****

# 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** | **6/15/23** | **Dylan Kusick** |  |

## Client



## Developer

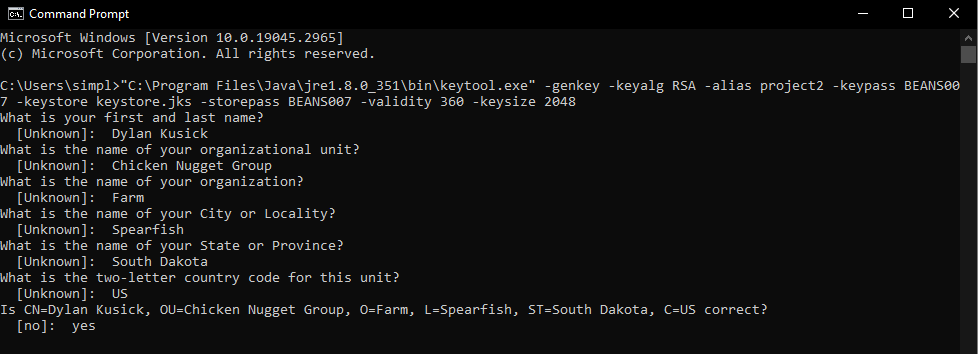
Dylan Kusick

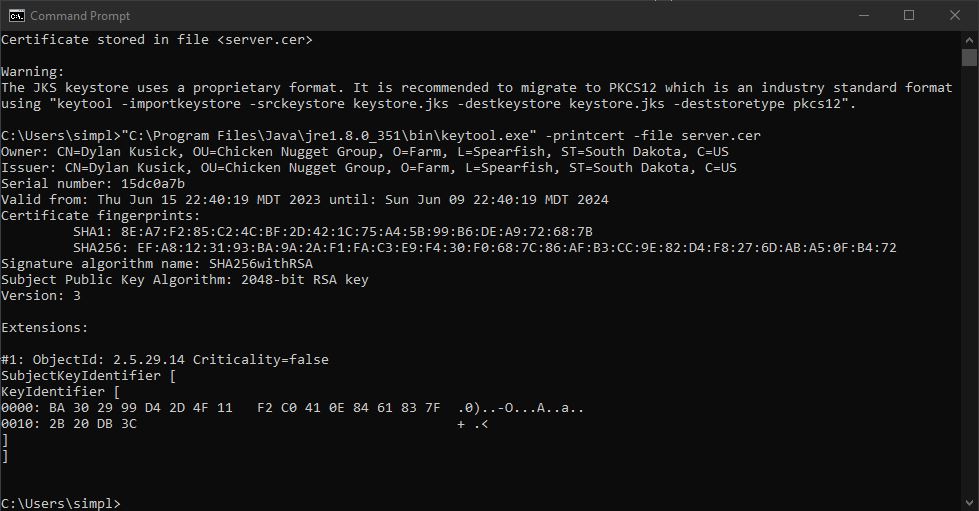
## Algorithm Cipher

Previously, I had recommended AES, or Advanced Encryption Standard for Artemis Financial. I do not think there is a need to change the encryption cipher given the presented scenario. AES has been around since 1997 and is so secure that it has been chosen as the encryption algorithm standard by the United States government (Bernstein, 2021). The cipher works by taking plain text and converting it into ciphertext, which essentially just looks like random numbers and letters mashed together. This happens by converting chunks of 128 bits into keys of 128, 192, or 256-bit keys. These keys are necessary to decrypt the message as they are the same ones that encrypted them (Jena, 2023). Therefore, these keys are very necessary to keep safe, especially so they do not get into the wrong hands. Symmetric versus non-symmetric keys are going to tell us whether the receiving end of the encrypted message will have a key to decrypt the message. Non-symmetric keys will have a public key that is used to encrypt the message and a private key that is used to decrypt the message (Poggi, 2021). The difference in the symmetric key is of course explained above as AES uses symmetric keys.

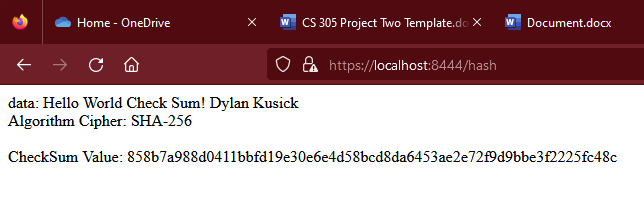
Encryption algorithms have changed drastically since they were introduced and will continue to evolve as necessary. Before AES, the standard for encryption algorithms was DES. DES was also a symmetric encryption algorithm but was being broken by distributed computers due to it only being a 64-bit encryption algorithm (Bernstein, 2021). As technology does, DES essentially became outdated, which is where AES was brought to life in 1997 (Bernstein, 2021). The need for an update will probably come at a time when quantum computing is relevant as brute force attacking this algorithm is extremely difficult.

