****

# 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** | **12/15/2024** | **Jime Balvin** |  |

## 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

Jime Balvin

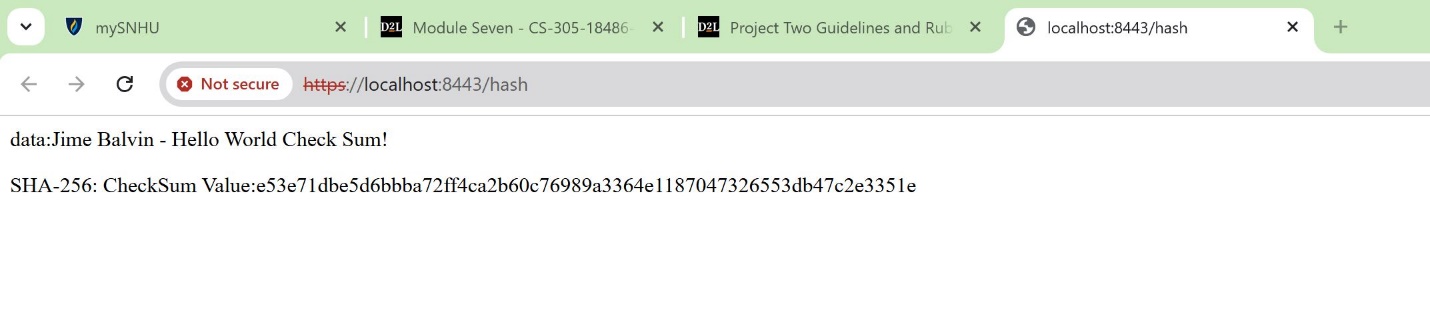
## Algorithm Cipher

The recommended Algorithm Cipher is AES. It is a symmetric encryption algorithm characterized by its strength and efficiency which makes it suitable for encrypting sensitive data. Combined with AES, it is recommended to used SHA-256 for hash functions since it is collision resistant ensuring that no two different inputs produce the same hash value (maintains integrity and security o the verification process). The used of random numbers ensures that keys are strong and less vulnerable to attacks; and the use of symmetric keys makes the process faster as the same key is used for encryption and decryption.

Encryption algorithms started with simple methods like Caesar cipher, then in the 1970s a new algorithm called DES (Data Encryption Standard) was introduced. However, once DES became vulnerable in the 1990s, the need for a more secure standard lead to the creation of AES which was adopted in 2001 as a stronger and more secure algorithm. AES remains as one of the most secure encryption methods but as the threats and technology advances, the improvement of encryption methods needs to keep growing.

