****

# 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** | **2.24.23** | **Tiffany Montero** |  |

## 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

Tiffany Montero

## Algorithm Cipher

Financial industries have a to meet a high level of security to ensure their user’s security and trust. Due to the nature of the information being handled by Artemis Financial, I strongly believe the best algorithm cipher for the job is the Advanced Encryption Standard (AES). AES had been the government standard since 2002 (Bernstein & Cobb, 2021) and is used by many private institutions. AES is available in multiple bit levels, those being 128-bit, 192-bit, and 256-bit. The larger key size is more secure. However, this means it will take longer to decrypt information, which could potentially affect the user experience.

AES is a symmetric encryption algorithm, meaning one key is used for encryption and decryption. Proper implementation is crucial, since anyone with access to the key can decrypt data (Nagaraj, 2023). Proper implementation includes requiring strong passwords, multifactor authentication, anti-malware software, and firewalls (Bernstein & Cobb, 2021).

Hash functions are one-way encryption, meaning it cannot be decrypted. This is incredibly useful to verify data such as passwords while keeping the information secure. SHA-256 is one of the best regarded hashing algorithms. Hashing passes the data via a function and returns an alternate value (Jena, 2023). Any data that needs to be verified against it, will also be passed through the hash function. The alternate values are compared for equality.

## Certificate Generation

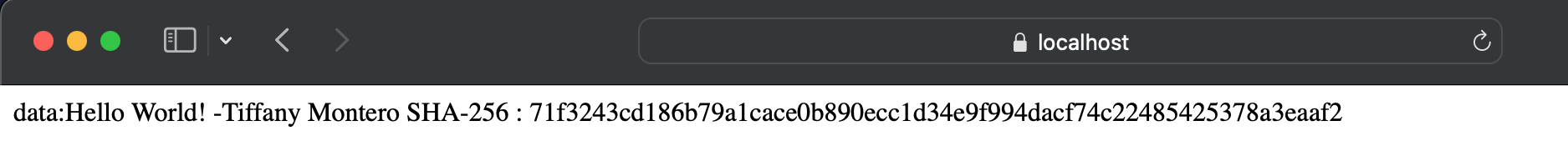
Insert a screenshot below of the CER file.

A screenshot of a computer

Description automatically generated

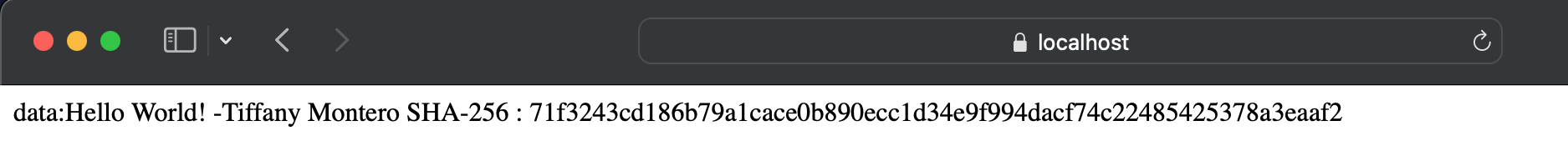
## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

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



## Secondary Testing

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

A screen shot of a computer program

Description automatically generated

A screenshot of a check

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

## Summary

After reviewing the Vulnerability Assessment Process Flow chart, we can start to understand what all was implemented. APIs were implemented in https and displaying the data. Cryptography is implemented with the use of encryption, specifically SHA-256 in this case. Code error was addressed with the NoSuchAlgorithm exception.

References

Bernstein, C., & Cobb, M. (2021, September 24). *What is the Advanced Encryption Standard (AES)?*. TechTarget. <https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard>

Dworkin, M. , Barker, E. , Nechvatal, J. , Foti, J. , Bassham, L. , Roback, E. and Dray, J. (2001), Advanced Encryption Standard (AES), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD, [online], <https://doi.org/10.6028/NIST.FIPS.197>

Jena, B. K. (2023, August 29). What is SHA-256 algorithm: How it works and applications: Simplilearn. Simplilearn.com. https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

Nagaraj, K. (2023, February 22). Advanced encryption standard (AES): A secure and efficient symmetric encryption algorithm. Medium. https://infosecwriteups.com/advanced-encryption-standard-aes-a-secure-and-efficient-symmetric-encryption-algorithm-319eedb49905