****

# 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** | **01/23/2023** | **Theresa Vassell** |  |

## 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

Theresa Vassell

## Algorithm Cipher

For this scenario, I am working with Artemis Financial in order to help protect their organization from outside threats. After reviewing Artemis Financials security vulnerabilities, I am recommending the use of AES 256 as an appropriate algorithm cipher that will be able to meet their needs. “AES encryption, or advanced encryption standard, is a type of cipher that protects the transfer of data online. Currently, AES is one of the best encryption protocols available, as it flawlessly combines speed and security” (n.d). AES 256 is currently the most secure version of the AES implementation.  AES can be found in software used all around the world from the US government to various banking industries. AES is a symmetric key cipher, meaning it uses the same secret key to encrypt and decrypt data. AES -256 algorithms are almost impossible to break and would take years to be broken by a brute-force attack.

The use of random numbers in encryption prevents hackers from gaining access to protected and sensitive information. Symmetric keys are used for encrypting and decryption data while non-symmetric keys use two separate keys for encryption and decryption, however, it is much slower than using symmetric keys. Encryption algorithms can be traced as far back as ancient Egypt about 4000 years ago. This shows us that the need to keep certain information secret from prying eyes came about not long after the invention of writing. Encryption has since been traced from ancient Egypt, Greece, and the Roman military to the World Wars and now to the modern day. Today we find that encryption has greatly evolved since it was first documented and is now widely used throughout our daily lives.

## Certificate Generation

Insert a screenshot below of the CER file.

