****

# 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** | **10/21/23** | **Katelynn Thompson** |  |

## 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

Katelynn Thompson

## Algorithm Cipher

For Artemis Financials’ needs, I recommend deploying the Advanced Encryption Standard (AES) cipher for the file verification step in their web application. AES is a widely accepted encryption algorithm standardized by the National Institute of Standards and Technology (NIST) and is commonly used in modern cryptographic protocols (Crawford, 2019). It is a symmetric key cipher, meaning the same key is used for encryption and decryption. The AES algorithm uses a block cipher, which encrypts data in fixed-size blocks of 128 bits. It supports three key lengths - 128, 192, and 256 bits, with 256 bits being the most secure option (Crawford, 2019). AES also incorporates hash functions, precisely the SHA-256 hash function, which generates a checksum for the transferred data. This provides an added layer of security and helps ensure the data's integrity during transmission. Random numbers are used by AES during the encryption process to generate the initial key and to create the so-called "subkeys" used in each round of encryption. In terms of history, AES was chosen as the replacement for the aging Data Encryption Standard (DES) in 2001 after a rigorous selection process that involved many different encryption algorithms. Since then, AES has become the de facto standard for encryption and is widely used in many industries, including finance, healthcare, and government (Kantarcioglu, n.d.). In summary, AES is a highly secure and widely accepted encryption algorithm that would be a good choice for Artemis Financials’ file verification step. It uses symmetric key encryption, supports different vital lengths, incorporates hash functions for data integrity, and uses random numbers for added security.

## Certificate Generation

Insert a screenshot below of the CER file.

A black screen with white text

Description automatically generated

A screenshot of a certificate

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

## Secure Communications

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

Struggled to make the webpage secure even though the certificate was still valid:

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 screen shot of a computer

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 screen shot of a computer program

Description automatically generated A screen shot of a computer code

Description automatically generated

## Summary

Based on my analysis of the code, I have refactored it to comply with security testing protocols. I addressed various security concerns such as adding certificates and researching and implementing better coding practices that eliminate vulnerabilities. I used the Vulnerability Assessment Process Flow Diagram as a reference point to guide my work. In particular, I focused on input validation, access control, and error handling. To increase security measures, I implemented encryption and secure communication protocols. I also performed dependency checks to identify and address potential vulnerabilities. Our approach to secure software development involved a combination of preventive and detective measures to minimize the risk of security breaches.

## Industry Standard Best Practices

To ensure the code was up to the best standards, patching the software and systems is one of the best practices to maintain the security of the application. This helps to ensure that attackers cannot exploit out-of-date systems. I also implemented encryptions as well as recognizing the need for ensuring that users have access only to the features they need, instead of giving them access to everything, can protect the organization from attacks that could originate from within the group. Also dduring the process, we ran various dependency checks to search for vulnerabilities as well as adding checksum verification and certifications. By implementing these best practices, we can ensure that our application remains secure and that our organization is protected from threats. Secure coding best practices are essential for maintaining software and system security and integrity by helping resist attacks from external and internal sources and safeguarding the company's reputation, customer data, and business operations. Implementing these practices can also help the company comply with legal and regulatory requirements and avoid costly penalties.

Citations:

Crawford, D. (2019, February 4). *AES encryption: Everything you need to know about AES*. ProPrivacy.com. <https://proprivacy.com/guides/aes-encryption>

Kantarcioglu, M. (n.d.). *Advanced encryption standard - personal.utdallas.edu*. Advanced Encryption Standard. https://personal.utdallas.edu/~muratk/courses/crypto07\_files/aes.pdf