****

# 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** | **6/25/2023** | **Chad Nadeau** |  |

## 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

Chad Nadeau

## Algorithm Cipher

In this scenario, I believe SHA-256 would be the most beneficial. I believe this would be the most beneficial because SHA-256 is considered secure against known cryptographic attacks. It is designed to be resistant to collision attacks, where two different inputs produce the same hash output. While no cryptographic algorithm is completely immune to future attacks, SHA-256 has withstood rigorous review and analysis from the security community. The hash function is optimized for modern computer architectures and can be implemented efficiently in both software and hardware. Its efficiency makes it suitable for various applications that require hashing, such as digital signatures, password hashing, and data integrity checks.

The use of random numbers SHA-256 provides a strong cryptographic strength with a 256-bit hash output. The 256-bit length provides a large address space, making it extremely difficult to find two inputs that produce the same hash value or reverse engineer the original input from the hash output. Symmetric encryption is a type of encryption where only one private key is used to both encrypt and decrypt electronic data, whereas asymmetric encryption uses two keys, one private and one public key.

Encryption algorithms have been around for thousands of years, for example, the Caesar cipher is known as an early form of encryption as it involved substitution and transportation of letters to protect sensitive information. In its current state, encryption algorithms are constantly evolving to stay relevant and avoid attacks from quantum computers. The current standard for encryption, AES, is widely regarded as secure and is extensively used for symmetric encryption. As for asymmetric encryption, RSA and ECC remain popular choices. Additionally, the adoption of secure cryptographic protocols, such as SSL/TLS for secure communication over the internet, has become widespread.

## Certificate Generation

Insert a screenshot below of the CER file.

A picture containing text, screenshot, font

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated with medium confidence

## Secure Communications

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

A screenshot of a computer

Description automatically generated with medium confidence

I tried everything but I could not get my certificate to validate and show as properly secure.

## Secondary Testing

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

A screenshot of a computer

Description automatically generated with medium confidence

## Functional Testing

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

A screenshot of a computer program

Description automatically generated with medium confidence

## Summary

I have made improvements to my code by incorporating a secure RestController, which serves as the protected controller for my hash RESTful operations. The ServerController class addresses the issues identified in the vulnerability assessment diagram. To enhance the security of the application, I have opted to utilize the SHA-256 hashing cipher, which offers a high level of security and minimizes the risk of collisions. To effectively maintain the current security of the application, I recommend performing semi-frequent dependency checks. This practice will ensure that the application remains up to date and protected against potential vulnerabilities, safeguarding the company's sensitive data. Furthermore, it is advisable to include the latest versions of plugins in the pom.xml file, as this will ensure that the application benefits from the most recent enhancements and has the highest level of security.

## Industry Standard Best Practices

Many industries have specific regulations and standards that require adherence to secure coding practices. By following these industry standards, the company ensures compliance with legal and regulatory requirements, avoiding penalties, legal complications, and reputational damage. Along with that, industry-standard practices address known security vulnerabilities, ensuring that potential risks are identified and mitigated effectively. By proactively applying these practices, the company minimizes the chances of data breaches, cyberattacks, and financial losses associated with security incidents. By following industry best practices, such as implementing secure authentication and encryption mechanisms, the company's sensitive data is protected against unauthorized access or attacks. This helps to maintain the trust of customers, partners, and stakeholders.