## Certificate Generation



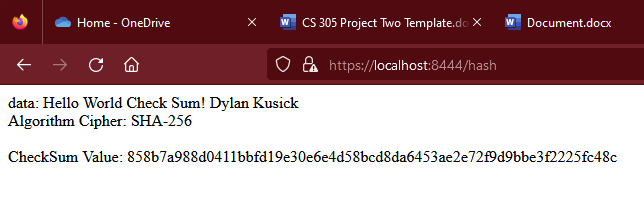


## Deploy Cipher

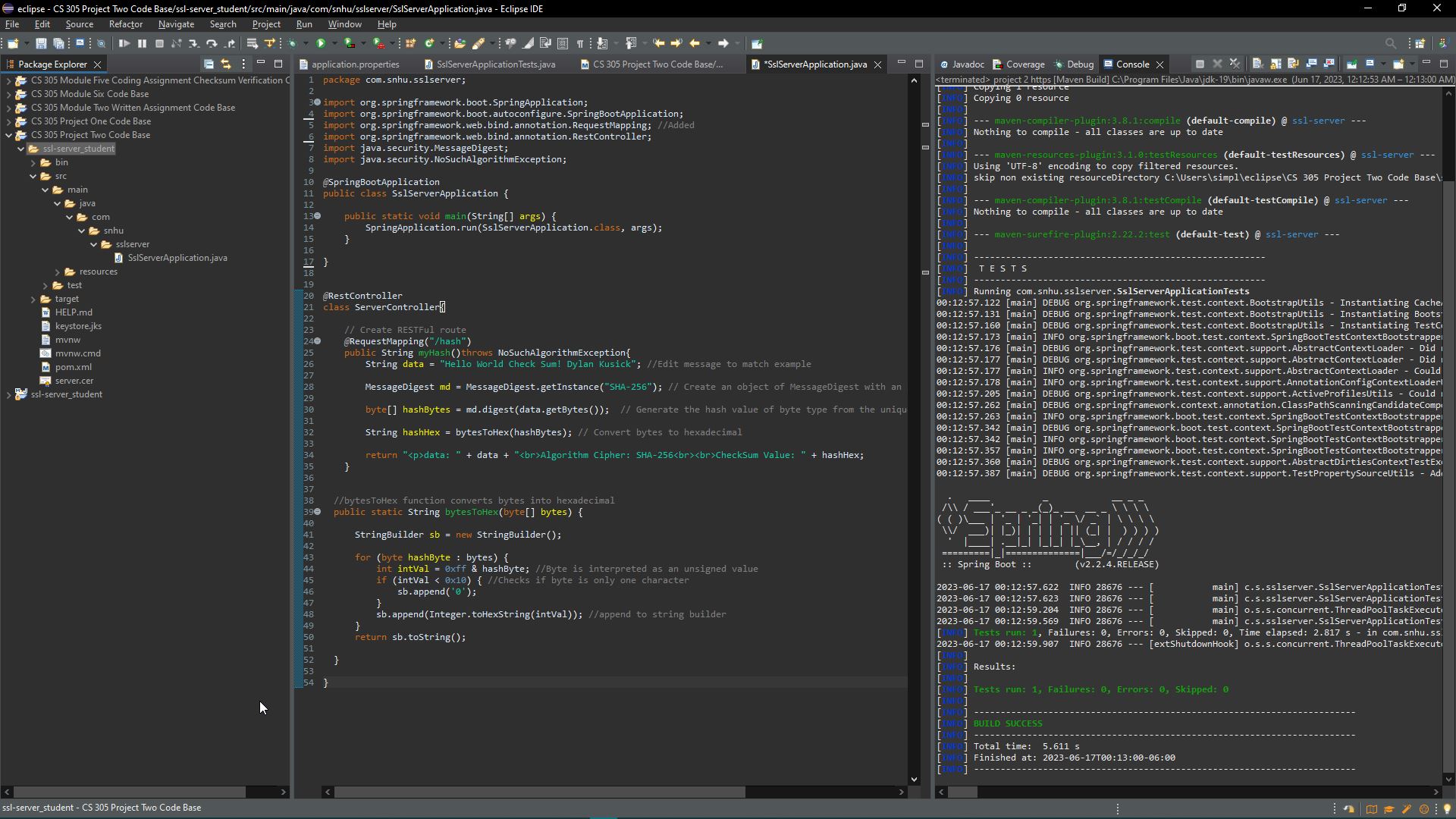


