****

# 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** | **12/15/24** | **Jose Munoz** |  |

## 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

Jose Munoz

## Algorithm Cipher

* **Algorithm:** AES (Advanced Encryption Standard)
* **Bit Levels:** AES-256, providing high security.
* **Overview:** AES is a symmetric encryption algorithm widely adopted due to its speed and robust security. It encrypts data using a single key for both encryption and decryption.
* **Hash Function:** Utilizes SHA-256 for generating secure hashes.
* **Random Number Use:** Strong pseudo-random number generators ensure unpredictability.
* **Symmetric Key:** Easier to implement and manage compared to asymmetric encryption for bulk data encryption.
* **History and Current State:** Introduced as a replacement for DES, AES remains the gold standard in encryption.

## Certificate Generation

Insert a screenshot below of the CER file.

A screenshot of a certificate

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer program

Description automatically generated

## Secure Communications

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

A computer screen with white text

Description automatically generated

## Secondary Testing

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

A black background with white text

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

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

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

## Summary

**Refactoring Process:**

* Addressed vulnerabilities identified through the **Vulnerability Assessment Process Flow Diagram**.
* Applied layers of security, including input validation, secure error handling, and encryption.

**Security Enhancements:**

* Ensured compliance with industry standards through rigorous testing and secure coding practices.

## Industry Standard Best Practices

1. Followed **OWASP Guidelines** for secure coding.
2. Used **Java Keytool** for certificate generation.
3. Enforced **HTTPS** to secure communication channels.

**Value of Best Practices:**

* Mitigates risks of data breaches.
* Ensures client trust and application integrity.
* Aligns with industry benchmarks for secure software development.