****

# 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** | **10/15/2023** | **Winnie Kwong** | **CS 305 project 2** |

## Client



## Developer

Winnie Kwong

## Algorithm Cipher

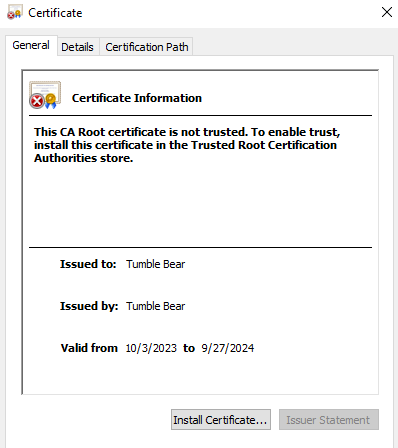
In software security, collision attacks find identical inputs of an encrypted hash to challenge one’s security. If the attack is successful, the attacker can create malicious activities, such as fraudulent data, that can diminish the company’s integrity and authenticity. One of the best practices I recommend for Artemis Financial is the SHA 256 algorithm that falls under the Secure Hash Algorithm (SHA) 2 family. According to Jena, SHA 256 was created in 2001 because its predecessor, SHA 1, became more accessible to decipher as technology advanced. (Jena, 2023, para 6). SHA 1 consisted of an output of 160 bits, making it more vulnerable to attacks, whereas SHA 256 has an output size of 256 bits, making it much more challenging to decode.

By using SHA 256, it is nearly impossible to crack because of the blockchain that uses the combination of hashing and bit levels. Hashing is created by converting data into plaintext to make the key-value pairs in the hash table. Like a digital signature, without access to the signer’s private key, the encrypted data becomes unreadable, and it is difficult for unauthorized users to enter the index and obtain sensitive information within the signer’s data storage. (BlockChainSentry, 2022, para 2). However, each hash size will depend on the bit levels of the cipher. With the SHA 256, since there are 256 bits, this means there are or 1.1579e +77 possibilities when attempting to decode the encryption. Due to the complexity of SHA 256, attackers could not quickly discover the code in a reasonable amount of time.

When the hash algorithm is converted, users will see a data string consisting of various numbers and characters with a checksum of 64 lengths. Although the checksum looks like a bunch of random numbers, it is derived from another block of digital data that can be parsed into 512-bit blocks to concatenate the key value. (Sunnatovich, 2019, para 4). Even though SHA 256 is a hash function, it can be combined with a signing algorithm such as a symmetric, asymmetric, or hybrid approach to create a signed token for the application. A symmetric key means having a single cryptographic key to encrypt or decrypt. If the key is compromised, all communication will be compromised. If an asymmetric key is used, there are two private and public keys. One is to encrypt while the other decrypts. Public keys are bound to certificate authorities and are distributed for anyone to access, while the private key, meant to be a secret, is to create the signature to validate authentication.

According to Sidhpurwala, the earliest form of encryption can date as far back as 1900 BC in the main chamber of the tomb of the nobleman Khnumhotep II in Egypt. Egyptians used hieroglyphics to record important events such as wars and stories of their gods and Pharaohs. (Sidhpurwala, 2023, para 2). Hieroglyphics have influenced society to create secret messages to transfer data. Today, the Advanced Encryption Standard (AES) is the algorithm trusted and used by the U.S. Government and other organizations. (Arcserve, 2023, para 14). With AES, it isn't easy to decipher due to its combinations of 128, 192, or 256-bit symmetric algorithms.

