****

# 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** | **8/12/2024** | **Mohammed Khan** |  |

## 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

Mohammed Khan

## Algorithm Cipher

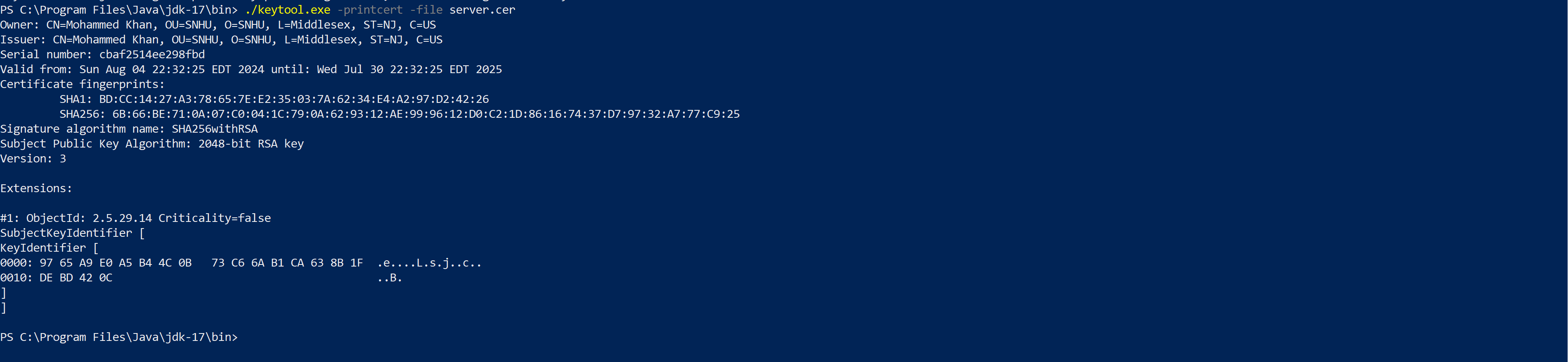
## Provide a brief, high-level overview of the encryption algorithm cipher. AES is a popular encryption method used to protect data. It’s fast, reliable, and works well on different devices. AES uses the same key to encrypt and decrypt data, which makes it easy to use but requires careful handling of the key to keep it safe.

## Discuss the hash functions and bit levels of the cipher. For verifying data, SHA-256 hashing would be a strong and trusted method that creates a unique 256-bit hashing from any input data. This hash is like a fingerprint for the data which makes sure that even a small change in the input will result in a completely different hash.

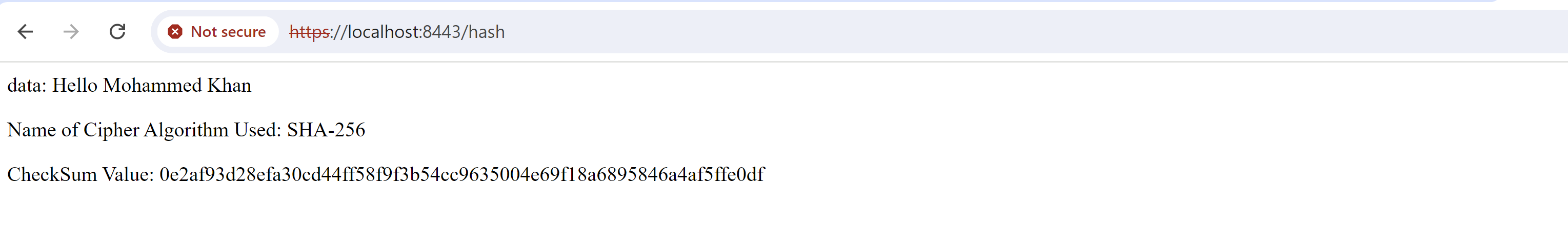
## Explain the use of random numbers, symmetric versus non-symmetric keys, and so on. Random numbers are essential in encryption to make keys unpredictable, which adds an extra layer of security. Symmetric Keys AES uses symmetric keys, meaning the same key is used for both locking and unlocking the data. This method is fast and efficient which makes it ideal for encrypting large amounts of data. Asymmetric Keys unlike AES, asymmetric encryption uses two different keys, a public key for encryption and a private key for decryption. This method is slower but is often used to securely exchange the symmetric key.

