****

# Practices for Secure Software Report

**Table of Contents**

[**Document Revision History 3**](#_heading=h.30j0zll)

[**Client 3**](#_heading=h.1fob9te)

[**Instructions 3**](#_heading=h.3znysh7)

[**Developer 4**](#_heading=h.2et92p0)

[**1. Algorithm Cipher 4**](#_heading=h.tyjcwt)

[**2. Certificate Generation 4**](#_heading=h.3dy6vkm)

[**3. Deploy Cipher 4**](#_heading=h.1t3h5sf)

[**4. Secure Communications 4**](#_heading=h.4d34og8)

[**5. Secondary Testing 4**](#_heading=h.2s8eyo1)

[**6. Functional Testing 4**](#_heading=h.17dp8vu)

[**7. Summary 4**](#_heading=h.3rdcrjn)

[**8. Industry Standard Best Practices 4**](#_heading=h.26in1rg)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **[Date]** | **[Your Name]** |  |

## Client



## Instructions

Submit these completed practices for a 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

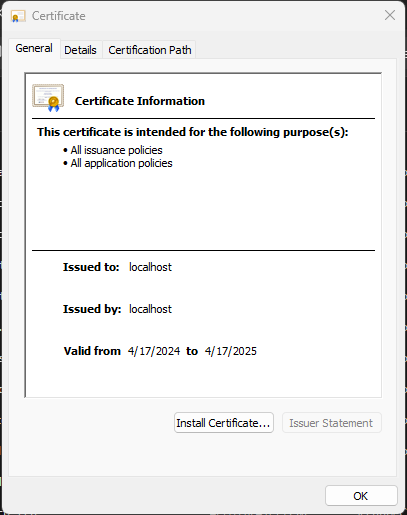
Dawson Kennedy

## Algorithm Cipher

I went with AES, Advanced Encryption Standard, for my algorithm cipher. AES is regarded as the Industry standard. In 2003 the NIST, or the National Institute of Standards and Technology, made AES the default encryption algorithm. (Rahul Awati, 2024) Boasted for its robustness and almost impossible resilience to brute force attacks. (Rūta Rimkienė, 2024) AES boasts a fixed block size of 128-bits, or 16 bytes, the key length can vary in length. AES even boasts a 256-bit key length, regarded as “military-grade”. (Ed Oswald, 2024) On top of all that it has a fast encryption and decryption time as well. In short AES is a standard go to for any and all encryption needs, from personal devices to “top secret” level data hosted by the US Government.

## Certificate Generation

Insert a screenshot below of the CER file.



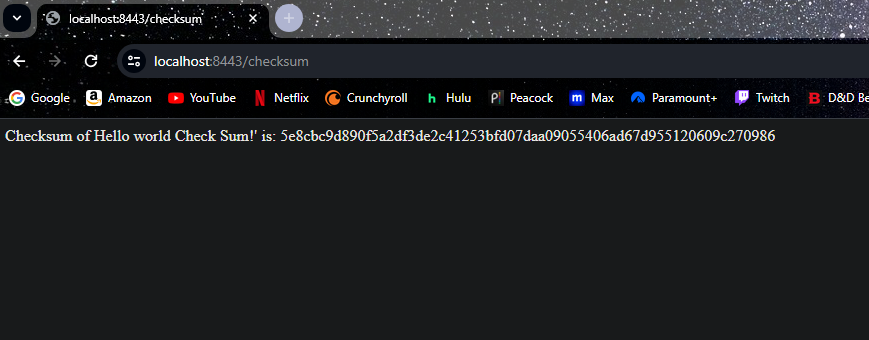
## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

