****

# 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** | **October 12, 2023** | **Brandon Goller** |  |

## Client



## Developer

Brandon Goller

## Algorithm Cipher

Artemis Financial, a financial consulting company, aims to modernize its operations and enhance the security of its public web application. Their services involve creating financial plans related to savings, retirement, investments, and insurance. To achieve the highest level of security, Artemis Financial plans to implement robust software security measures.

One fundamental security enhancement is encryption. Encryption secures data at rest by converting it into a secret code, which can only be decoded with the appropriate key. The recommended encryption standard for Artemis Financial is AES (Advanced Encryption Standard). AES is a symmetric block cipher, meaning it uses the same key for both encryption and decryption. It is trusted by the U.S. government and offers various key lengths, such as 128, 192, or 256 bits. Longer key lengths make it exceedingly difficult for attackers to decrypt the data through brute-force methods.

Another crucial security measure involves hash functions. Hash functions serve various purposes, such as securely storing passwords in a database or ensuring data integrity through checksums. A secure hash function should be collision-resistant, lack predictable patterns, and provide a wide range of unique hash values. SHA-256, which is the second version of SHA, meets all these requirements, making it a suitable choice for Artemis Financial.

Random numbers play a significant role in cryptography, particularly in key generation. There are two key types used in encryption: symmetric and asymmetric. Symmetric encryption utilizes a single key for both encryption and decryption. Asymmetric cryptography relies on a pair of public and private keys to secure data and is commonly used for digital signatures. The private key is kept confidential and known only to the sender, while the public key is openly accessible.

Encryption has evolved over time, with different algorithms reflecting varying levels of security. For instance, DES was commonly used until 2002 when AES became the standard. DES was phased out due to significant vulnerabilities, highlighting the importance of staying up to date with encryption standards for robust data security.

## Certificate Generation

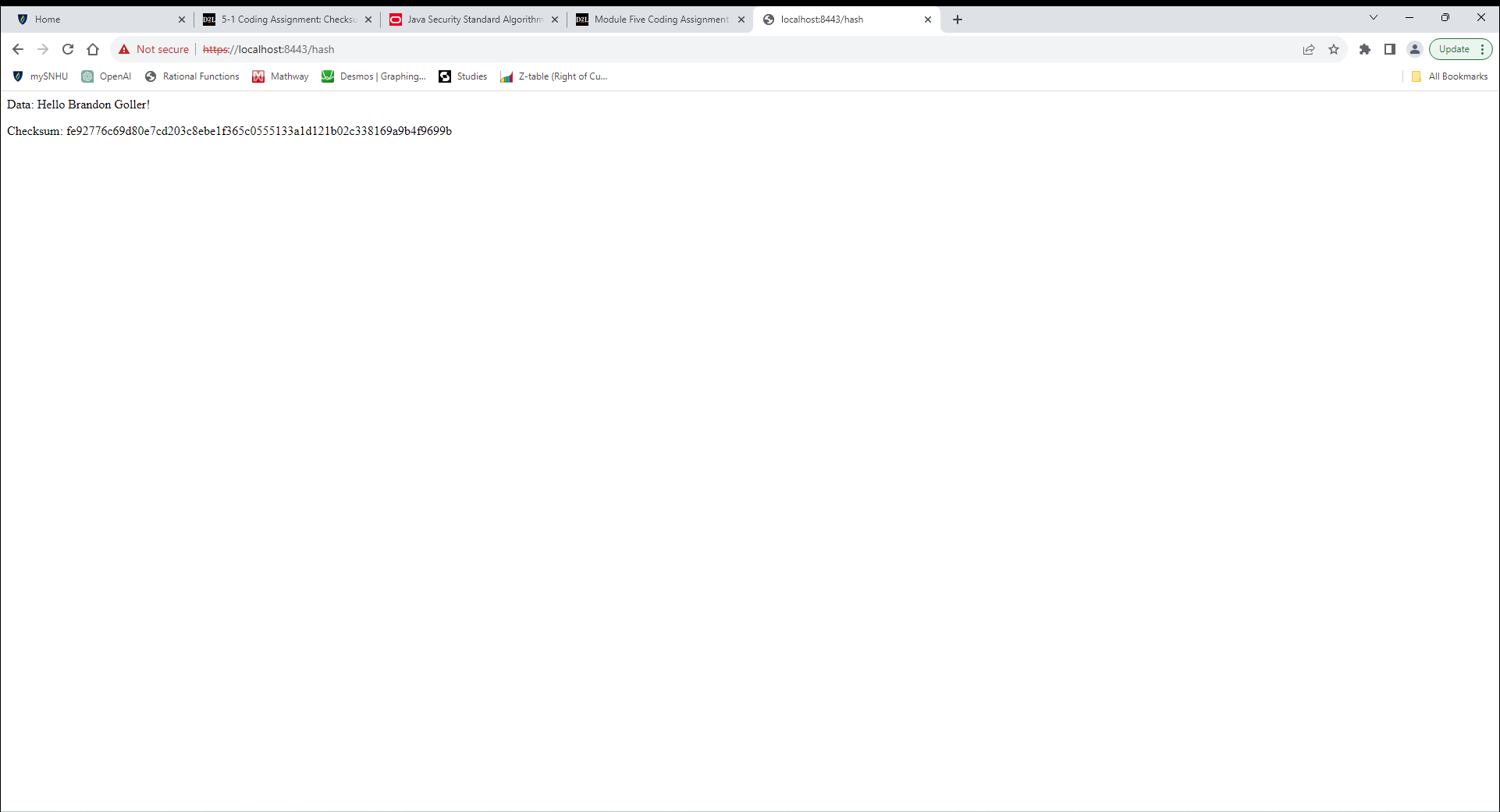
Insert a screenshot below of the CER file.