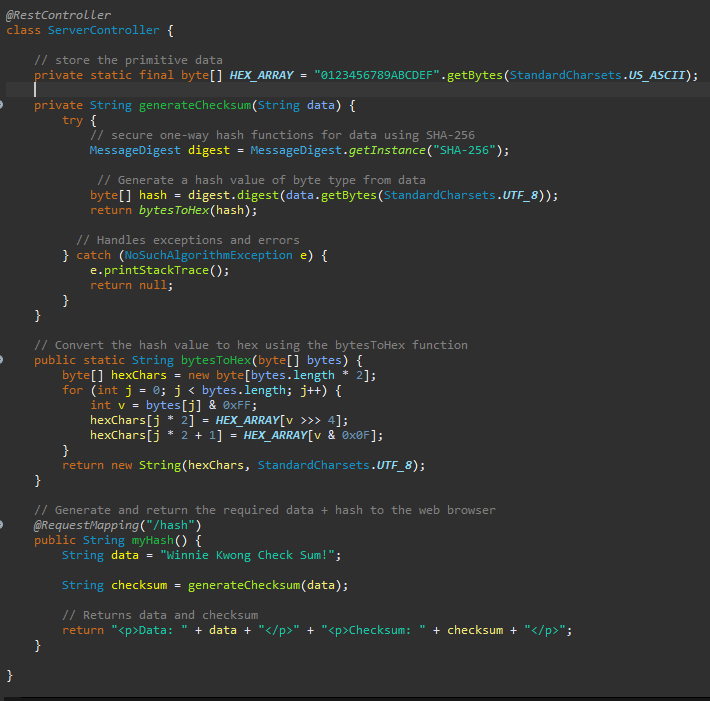
## Certificate Generation



A computer screen with text on it

Description automatically generated

## Deploy Cipher



## Secure Communications

A screenshot of a computer

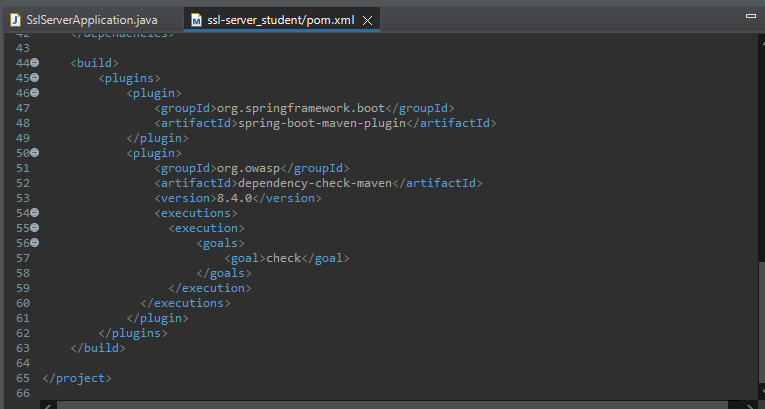
Description automatically generated

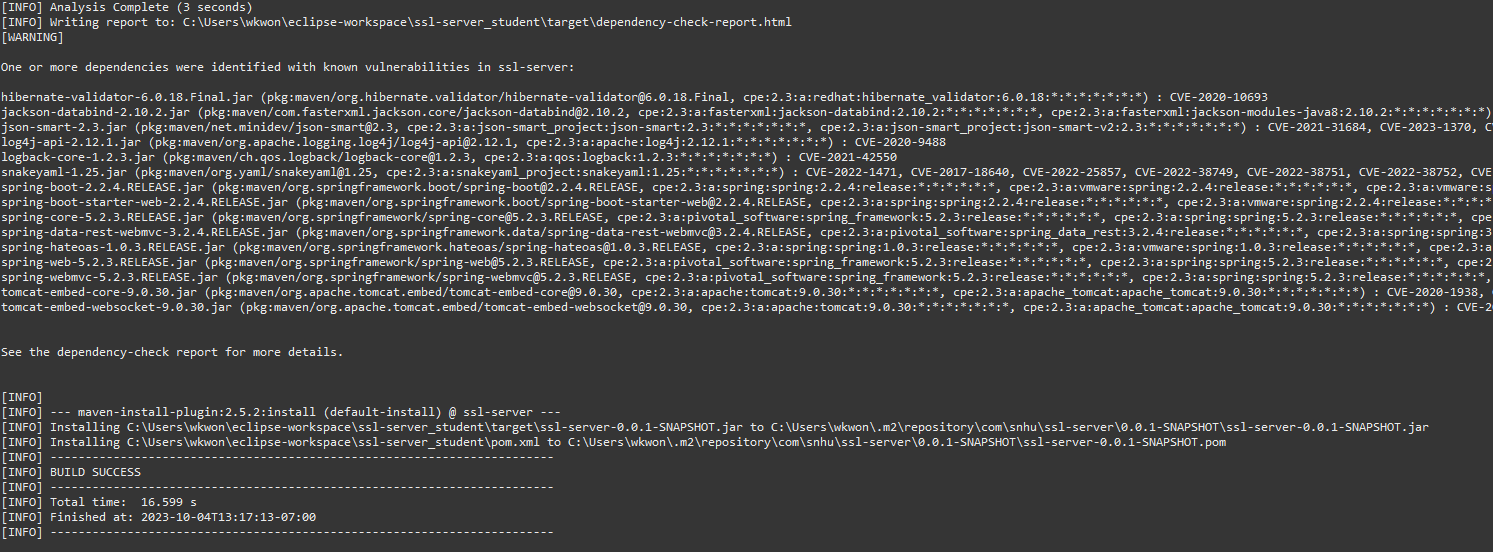
A screenshot of a computer

Description automatically generated  
  
A screenshot of a computer

Description automatically generated

## Secondary Testing





A screenshot of a computer

Description automatically generated

## Functional Testing

A screen shot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

## Summary

Refactoring a code has many benefits, such as readability, enhancing performance, and reducing complexities. However, compiling for security testing protocols helps developers identify bugs or other vulnerabilities within the software. According to Pankaj, RestController would create RESTful web services using Spring MVC and handle all REST APIs such as GET, POST, Delete, and PUT requests. (Pankaj, 2022, para 1). The RestConroller is a security benefit because it helps to authenticate before it can be executed. Since the system will require authentication first, the system would be able to determine if a user would be allowed to access the system, preventing unauthorized users. Including a checksum also helps with security because it acts similar to a fingerprint when comparing files during the scanning phase and detecting errors in the system. Also, within the pom.xml file, I have updated the OWASP Maven Dependency to its most recent version. By having the most updated version, I can access new and improved functionalities that resolve any previous bugs or other issues within the system. If I continued to utilize an outdated version, I would be more at risk for malicious attacks and need more knowledge to fix security vulnerabilities. Refactoring the pom.xml file also helps assess vulnerabilities within the dependency check properly. An additional layer of security added was using a self-signed certificate. Self-signed certificates are signed digital certificates with a private key. Self-signed certificates help boost security by allowing the developer to examine the source code to ensure no vulnerabilities with the internal framework. Activating a self-signed certificate will enable HTTPS to be started with encryption and verification. Compared to HTTP, HTTPS is by far more secure to use because the communication between clients and the server is protected by encryption, making it difficult for an attacker to intercept. Without refactoring and additional layers of security, developers could be more at risk with code smells and even spaghetti codes.

## Industry Standard Best Practices

By utilizing best practices to meet the coding standards, developers can create quality codes that are consistent and efficient. With the guidelines that are set, developers would have codes that are clean and readable. A few best practices that were applied are:

* According to OWASP, input validation helps ensure data is functioning in the workflow to prevent malicious data from entering the database and malfunctioning the system. (Input Validation - OWASP Cheat Sheet Series, n.d., para 2). Input validation helps to maintain the software's application from security vulnerabilities such as SQL injection or buffer overflow attacks. Preventing security vulnerabilities assists the company's overall well-being by reducing the number of attacks from weak codes.
* Good code quality depends on whether the code is free of bugs or defects while also being available to increase the scope of the application and maintain comprehensibility. One of the best strategies to include is a code review to identify potential security issues that can occur. To improve the company's overall wellness, developers should use code review to detect errors early to avoid a hefty cost for mistakes.
* Utilizing the most current version when using third-party libraries and frameworks helps to regulate software updates and patches that can address security vulnerabilities and breaches. Ways to control updates and patches is to create an automated patch management that can scan, test, and install selected software updates and patches regarding the application. Maintaining up-to-date software and patches makes the company's overall well-being less at risk from attacks by identifying potential weaknesses within the infrastructure. Also, monitoring vulnerabilities can help fix security concerns before the application is deployed.
* Using secure network communication, such as HTTPS instead of HTTP, helps ensure the software is being deployed with the proper configurations. By using configuration management, it helps to reduce the risks of unauthorized users that can inflict malicious activities. Besides reducing unauthorized users, it helps build client trust when providing sensitive information to the company. Establishing trust with valued clients creates a positive relationship with the company and opportunities to grow.

**References**

Arcserve. (2023). 5 Common encryption algorithms and the unbreakables of the future. *Arcserve*. <https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future>

BlockChainSentry. (2022, October 26). *Hashing in blockchain?* BlockChainSentry. <https://blockchainsentry.com/blog/hashing-in-blockchain/>

GeeksforGeeks. (2022). Difference between controller and RestController annotation in spring. *GeeksforGeeks*. <https://www.geeksforgeeks.org/difference-between-controller-and-restcontroller-annotation-in-spring/>

*Input Validation - OWASP Cheat Sheet Series*. (n.d.). <https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html>

Jena, B. K. (2023, August 29). *A Definitive Guide to Learn The SHA-256 (Secure Hash Algorithms).* Simplilearn.com. <https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm>

Pankaj. (2022). Spring RestController. *DigitalOcean*. <https://www.digitalocean.com/community/tutorials/spring-restcontroller>

Sidhpurwala, H. (2023, January 12). A Brief History of Cryptography. *RED HAT BLOG*. <https://www.redhat.com/en/blog/brief-history-cryptography#:~:text=The%20first%20known%20evidence%20of,place%20of%20more%20ordinary%20ones>.

Sunnatovich, M. I. (2021, December 9). Use cases for hash functions or what is SHA-256? - Makhmud Islamov Sunnatovich - Medium. *Medium*. <https://medium.com/@makhmud.islamov/use-cases-for-hash-functions-or-what-is-sha-256-83036de048b4>