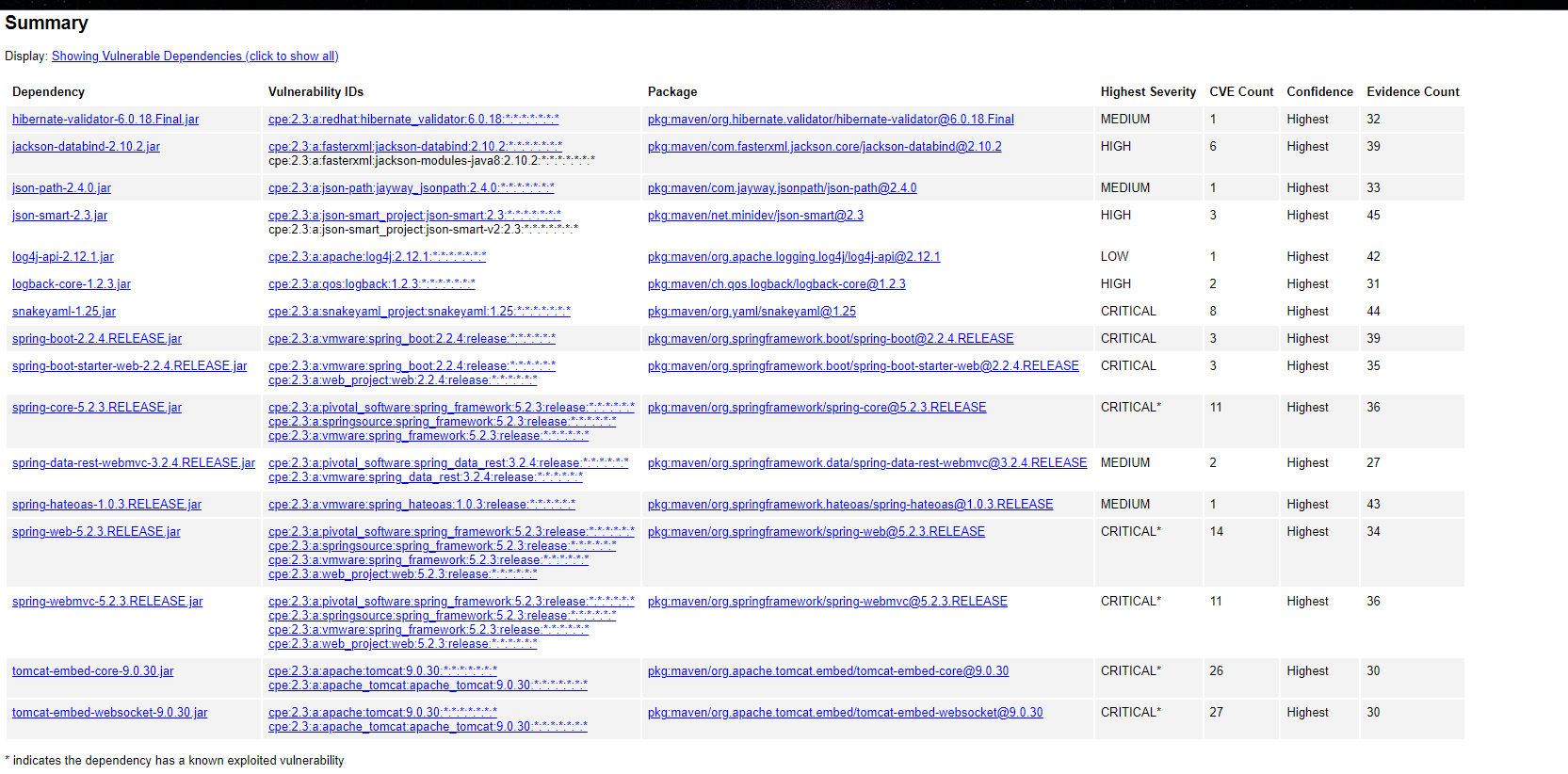
Insert a screenshot below of the web browser that shows a secure webpage.



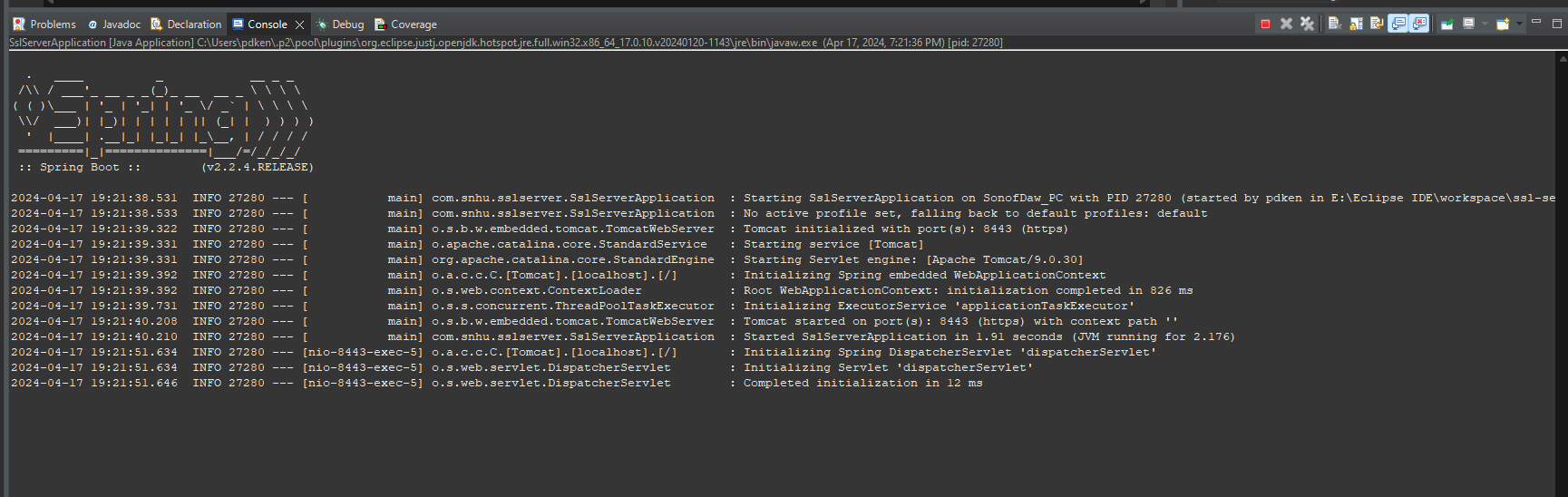
## Secondary Testing

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

Dependency-check:

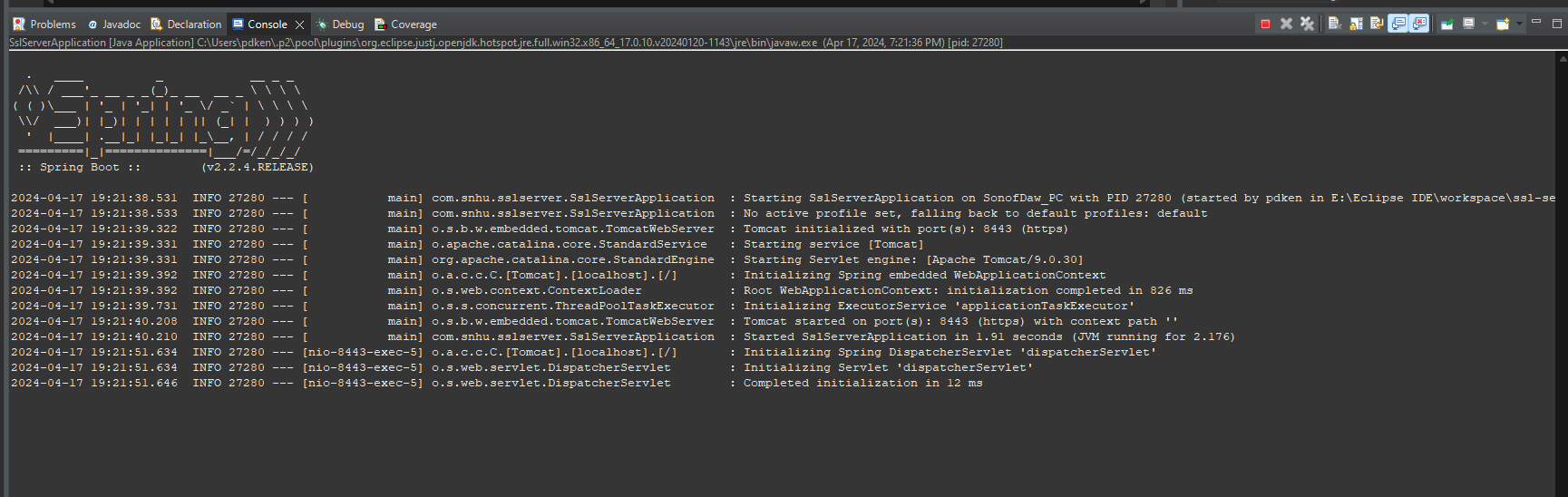


code:



## Functional Testing

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



## Summary

I made the code to address these areas of vulnerability. Cryptography, Client/ Server, Code Quality. I did this by implementing secure code that would encrypt the data being given to the server. Along with that I made the data encrypted using a HEX cipher. I then generated keystores and certifications to secure the server on its port while running to safely and securely send its data to the server while running and verified the certification with the browser to allow it to know that the URL and server was safe.

## Industry Standard Best Practices

I used encryption, keystores, and certification to make sure that the server I was making was safe. I used AES encryption Cipher to achieve this as it is the industry standard. I used 256 bit keys for the encryption as it is a strong encryption value. Applying industry best standards is an excellent way to make sure that the server you are building is going to be safe for whoever may use it. Making sure the server is safe is a key competency when building a server as you do not want the user base to be open to malicious attacks. Security of a server is the most important especially when other people may use it as their personal information should be kept private from prying eyes and not be used in a way as to threaten them.

Sources:

Awati, R., Bernstein, C., & Cobb, M. (2024, February 20). *What is the Advanced Encryption Standard (AES)?: Definition from TechTarget*. Security. https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard

Oswald, E. (2022, December 16). *What is the Advanced Encryption Standard (AES)? | U.S. news*. What Is the Advanced Encryption Standard (AES)? https://www.usnews.com/360-reviews/privacy/what-is-advanced-encryption-standard

Rimkienė, R. R. (2022, August 29). *What is AES encryption and how does it work? | Cybernews*. What is AES encryption and how does it work? https://cybernews.com/resources/what-is-aes-encryption/