## Describe the history and current state of encryption algorithms. Over time, encryption methods have improved as computers have become more powerful. Older methods like DES were eventually replaced because they became vulnerable to attacks. AES was introduced in 2001 and has since become the global standard for encryption which is widely trusted and used around the world.

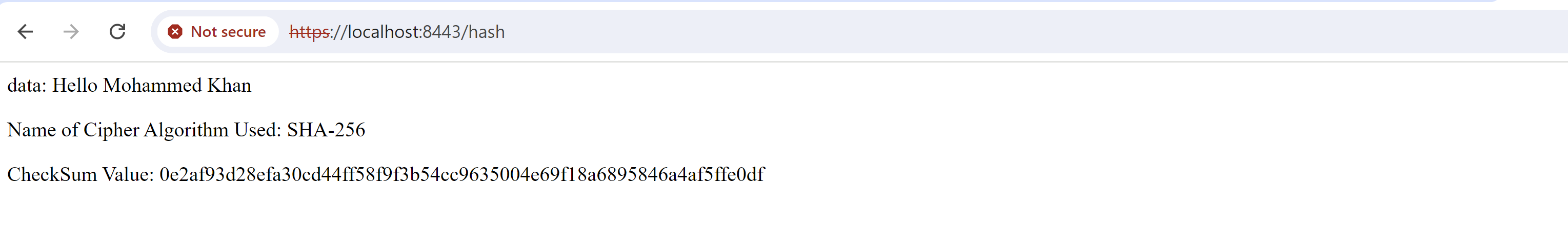