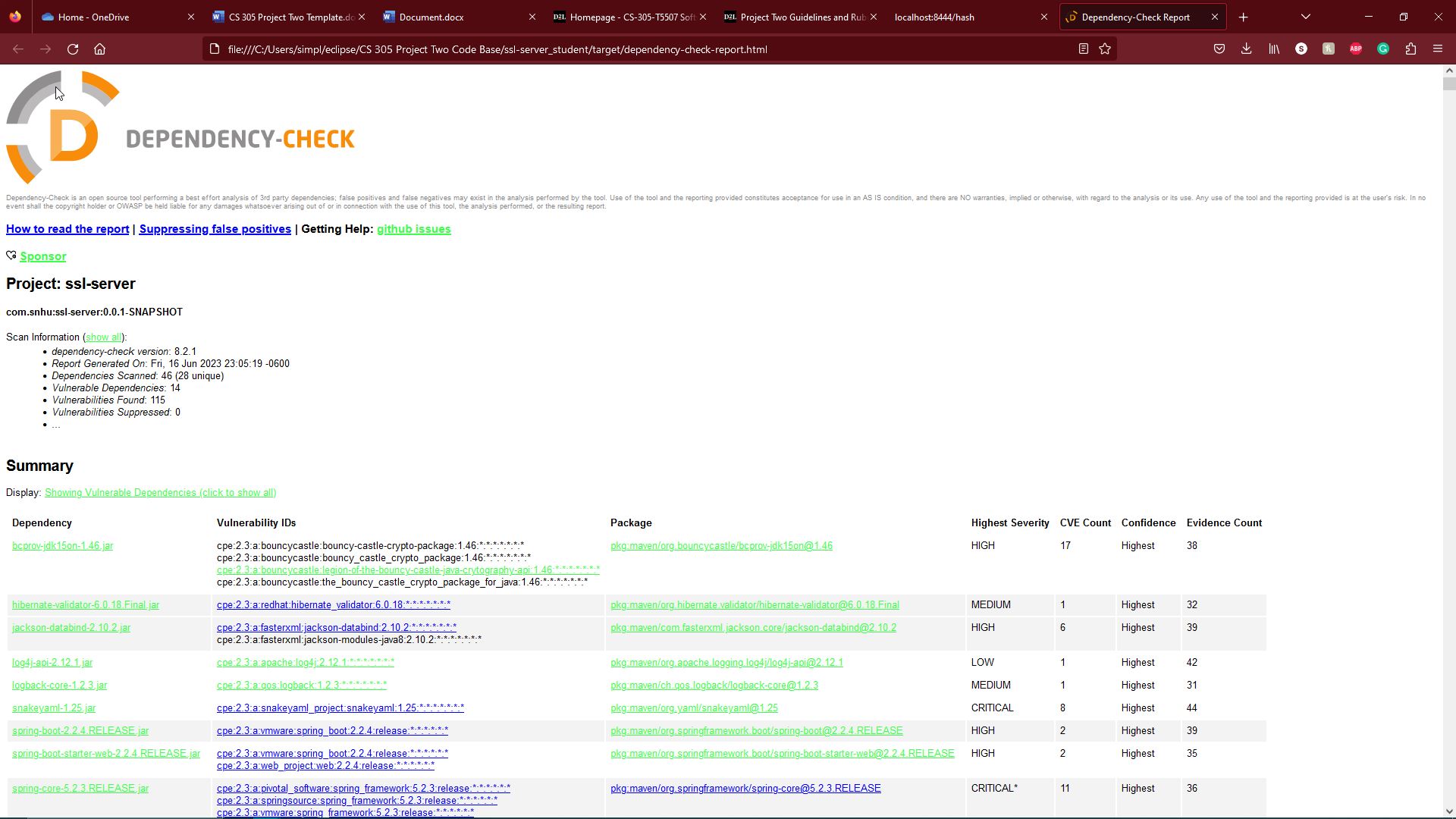
## Secure Communications

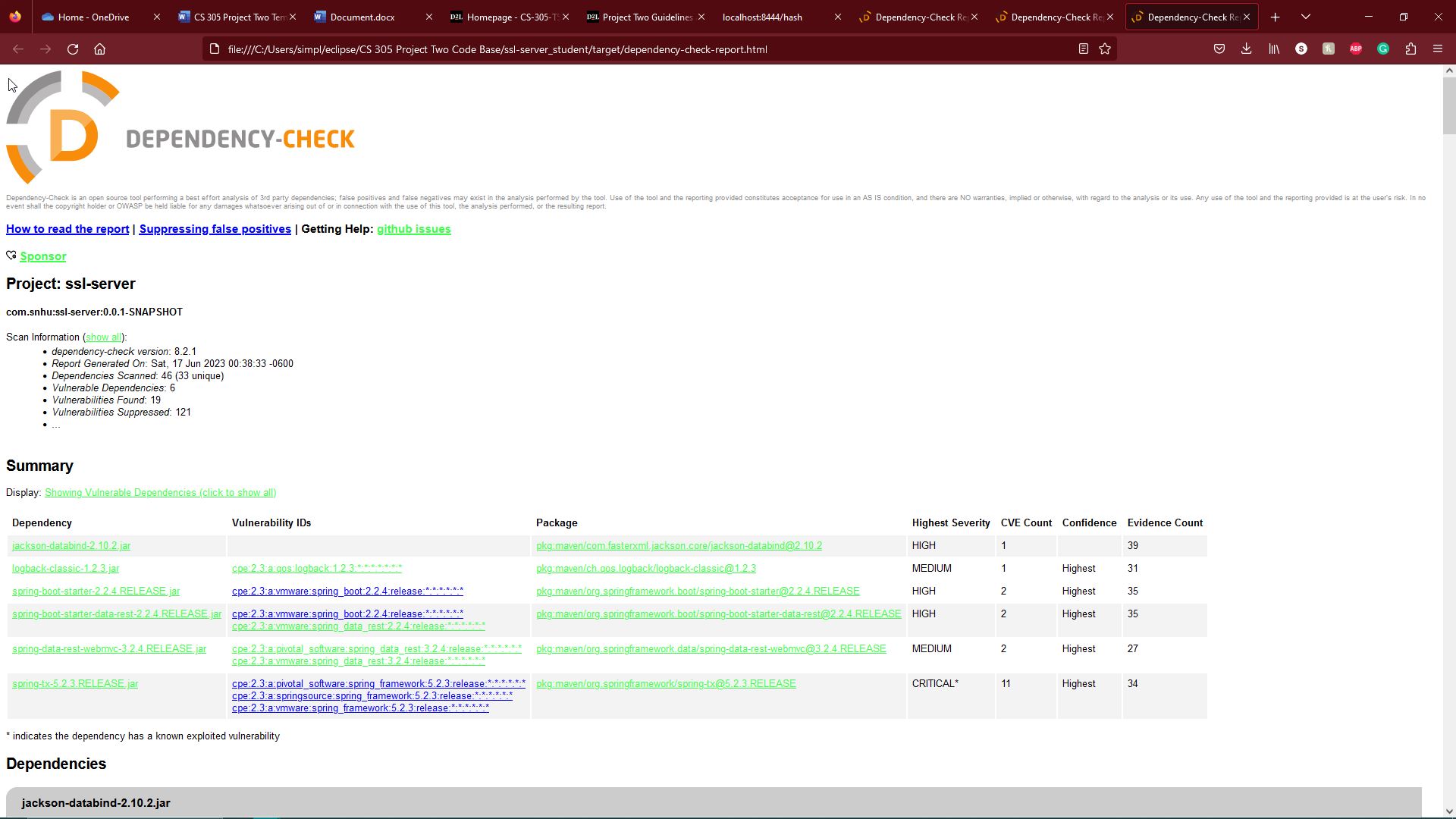
I made my message display on the 8444 port instead of 8443 as I was running into difficulties and was not sure how to close the port.



