****

# 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** | **6/16/2023** | **Robert Golden** |  |

## 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

Robert Golden

## Algorithm Cipher

Based on the security vulnerabilities present in the software and the type of data Artemis Financial handles, I would recommend the AES-256 symmetric key encryption algorithm. The strength of algorithm has a lot to do with the complexity of brute-force attacks against the large key size, making it a trusted choice for encryption in various applications. This cipher has a bit level of 256 which means that there are 2^256 possible combinations of key values. The AES-256 cipher is a symmetric encryption algorithm which means a single key is shared for encryption and decryption. This results in a faster decryption time, but also means its crucial to keep the key secure.

The encryption methods over the course of the twentieth century have evolved greatly. The first publicly available encryption standard, Data Encryption Standard, is now vulnerable to brute force attacks because of the massive increase in computing power over the last 50 years. Currently the most widely used encryption standard is AES-256 which came in to existence in the late 1990’s.

## Certificate Generation

A picture containing text, screenshot, font

Description automatically generated

## Deploy Cipher

A black text on a white background

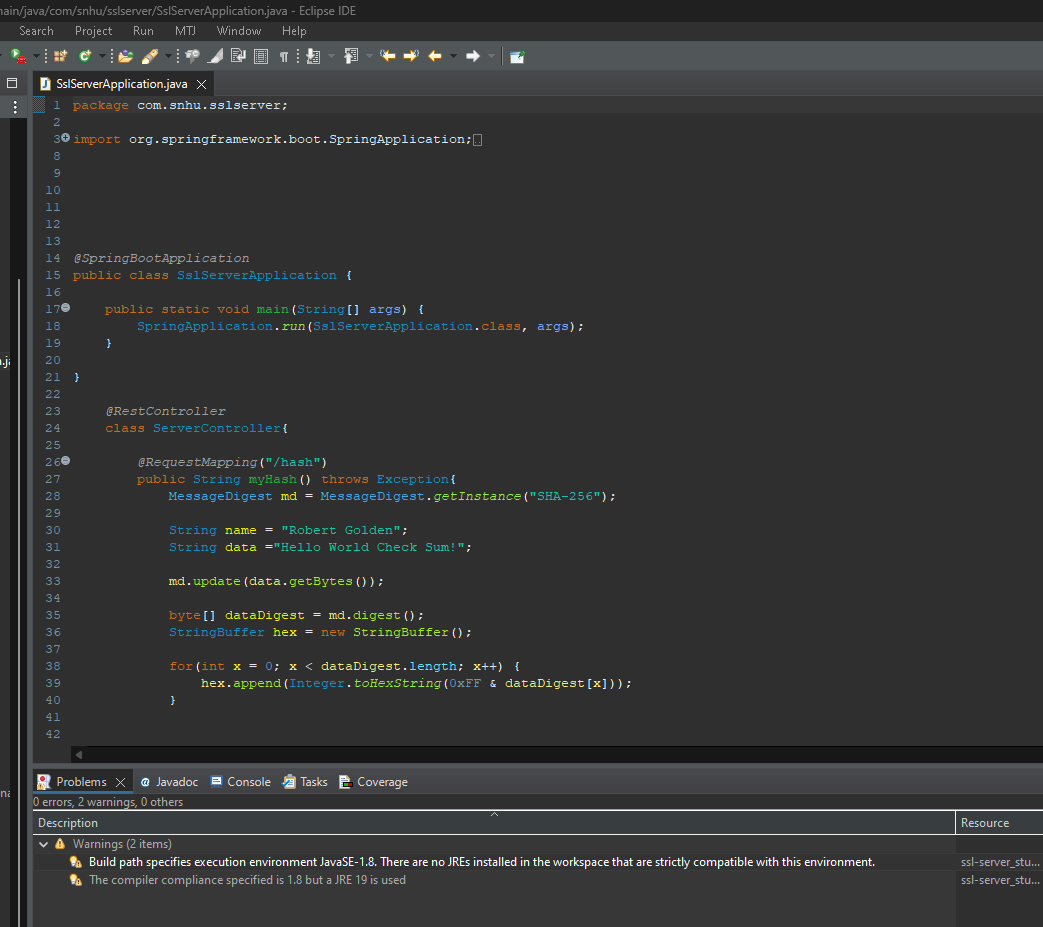
Description automatically generated with low confidence