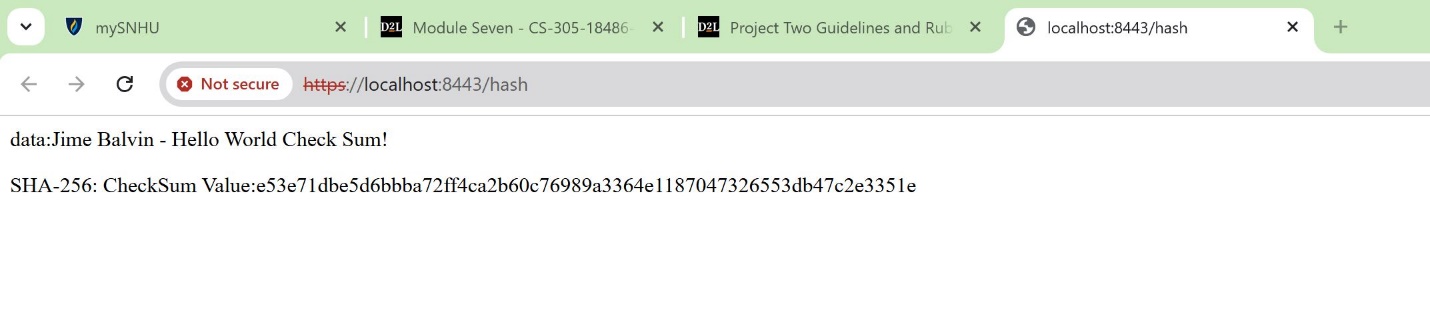
## Certificate Generation

## Deploy Cipher



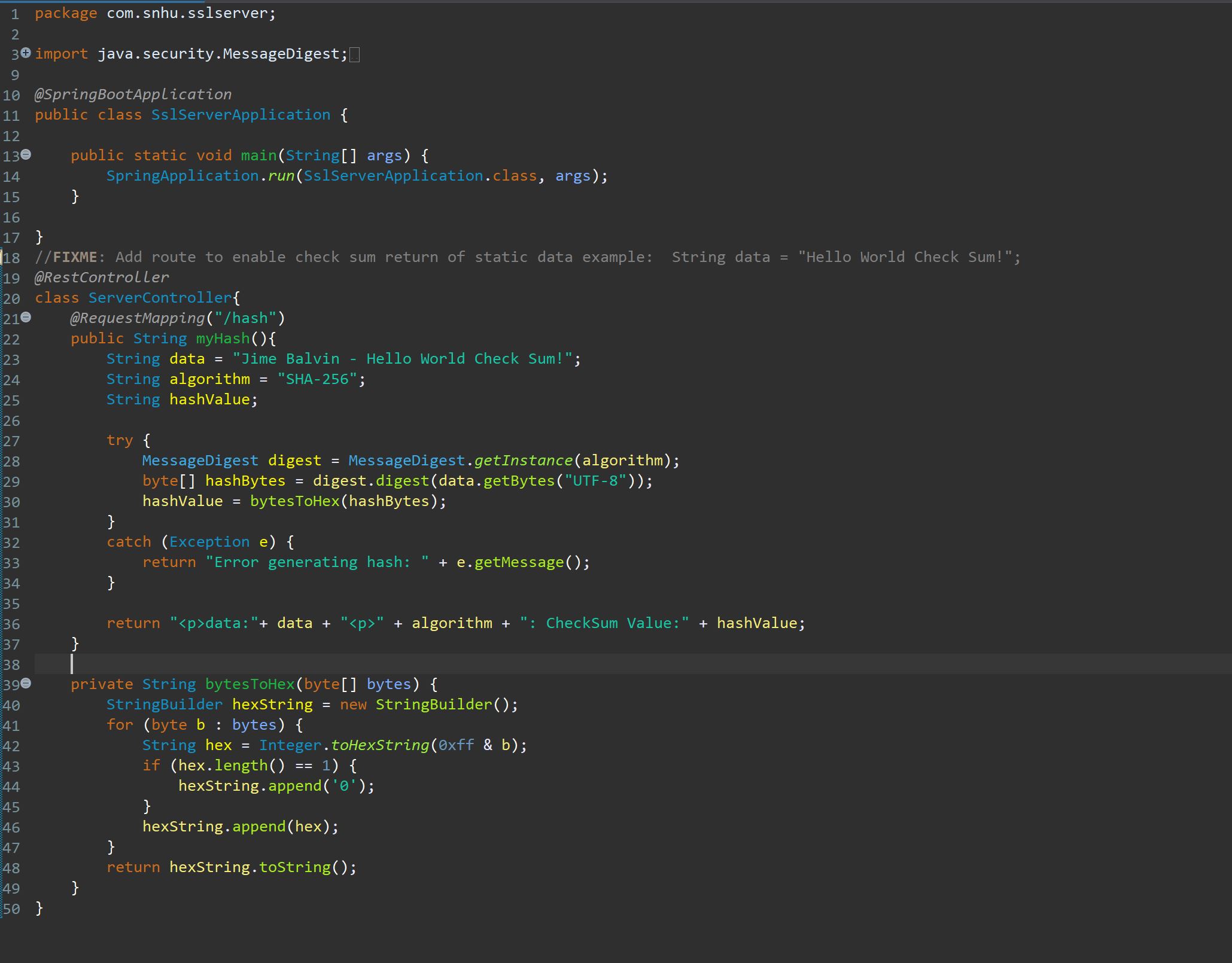
## Secure Communications

## Working but showing not secure because it is self-signed.

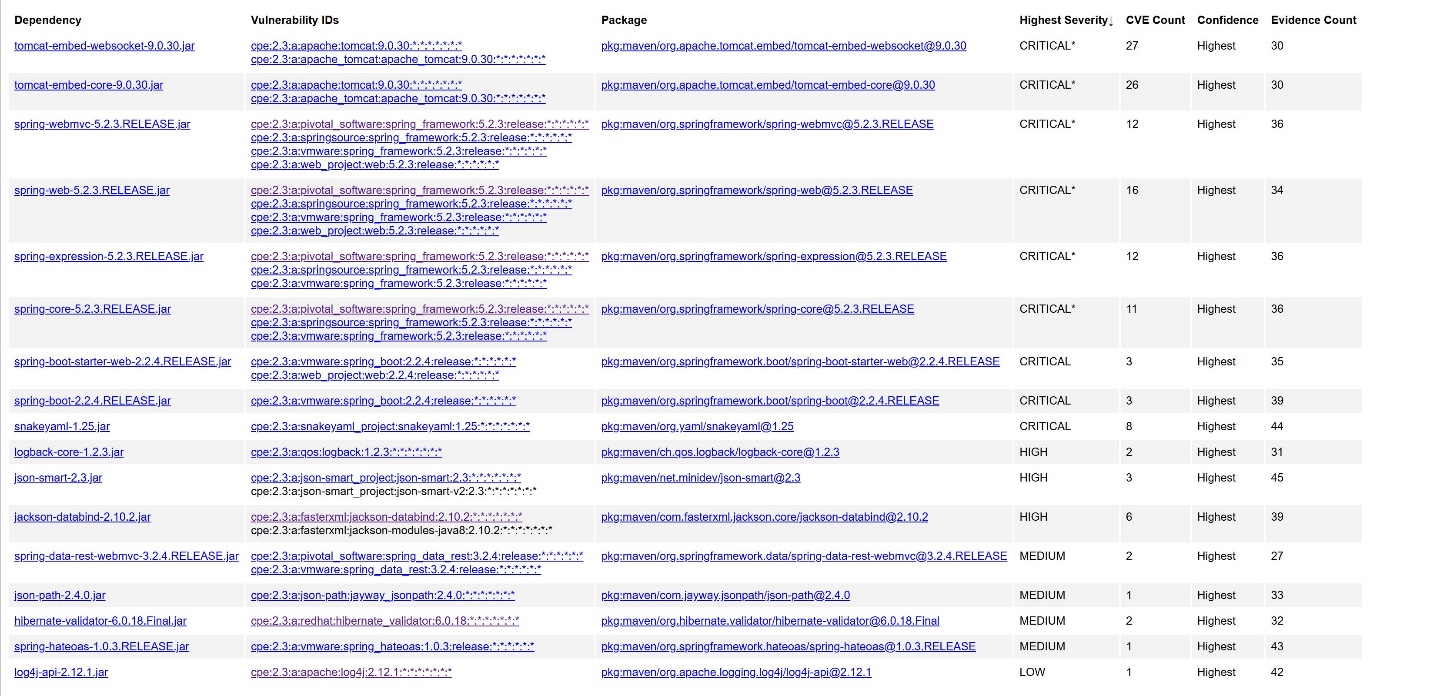


## Secondary Testing

Refactored code executed without errors

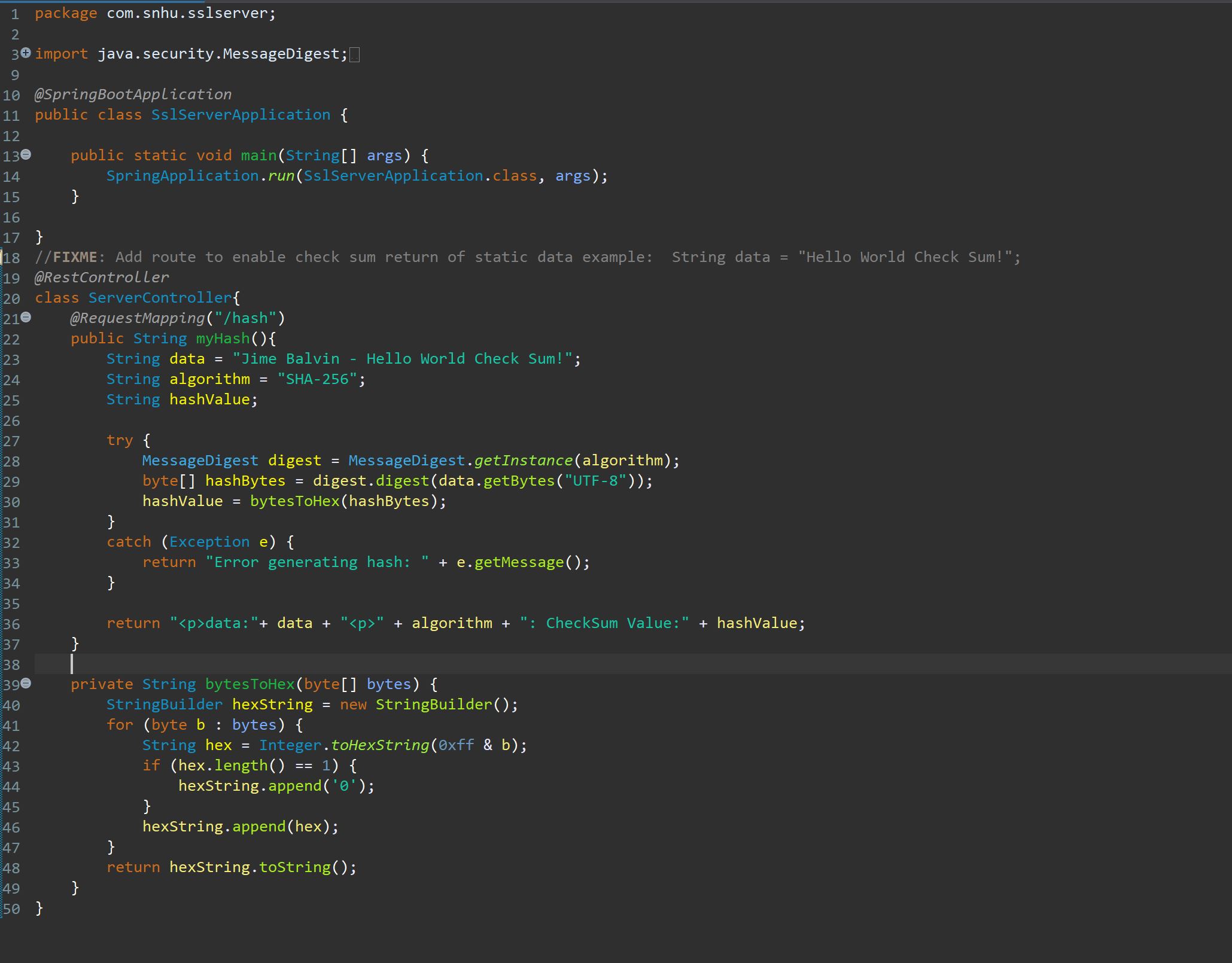


Dependency-check report.



## Functional Testing

Refactored code executed without errors.



## Summary

Implementation of checksum with SHA-256 hashing that provides data integrity and authenticity. Error handling implementation that avoids leaking sensitive information. Data correctly encoded into bytes using UTF-8 avoiding encoding mismatches. Code implemented on a modular and maintainable approach.

## Industry Standard Best Practices

In order to secure coding and mitigate known security vulnerabilities, industry standard best practices were applied like secure hashing, effective error handling, proper data encoding and modular code design. Using these best practices is beneficial for Artemis Financial since more than secure code, it contributes to its reputation and how their clients feel about a secured and reliable company handling their finances. As well as staying compliant and mitigating financial risks. Deliver high value means delivering high business.