****

# 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** | **08/13/2024** | **Jasper Conneway** |  |

## 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

Jasper Conneway

## Algorithm Cipher

Artemis Financial wants to add a file verification step to its web application to ensure secure communications. It is recommended that AES (Advanced Encryption Standard), an encryption algorithm cipher, be deployed to meet this requirement. Further, AES shall be paired with SHA-256 as it will give this business the best security possible. AES can provide strong encryption, key management, and layered security that is regularly updated. AES is known for its security and speed. It is symmetric because the same key encrypts and decrypts the data it protects. It uses the SPN (substitution permutation network) algorithm by encrypting plaintext into ciphertext with multiple rounds of substitution and permutation. AES has different key lengths: 128-bit, 192-bit, and 256-bit. AES was built not to be susceptible to collisions.

SHA-256 is a cryptographic hash function with a key length of more than 128 bits is not susceptible to collisions and protects sensitive data. This cryptographic hash function will provide this business with the best checksum verification program possible.

Encryption algorithms first appeared in the “Old Testament of The Bible circa 500-600 B.C” (*Encryption: The past, present, and future* 2021). The encryption used was a substation cipher. Today, encryption algorithms are mathematical equations or random number algorithms that protect information more securely.

## Certificate Generation

A screenshot of a computer

Description automatically generated

A screenshot of a certificate

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

A screenshot of a computer

Description automatically generated

## Summary

The Code Base was refactored and complied with security testing protocols. There is now a RestController class and a checksum verification. This will ensure secure communication. Application properties were updated with the self-signed certificate. The SslServerApplicationTest class annotation now includes the SslServerApplication.class. The Spring Framework start parent was updated to 3.2.2, Java library to version 17, 'com.snhu.ssl-server' to 'com.snhu.sslserver', Jackson databind was updated to version 2.17.2, JSON was updated to version 2.9.0, and the dependency check is the latest version. All these code updates ensure fewer vulnerabilities and will need to be frequently checked.

## Industry Standard Best Practices

Industry Standard Best Practices are beneficial for secure coding to mitigate known security vulnerabilities. Input was validated to prevent attacks like SQL Injection. Checksum verification helps implement authentication and the application properties secures communication. Updating to more recent versions reduces bugs and vulnerabilities that may not have been patched in earlier versions. Error handling ensures these can’t be taken advantage of and do not leak sensitive information.

Industry Standard Best Practices are beneficial for the company’s overall well-being. It reduces attacks that can lead to financial loss, lawsuits, and a bad reputation. It can cost more to fix something than it does to prevent attacks. Using these standards gives our customers a reason to trust our company and are more likely to continue using our products.

References

*Advanced encryption standard (aes)questions and answers*. ADVANCED ENCRYPTION STANDARD (AES) Fact Sheet. (n.d.). <https://csrc.nist.rip/encryption/aes/aesfact.html>

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

IToolkit. (2023, August 23). Does AES use SHA-256? https://itoolkit.co/blog/2023/08/does-aes-use-sha-256/

Rimkienė, R. (2022, August 29). *What is AES encryption and how does it work? | Cybernews*. What is AES encryption and how does it work? https://cybernews.com/resources/what-is-aes-encryption/

*Secure coding practices*. OWASP Secure Coding Practices - Quick Reference Guide | Secure Coding Practices | OWASP Foundation. (n.d.). https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/01-introduction/05-introduction