****

# 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** | **12/9/2023** | **Sean Nicolai** | **Created Report** |

## 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

Sean Richard Julius Nicolai

## Algorithm Cipher

**Overview of AES Encryption Algorithm**

For Artemis Financial's requirements, the Advanced Encryption Standard (AES) is chosen as the preferred encryption algorithm. AES is a symmetric key algorithm known for its strong security and efficient performance, making it suitable for securing sensitive financial data.

**Key Features of AES**

* Hash Functions and Bit Levels: AES operates on 128-bit data blocks and supports key lengths of 128, 192, or 256 bits. Given the sensitive nature of financial data, a 256-bit key is recommended for Artemis Financial, offering high security without compromising performance.
* Symmetric Keys: AES uses the same key for encryption and decryption. This necessitates a secure key exchange mechanism, particularly for initial key distribution.
* Role of Random Numbers: AES requires cryptographically secure pseudo-random number generation for strong key creation, ensuring resistance to cryptographic attacks.

**AES in the Context of Current Encryption Standards**

AES, established as a federal standard by the U.S. National Institute of Standards and Technology (NIST) in 2001, is now a cornerstone in encrypting web traffic and securing government and financial records. Its widespread adoption and proven security record make it an ideal choice for Artemis Financial's software security upgrade.

## Certificate Generation

Insert a screenshot below of the CER file.

A computer screen shot of a computer program

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.

A screenshot of a computer

Description automatically generated

## 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.

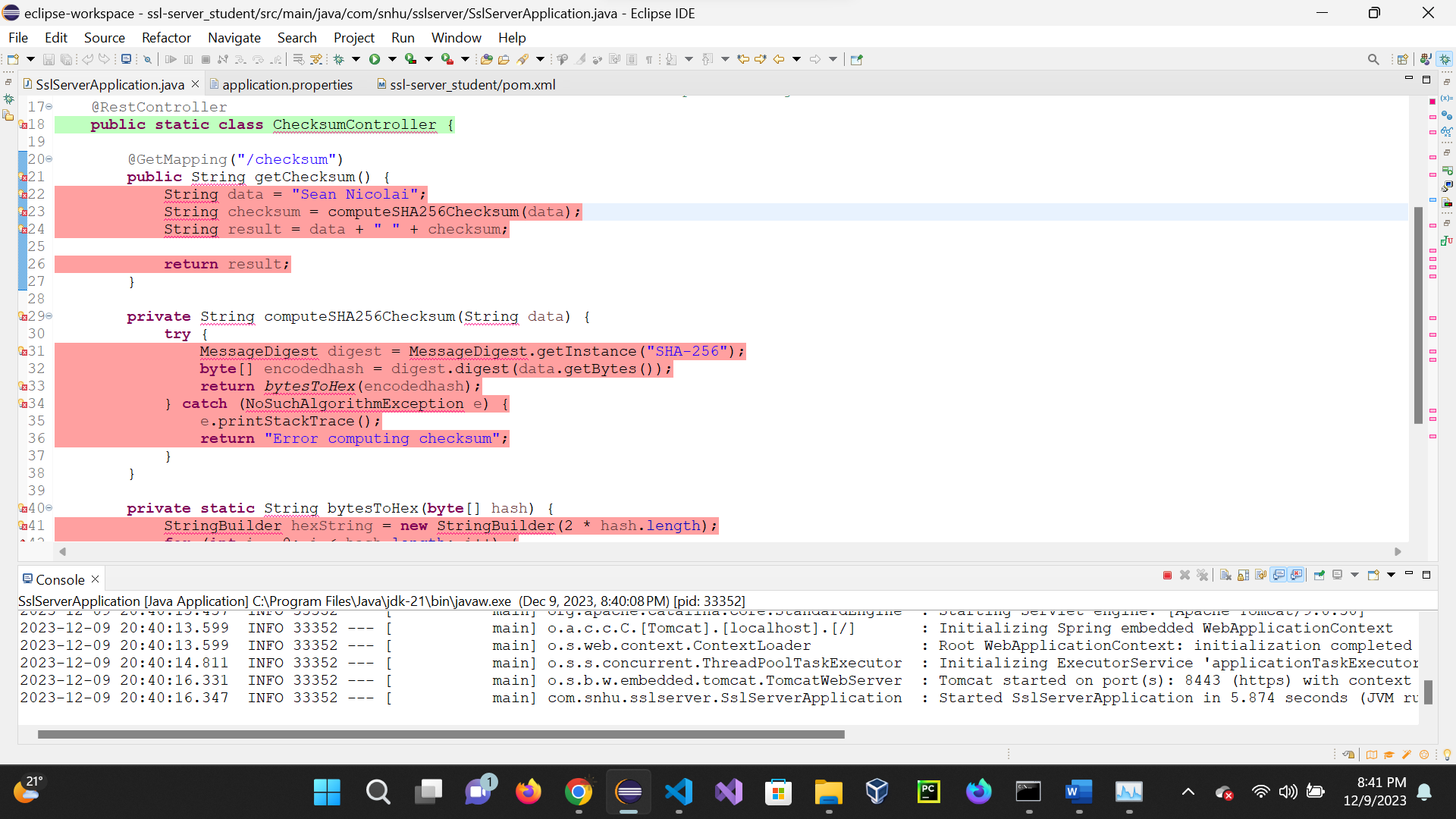
A screenshot of a computer

Description automatically generated  
A screenshot of a computer

Description automatically generated

## Functional Testing

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



## Summary

This project entailed comprehensive refactoring of Artemis Financial's software application to bolster its security measures. Key enhancements included implementing the AES encryption algorithm for robust data encryption and transitioning from HTTP to HTTPS to secure communications.

However, our recent OWASP Dependency-Check revealed a significant challenge: the presence of 115 vulnerabilities across 15 dependencies. This critical finding necessitates immediate and thorough action. We are currently developing a comprehensive strategy to address these vulnerabilities. Our approach involves a detailed analysis of each vulnerability, prioritizing them based on severity and impact, and subsequently formulating a plan for systematic resolution. This phase of vulnerability management is critical and will be an ongoing focus to maintain and enhance the application's security posture. This journey underscores the dynamic nature of software security and the necessity of continuous vigilance and adaptability in our security practices.

## Industry Standard Best Practices

In response to our recent findings from the dependency-check scan, we are intensifying our focus on industry-standard best practices, especially in areas of dependency management and vulnerability response. We are establishing a routine for regular dependency checks and updates as an integral part of our development process. This will enable proactive identification and remediation of security vulnerabilities in third-party components. Additionally, we are enhancing our secure coding practices to include more rigorous code reviews, expanded testing protocols, and the adoption of automated tools for early detection of vulnerabilities in our codebase. By integrating these practices and tools into our continuous integration/continuous deployment (CI/CD) pipeline, we can detect and address security issues more efficiently. These steps are vital for upholding our commitment to security and will be continuously evolved to align with emerging threats and industry standards. This proactive approach to security is invaluable to the company's overall well-being, as it prevents data breaches and the resultant financial and reputational damages.