****

# 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** | **10-22-2024** | **Landon Phillips** |  |

## 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

Landon Phillips

## Algorithm Cipher

**Provide a brief, high-level overview of the encryption algorithm cipher.**

After reviewing Artemis Financial’s security needs for an appropriate encryption algorithm cipher to deploy, it has been concluded that the most suitable encryption algorithm to address the company’s security vulnerabilities is the Advanced Encryption Standard (AES) cipher with a 256-bit key length. Widely acknowledged for its security, this cipher safeguards sensitive information, including that of governments. “According to the US federal government, people should use AES when they are sending sensitive (unclassified) information.” (Mohn, 2023) AES offers the necessary level of protection to ensure the safety of financial records for the long term.

**Discuss the hash functions and bit levels of the cipher.**

The purpose of a hash function is to map a given data set into a fixed bit string or "hash." Hash functions are often used to verify that data has not been altered by comparing a hash to the original. If any data has changed, the hash will differ, indicating corruption. Bit levels refer to the length of the encryption key. The higher the bit level (like AES-256, i.e., “256”), the stronger the security level.

**Explain the use of random numbers, symmetric versus non-symmetric keys, and so on.**

In encryption algorithms and other forms of encryption, random numbers are used to generate secure encryption keys. The "randomness" is crucial because it makes the keys unpredictable and prevents attackers from guessing them. Symmetric keys are used for encryption and decryption, which can be fast, but protecting the key is imperative. Asymmetric keys use a pair of keys, a public and private key, for decryption. This approach can be more secure but also more computationally expensive.

**Describe the history and current state of encryption algorithms.**

Encryption has been used throughout history, with evidence showing that humanity has used encryption to secure messages. "Julius Caesar favored a substitution cipher to give orders and receive updates from his generals in the field" (Encryption: The Past, Present, and Future - AXEL.org, 2021). This is known as Caesar's cipher, but with technological advancements, this cipher is no longer recommended. In the 1970s, DES (Data Encryption Standard) became the adopted standard for encryption. However, with the advancement of computers, DES could be hacked in no time. AES is now the modern standard for the U.S. government. As time passes, computers and technology will continue to advance, requiring encryption to evolve as well.

