****

# 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** | **15 April 2024** | **Logan artha** |  |

## 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

Logan Martha

## Algorithm Cipher

When dealing with making sure your data is secured, implementing an encryption cipher is a popular and effective way in ensuring that the data indeed, remains secure. There are different algorithms to choose from, so making sure you are aware of your potential attackers is the best way to pick the proper cipher for your program. When deciding on a cipher, the cipher should be able to protect your data from a plethora of attacks, such as brute for attacks or plaintext attacks. When it comes to risks, making sure your cipher is constantly up to date in protecting you from attacks is the most important thing. The cipher also must be able to follow any government regulations. For example, in the US, the cipher must follow HIPAA regulations. When it comes to the specific cipher for your company, the algorithm will be used for encrypting sensitive data such as financial transactions, customer information, and other proprietary data. It will likely be used in various applications, including communication protocols, databases, and storage systems. With that being said, I believe the cipher that best meets these needs is the Advanced Encryption Standard (AES). Right now, in this current technology ecosystem, this is the best bet. Now, another choice may be better if there were to be advancements in cryptanalysis or quantum computing. If that were the case, looking for a more hybrid type cipher could be beneficial, since they use multiple encryption algorithms to strengthen security.

When talking about encryption as a whole, there are a few key terms to be explained. Hash Functions. Hash functions are used to map data of arbitrary size to fixed-size values, typically for the purpose of ensuring data integrity and generating digital signatures. And Bits. Bits are values of 1 and 0 that represent values in an encryption. The more bits the more secure the encryption is. Random Numbers and Symmetric / Non-Symmetric Keys. These three terms help add an element of unpredictability to the keys. Symmetric is a term that represents the encryption and decryption are solved with the same key. Non-symmetric uses multiple keys in order to decrypt and encrypt their data, making it a higher security measure, but may be slower and less efficient than an symmetric cipher. Like any form of technology, there is always advancements and versions to make the product better. Today, AES is one of the most well-known and effective and efficient ciphers, when implemented correctly, in today’s market. Overall, I do believe AES is the best algorithm for your company as it is the most used and reliable out there.

## 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.

A computer screen shot of a program

Description automatically generated

## Secure Communications

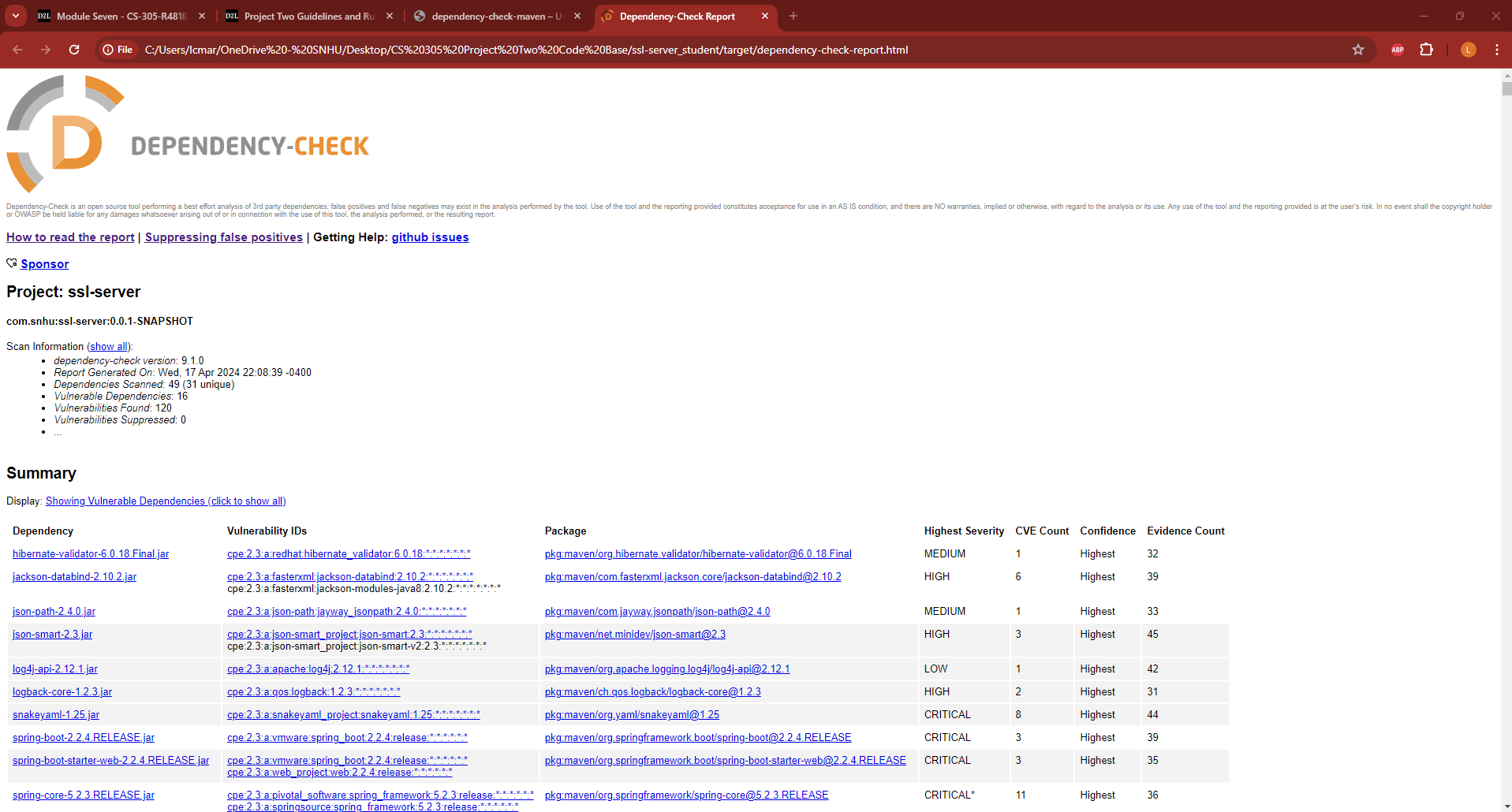
Insert a screenshot below of the web browser that shows a secure webpage.

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

## Functional Testing

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

A screenshot of a computer

Description automatically generated

## Summary

I've made some changes to the code to handle errors better and ensure it follows secure coding practices. While it doesn't directly validate input, it's important in real applications to have authentication and authorization mechanisms for security. The code uses standard Java libraries for encryption, which is good, but it's crucial to keep them updated to address any vulnerabilities. These updates should make the code more secure, but testing is still needed to be sure it's strong against potential attacks.

## Industry Standard Best Practices

The value of applying industry standard best practices for secure coding to the company's overall wellbeing cannot be overstated. By prioritizing security in software development, the company minimizes the risk of costly security breaches, data leaks, and reputational damage. Compliance with industry standards not only helps in protecting sensitive data and maintaining customer trust but also ensures regulatory compliance, which is essential for avoiding legal penalties and fines. Moreover, a strong security posture enhances the company's competitiveness in the market by demonstrating a commitment to safeguarding customer information and maintaining the integrity and reliability of its products and services. Ultimately, investing in secure coding practices contributes to the long-term sustainability and success of the company in an increasingly interconnected and threat-prone digital landscape. I made sure I was following the standard best practices to provide safe and efficient code. I made sure the code was readable and manipulatable so if necessary for change, it would be an easy task.