## Certificate Generation



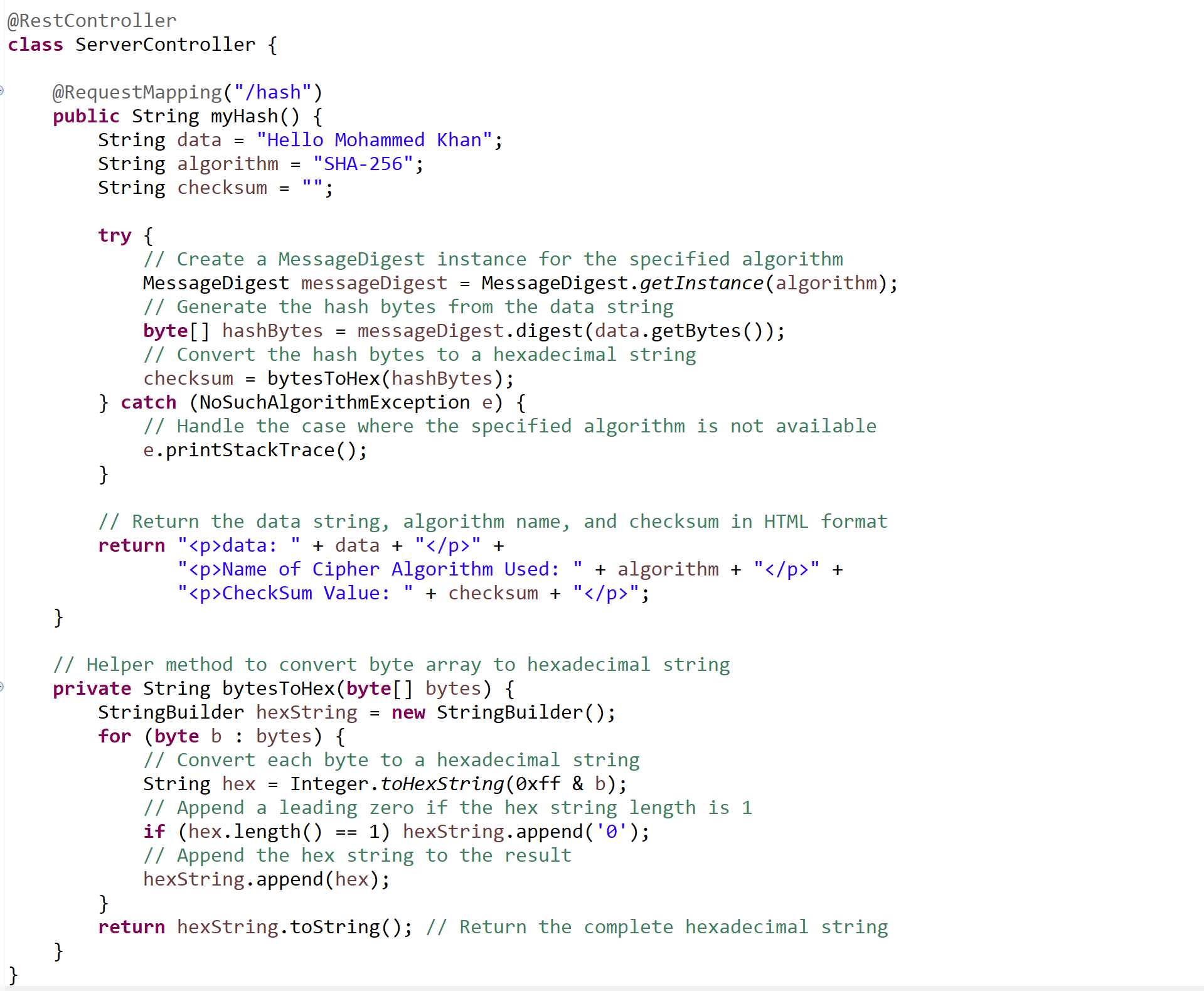
## Deploy Cipher

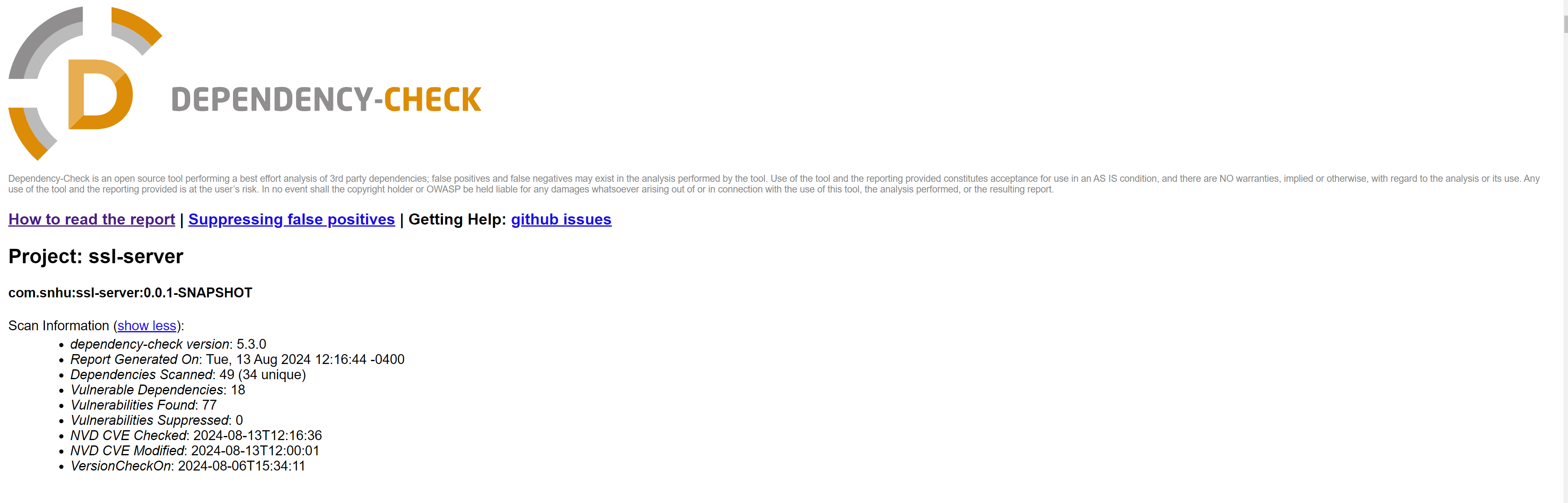


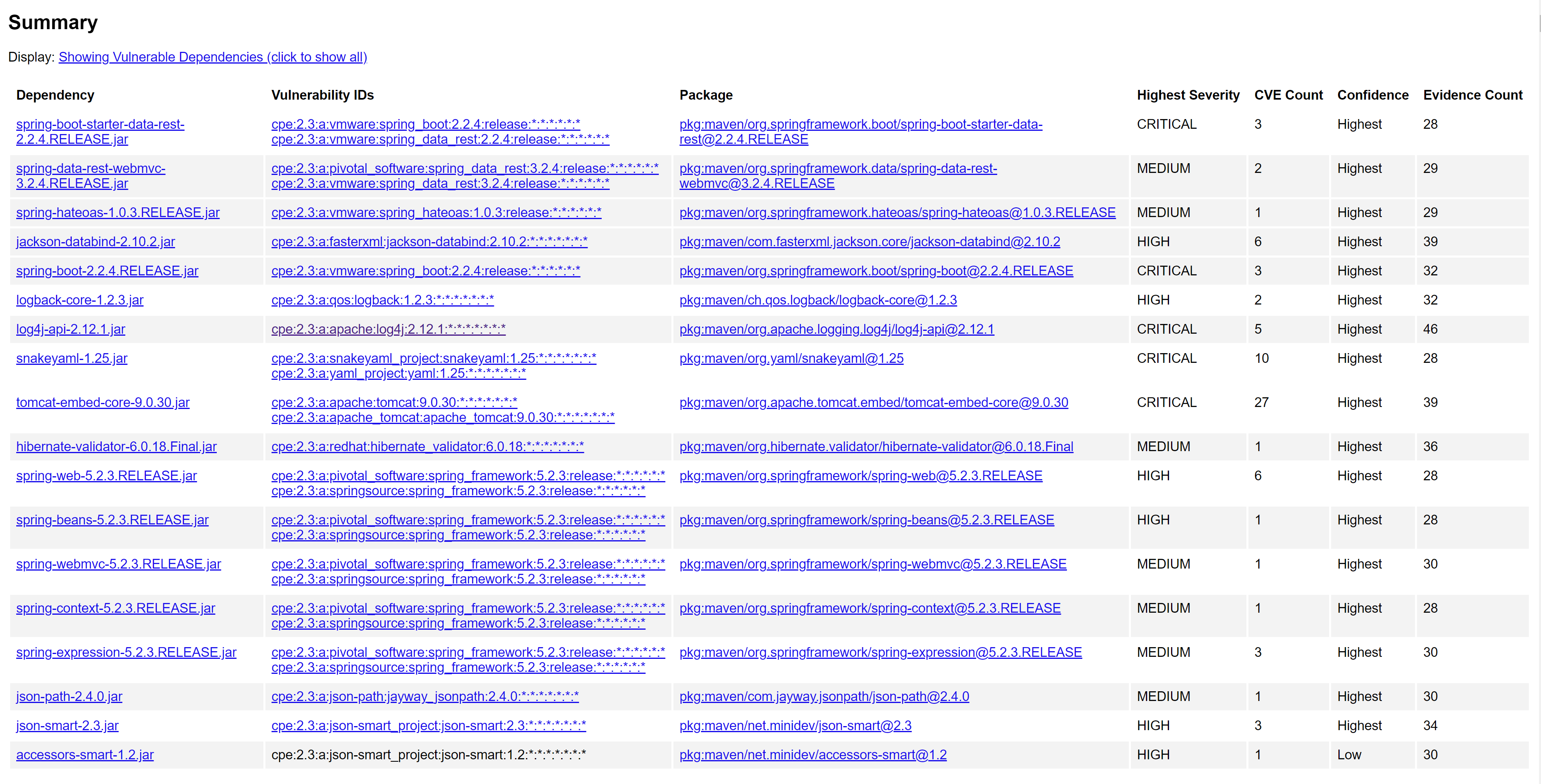
## Secure Communications



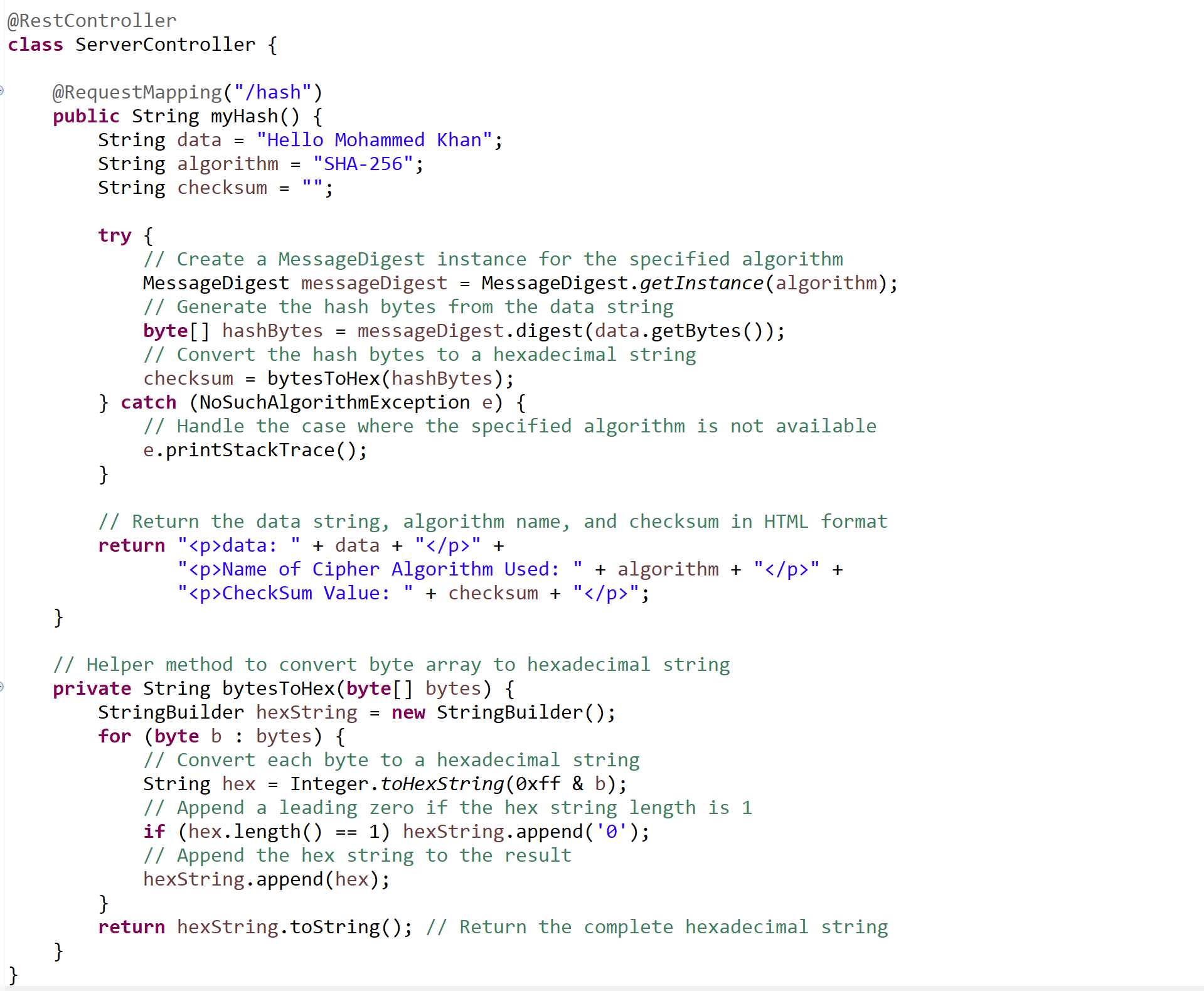
## Secondary Testing







## Functional Testing



## Summary

I updated the code to improve security by adding SHA-256 hashing encryption and secure HTTPS communication. These changes protect the data from being tampered with or accessed by unauthorized users which makes sure it stays safe both when stored and during transmission. These improvements help the company protect sensitive financial information. To maintain this security, it's important to keep the software updated by managing encryption keys carefully and regularly test for security issues.

## Industry Standard Best Practices

To keep data secure, it's important to follow industry practices such as use strong encryption like AES, keep software up to date, and control access with methods like multi-factor authentication. Regularly test for security issues and have good logging to spot and respond to threats. Also, protecting data integrity with hashing and make sure you have backups in case of problems.