A screenshot of a certificate

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

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

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

## Functional Testing

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

A computer screen shot of a computer screen

Description automatically generated

## Summary

During this project, the code underwent significant refactoring to align with security testing protocols, ensuring that Artemis Financial's software application is well-protected and compliant with the highest security standards.

Refactoring efforts primarily focused on enhancing data security and secure communications. These enhancements addressed key aspects of the Vulnerability Assessment Process Flow Diagram, effectively fortifying the application against potential threats.

One major area of concern was the introduction of a cryptographic hash algorithm, specifically the SHA-256 cipher, which ensures data integrity and confidentiality. This addition serves as a robust defense against data tampering and unauthorized access. By implementing secure encryption measures, we mitigated risks associated with data transmission and storage.

Additionally, we adopted secure coding practices throughout the application, emphasizing proper data validation, ensuring that input is sanitized to prevent common security vulnerabilities such as SQL injection or cross-site scripting (XSS). The code was refactored to perform comprehensive input validation, safeguarding it against malicious inputs and potential exploits.

Moreover, we integrated secure communications by transitioning the application from HTTP to the HTTPS protocol. This shift to HTTPS ensures data exchanged between the user and the application is encrypted, making it significantly more challenging for malicious actors to intercept and manipulate sensitive information.

Our process for adding layers of security was methodical and thorough. We began by assessing the existing vulnerabilities in the code and identifying potential weak points. Subsequently, we introduced appropriate encryption measures, ensured the generation and utilization of secure certificates, and systematically validated the refactored code for compliance with industry standards and best practices.

This multifaceted approach to security enhancement has transformed the application into a robust and resilient system, well-prepared to safeguard Artemis Financial's critical data and protect it from potential security breaches. By integrating advanced encryption, ensuring secure communications, and adopting secure coding practices, we have significantly fortified the software application and addressed the core areas of security outlined in the Vulnerability Assessment Process Flow Diagram.

## Industry Standard Best Practices

The application's enhancement and security measures align closely with industry-standard best practices for secure coding, ensuring the mitigation of known security vulnerabilities and the maintenance of the software's current security.

One fundamental aspect of our approach is the adoption of encryption technologies, which is an industry-standard best practice for securing sensitive data. By implementing the Advanced Encryption Standard (AES) and SHA-256, we have ensured that data is stored and transmitted securely, even in the face of sophisticated attacks. This approach maintains the application's current security by providing a robust defense against data breaches and unauthorized access.

In addition, we employed input validation and sanitation practices as another best practice. This is crucial to prevent common security vulnerabilities, such as SQL injection and cross-site scripting (XSS). By adhering to industry-standard recommendations in this regard, we have enhanced the application's overall resilience against malicious input and potential exploitation.

Moreover, the transition from HTTP to HTTPS for secure communications is in line with industry standards for web application security. This best practice encrypts data exchanged between users and the application, reducing the risk of data interception and manipulation. It further protects sensitive financial information, making the application more trustworthy and valuable for Artemis Financial's clients.

The value of applying industry-standard best practices for secure coding extends to the company's overall well-being in several ways. First and foremost, it enhances Artemis Financial's reputation for trust and reliability. Clients and partners are more likely to engage with a company that demonstrates a strong commitment to safeguarding their data. This, in turn, can lead to increased business opportunities and client loyalty.

Furthermore, secure coding practices reduce the likelihood of security breaches and the associated financial and reputational damage. The costs of recovering from a security incident can be significant, including expenses related to data recovery, legal matters, and potential fines for non-compliance. By applying industry-standard security practices, Artemis Financial can minimize these risks, saving valuable resources and maintaining its financial stability.

Lastly, in an era of increasing data privacy regulations and legal obligations, adhering to industry standards for secure coding is essential for regulatory compliance. Failure to do so can result in legal penalties and damage the company's legal standing. By ensuring compliance with industry standards, Artemis Financial positions itself to meet current and future regulatory requirements, safeguarding the company's long-term viability and legal standing.

In summary, implementing industry-standard best practices for secure coding provides tangible benefits for Artemis Financial, including enhanced reputation, reduced risks, cost savings, and legal compliance. These practices bolster the company's overall well-being and contribute to its success in a highly competitive and security-conscious financial industry.