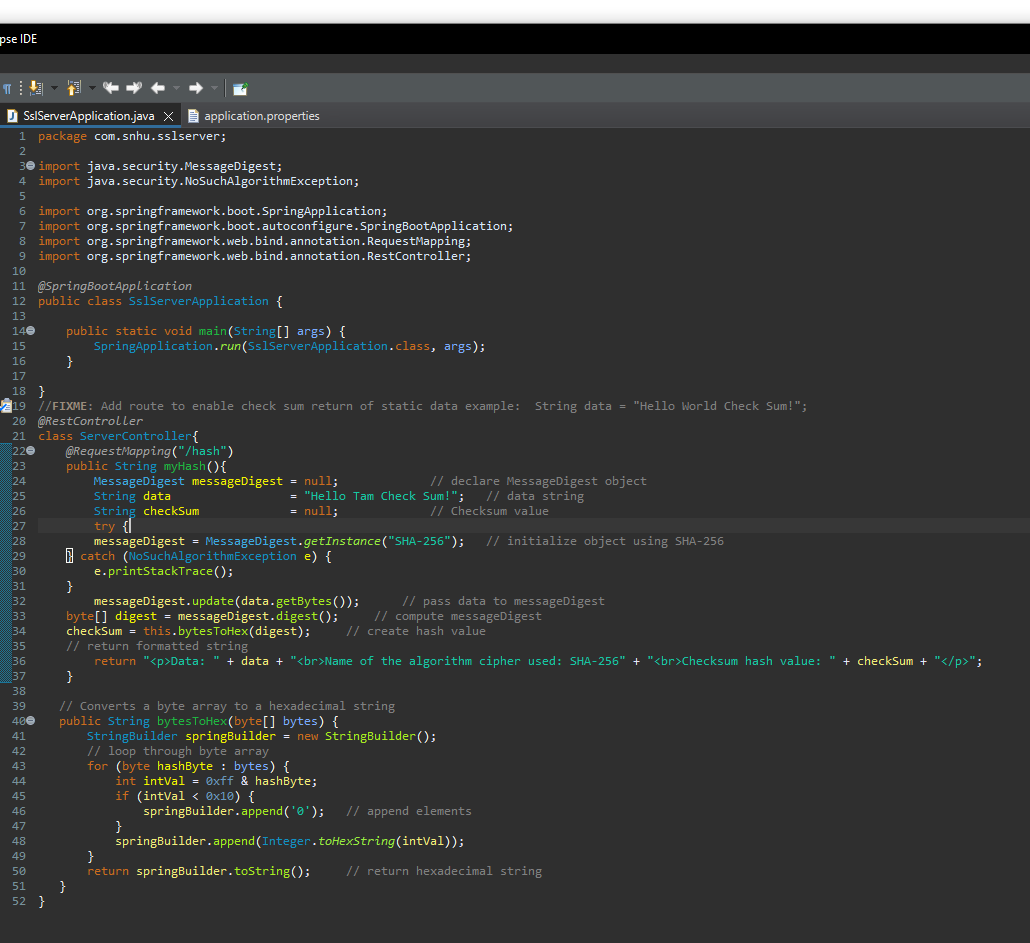


## Secondary Testing





## Functional Testing



## Summary

The code has been refactored to avoid collision by generating a checksum verification for a sample data string which is “Hello Tam Check Sum!” from implementing SHA-256 algorithm. This method also applies to the cryptography from vulnerability assessment process flow for encryption use to make the original data secure and protected from any alterations.

## Industry Standard Best Practices

Best practice is to update every dependency to the latest stable version to avoid any vulnerabilities while maintaining the code and apply best practice from the vulnerability assessment process flow