## Certificate Generation

A screenshot of a computer program

Description automatically generated

## Deploy Cipher

A screenshot of a computer

Description automatically generated

## Secure Communications

A screenshot of a computer

Description automatically generated

## Secondary Testing

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

A screenshot of a computer

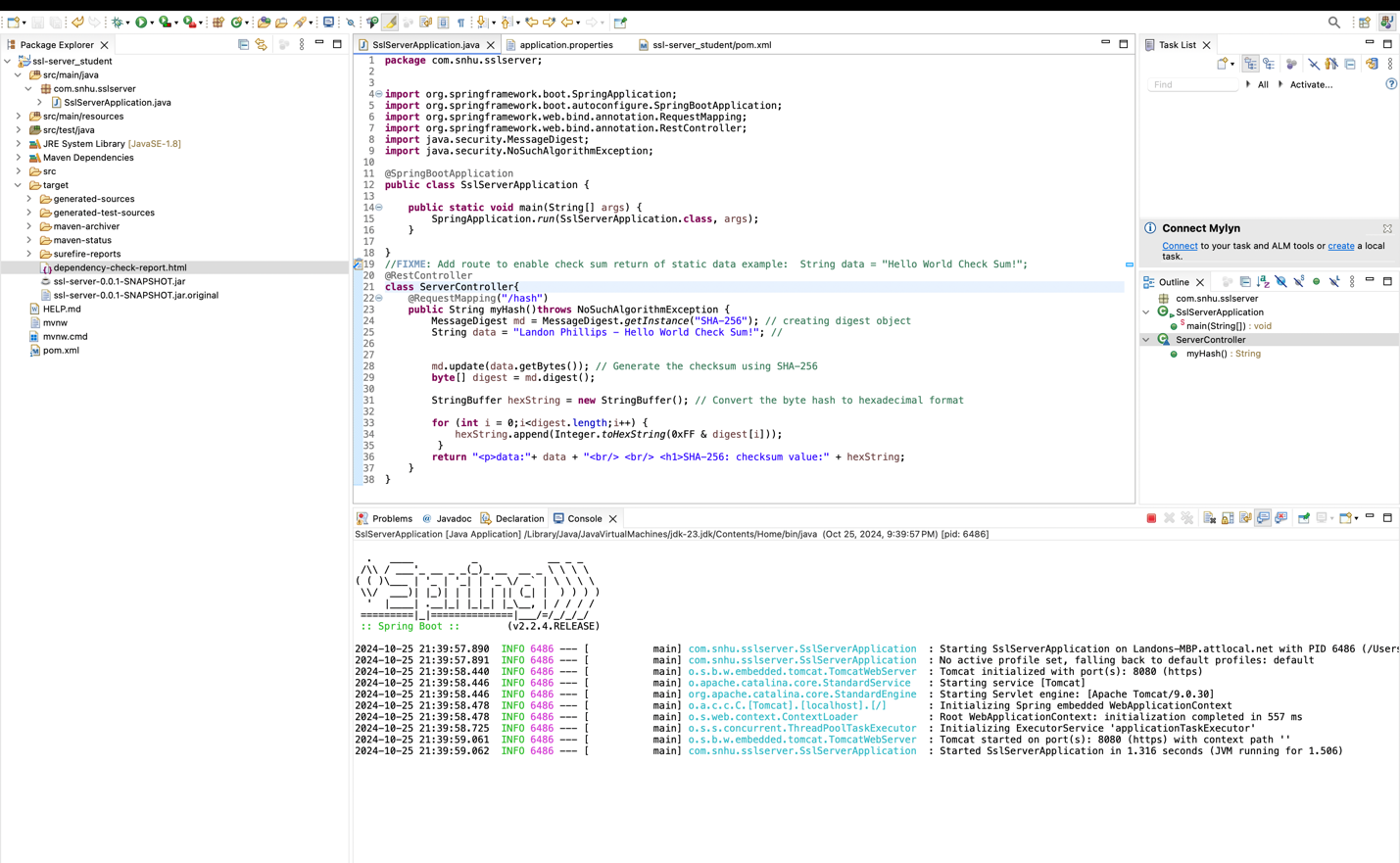
Description automatically generated

A screenshot of a checklist

Description automatically generated

## Functional Testing

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



## Summary

**Refer to the vulnerability assessment process flow diagram in the Supporting Materials section. Highlight the areas of security that you addressed by refactoring the code.**

During refactoring, I added a new REST endpoint in the ServerController class to generate a SHA-256 checksum for the static string "Landon Phillips - Hello World Check Sum!" This ensured secure user input by not allowing it. I created a new route "/hash," ensuring secure API interaction, and ran a dependency check to confirm no new vulnerabilities were introduced. I implemented cryptography utilizing a secure hashing algorithm and checksum verification to ensure the data has not been tampered with. Additionally, I conducted a thorough review of the code, ensuring high code quality and practices.

**Discuss your process for adding layers of security to the software application.**

To add security layers to the software application for Artemis Financials, I applied SHA-256 hashing to verify data integrity. After refactoring the code to ensure proper coding practices, I also ran a dependency check to assess any new vulnerabilities. This confirms secure coding protocols on top of verifying data integrity, creating multiple layers of security. Additionally, changing the protocol to HTTPS instead of using HTTP added another layer of security. This process of adding layers of security can ensure a secure application over the long run.

## Industry Standard Best Practices

## Explain how you used industry standard best practices to maintain the software application’s existing security.

## To uphold the current security standards of the software, I integrated SHA-256 for checksum generation, a solution that is widely acknowledged for its robust cryptographic hashing capabilities. This approach not only guarantees data integrity but also steers clear of introducing weak or outdated encryption techniques, adhering to industry best practices. By simply incorporating a REST endpoint and implementing a certificate to facilitate the use of HTTPS over HTTP, I effectively minimized code alterations and mitigated the risk of potential vulnerabilities. Furthermore, conducting a static analysis of dependencies aligns with industry standards, ensuring that any known vulnerabilities are addressed in a timely manner. By adhering to these best practices, we ensure that our software security remains current and anticipates the tactics of potential attackers.

## Explain the value of applying industry standard best practices for secure coding to the company’s overall well-being.

The primary advantage of adhering to industry-standard best practices lies in its ability to foster trust and ensure compliance. This approach not only illustrates a robust commitment to data protection but also instills confidence in customers, assuring them that their sensitive information is managed securely. Furthermore, implementing these best practices fortifies software against the ever-evolving landscape of cyber threats over the long run. It also facilitates compliance with regulatory demands, which are frequently shifting. By abiding by these standards, companies can enhance their reputations, thereby attracting new customers and investors. Ultimately, the integration of these practices not only secures the application but also contributes positively to the overall health of the organization.

**References:**

*Encryption: the past, present, and future*. (2021, May 28). https://www.axel.org/2021/05/28/history-of-encryption/

Mohn, E. (2023). Advanced Encryption Standard (AES). *Salem Press Encyclopedia of Science*.

Phillips, L. (2024). Algorithm Cipher. [unpublished manuscript, Southern New Hampshire University].