## Secure Communications

A screenshot of a computer

Description automatically generated

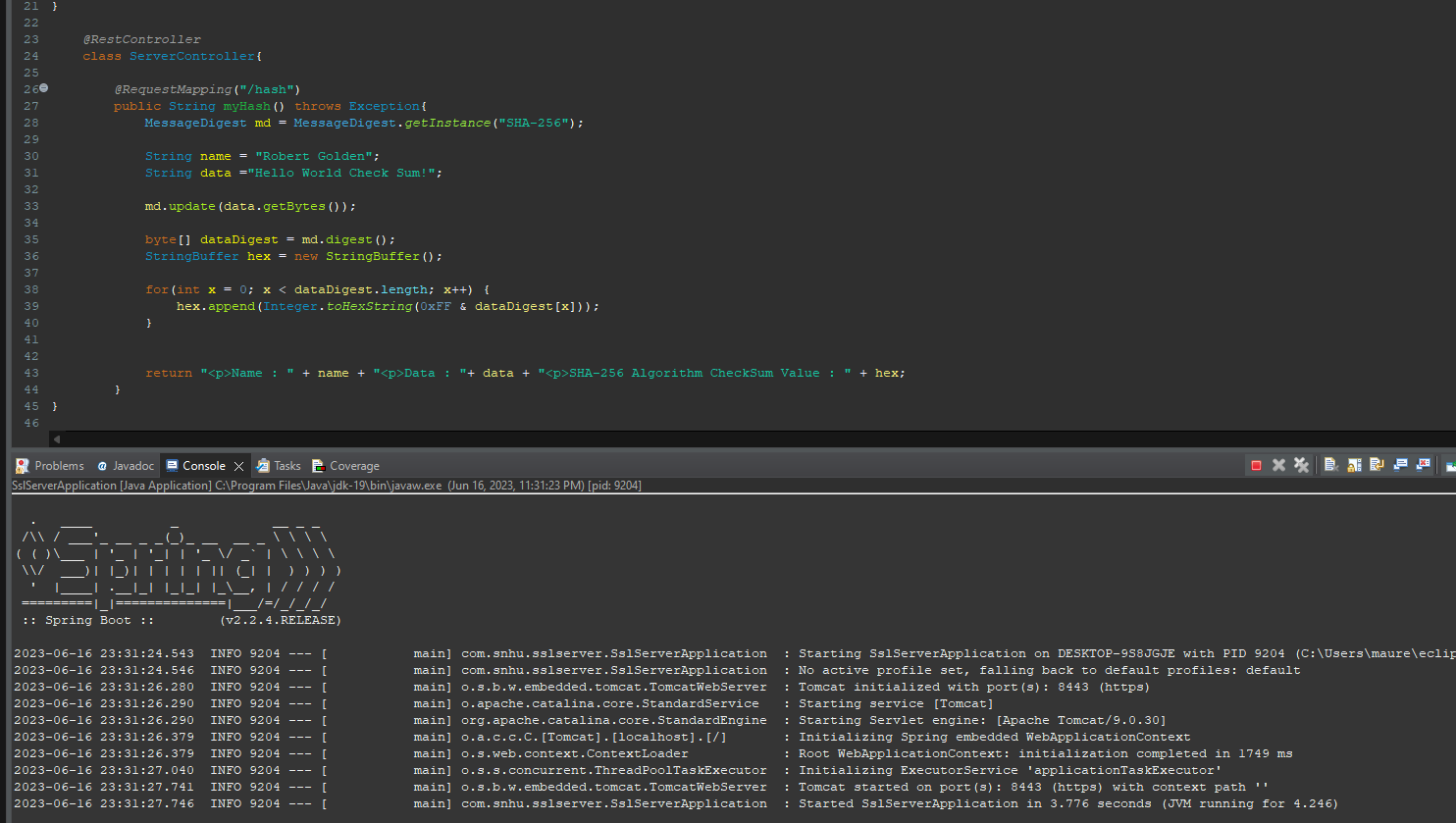
## Secondary Testing



A screenshot of a computer

Description automatically generated with medium confidence

## Functional Testing



## Summary

I got nothing…. I just don’t want to write anymore. This was the hardest project this semester, and even though I have this section and another, I have reached a wall. Thank you for the quick grading of all my assignments.

## Industry Standard Best Practices

[Insert text.]