Text

Description automatically generated

## Deploy Cipher

## Checksum code

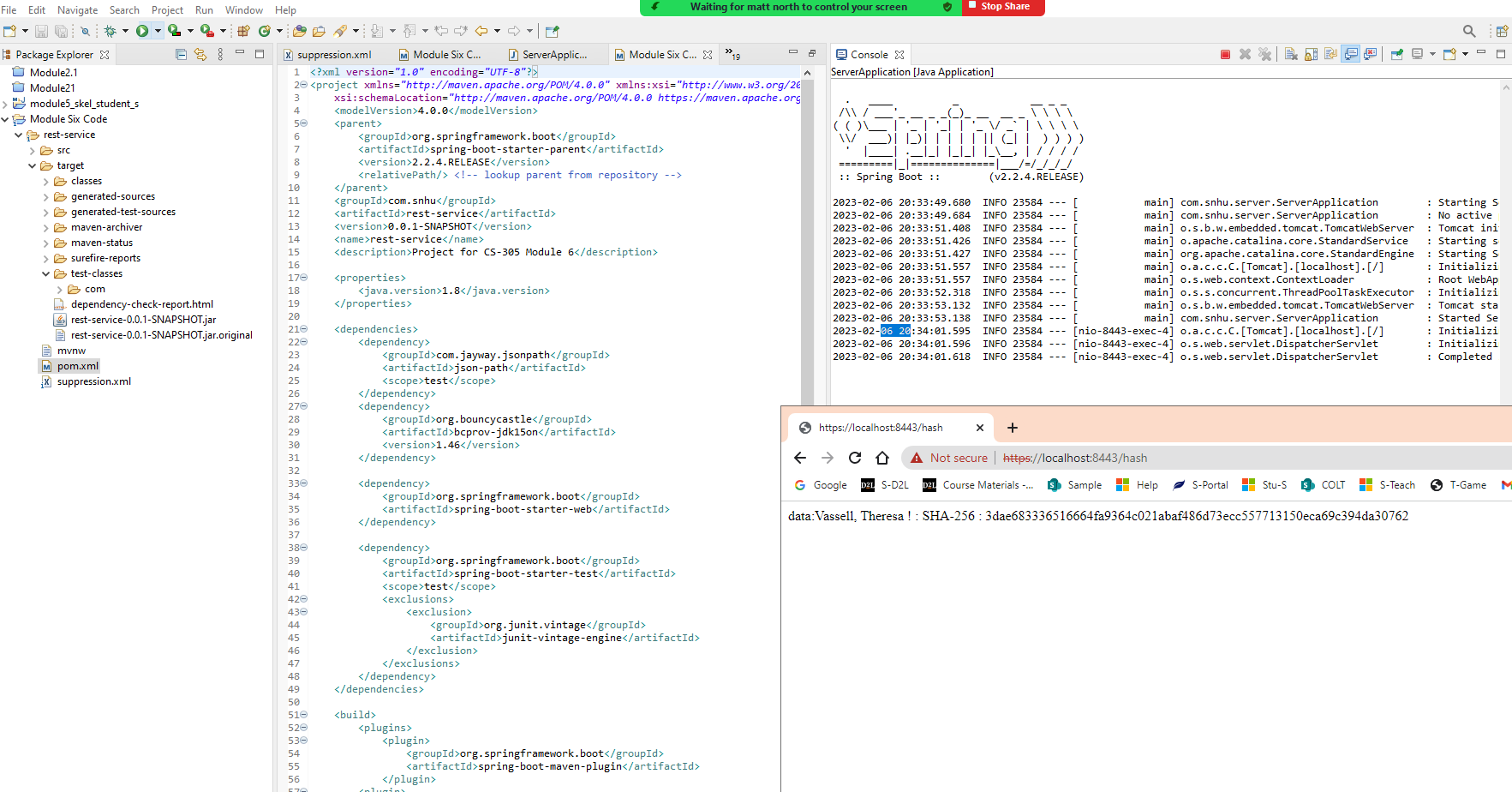
## 

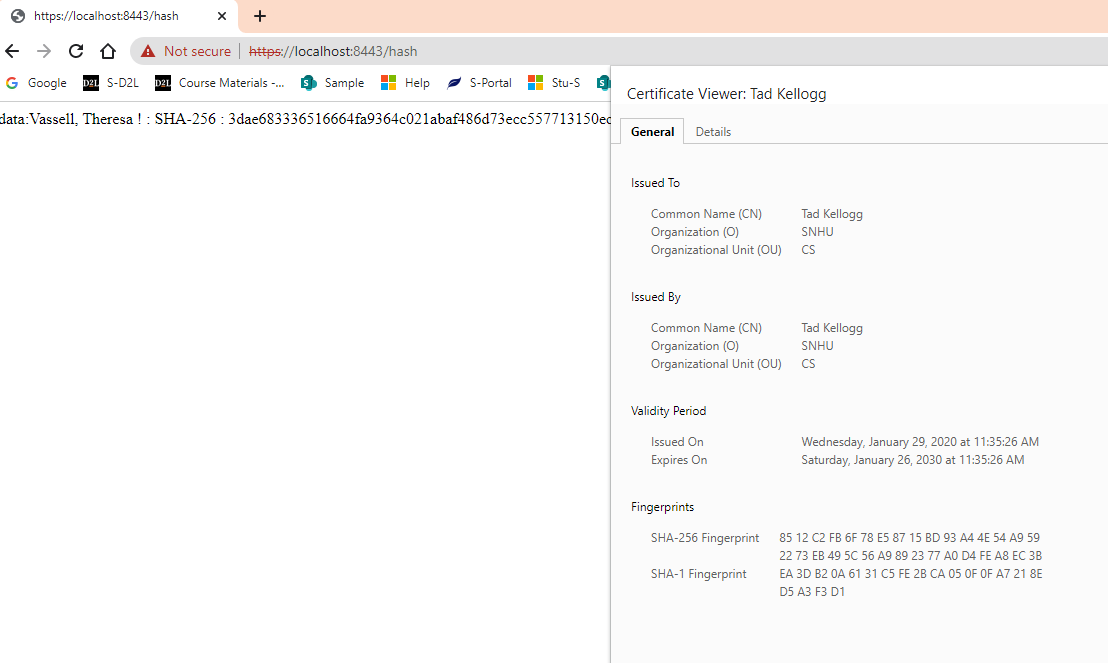
## Checksum results

## 

## Secure Communications

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

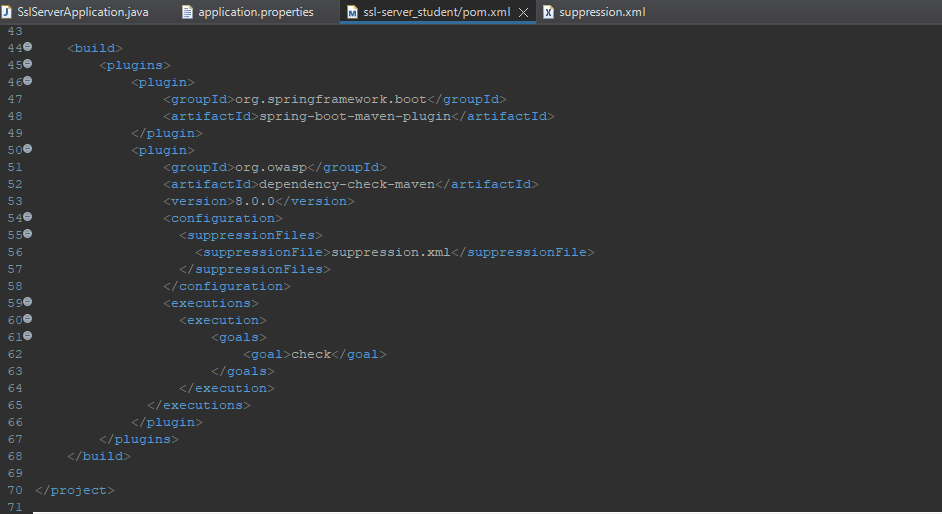




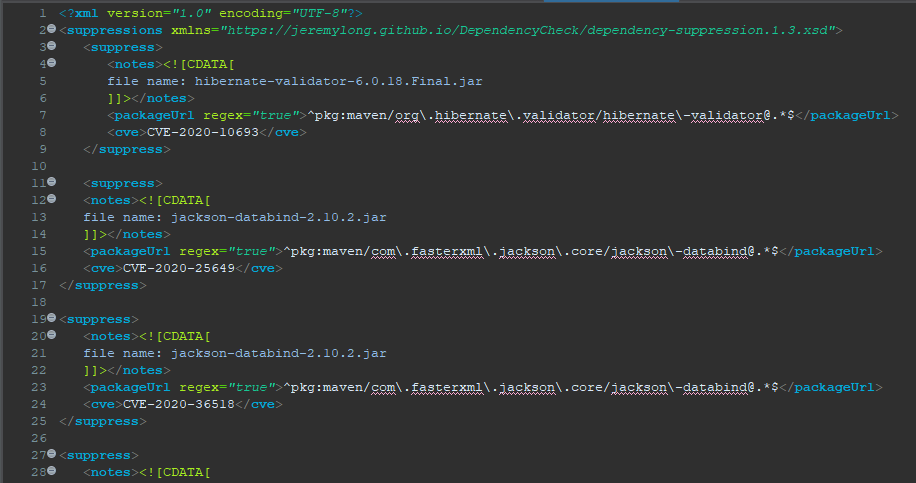
## Secondary Testing

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

**Screenshot of updated Pom.xml file with suppression code and updated dependency check version number.**



**Example of Suppression file**

****

**Screenshot of Dependency Check with suppressed vulnerabilities. Even after copying and pasting the all the suppression code into my suppression file I was not able to suppress all the vulnerabilities.**

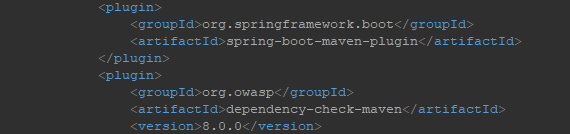
**Graphical user interface, text, application, email

Description automatically generated**

## Functional Testing

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

**One issue that was found when manually reviewing the code was that the Pom.xml file was an outdated version of the springframework. I corrected this by updating the code to the current version of springframework available 8.0.0.**

****

## Summary

After reviewing the Vulnerability Assessment Flow Diagram, I was able to locate various areas of security that needed to be addressed such as cryptography, API, and client/server areas. For this project, I spent a great deal of time ensuring that the project was complying with security testing protocols and that the above security vulnerabilities were addressed. During this process self-signed certificates were generated using the Java Keytool. This allows users to verify that our site is legitimate. I then moved on to implementing a cryptography hash function which ensured that sensitive data was scrambled and could not be accessed using a brute force attack. I also refactored the code in the application.properties files that allowed for the HTTP protocol to be converted to HTTPS protocol which ensured that data was being transferred securely over the internet. I also implemented the RESTful API using the spring framework. Lastly, I spent some time working on the POM.xml file ensuring that all vulnerabilities identified by the dependency check maven were updated or suppressed until a solution can be found. All of these changes ensured that the system was protected against hackers hoping to utilize bugs as a way of attacking the system.

## Industry Standard Best Practices

Applying industry-standard best practices for secure coding helps developers to locate and fix any security vulnerabilities that a system may have. This will prevent the transfer of protected and sensitive company data from getting into the hands of hackers or the public. Following industry best practices also show clients that Artemis Financials is a trustworthy company that has their customers best interest in mind, which will in turn help to build the company's reputation and draw in clientele.

**References**

* *What is AES encryption and how does it work? | Cybernews*. (n.d.). Retrieved January 21, 2023, from https://cybernews.com/resources/what-is-aes-encryption/