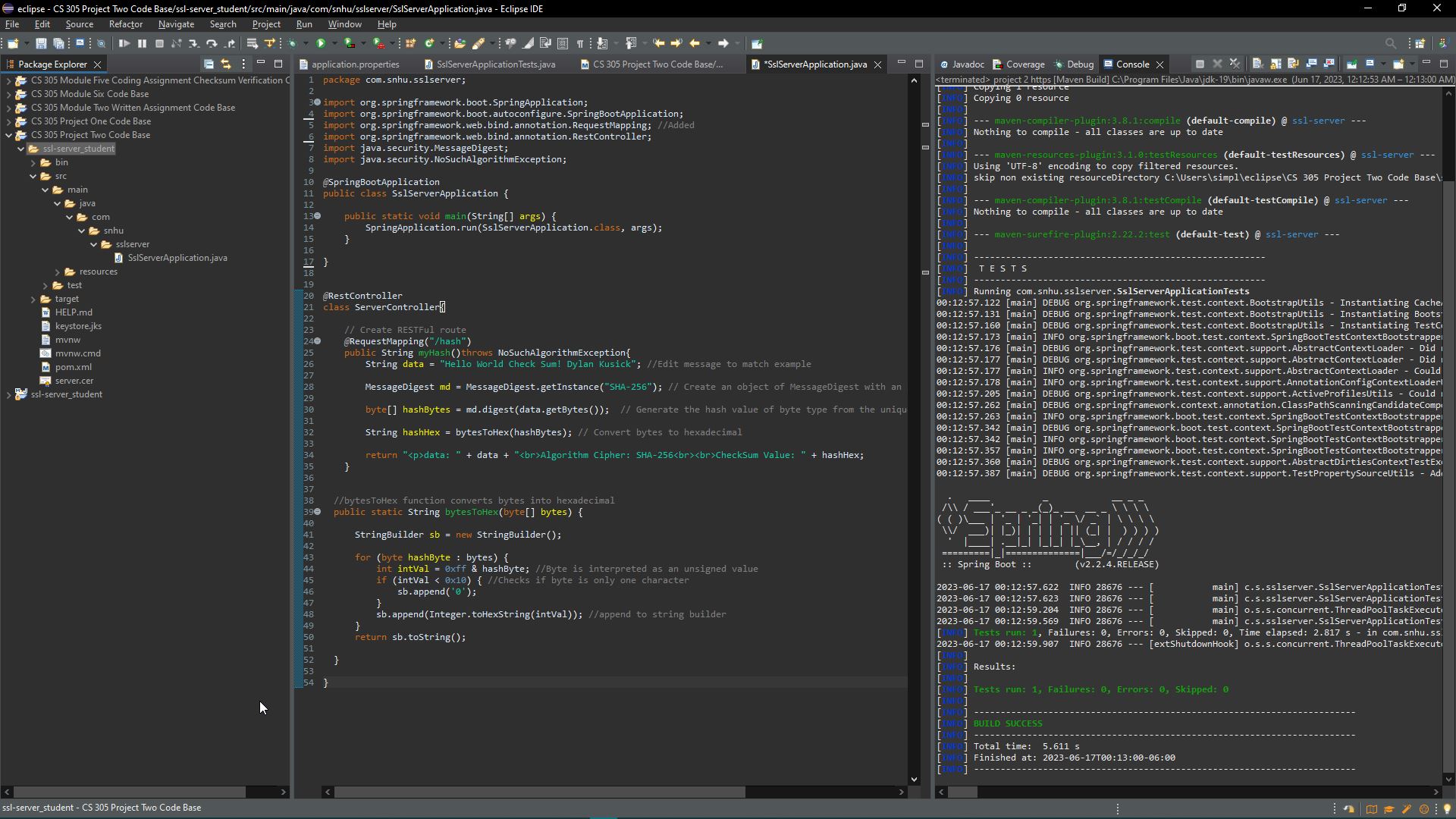
## Secondary Testing







## Functional Testing



## Summary

I addressed the encryption aspect of the Vulnerability Assessment Process Flow Diagram. Encryption is important for software like this due to the sensitive nature of the content that is being worked with. If there was no encryption, things like identity theft and fraud would be prevalent. This is because encryption is going to take the information that is on the system and jumble it into ciphertext, so the attacker has no idea what the sensitive information is.

Another aspect of the diagram that I implemented was consistent quality code practices. Unfortunately, this is an aspect that could be skipped over due to developers not being concerned with security as much as they probably should be. This step will ensure that code is able to be looked at and maintained easily in case updates need to be applied or there is an issue with the code in the future.

## Industry Standard Best Practices

I ran a dependency check on the code to check for vulnerabilities that may exist and leave the system vulnerable to attacks. As we learned in previous modules, these attacks could lead to harm for both the business as well as the clients that use the system. Information like social security numbers, addresses, card information, etc., should be hidden with some kind of encryption to ensure the physical and financial safety of everyone involved.

When systems contain information that is personal, it is important to take the necessary steps in the development process by using secure coding practices. Using coding practices that are not safe is like leaving the door open on your house; you wouldn’t leave your house vulnerable, so do not leave your system vulnerable. Encryption can make a world of difference for security, people that use your system, and people that maintain your system in the future, will thank you.

References

Bernstein, C., & Cobb, M. (2021, September 24). *What is the Advanced Encryption Standard (AES)? definition from searchsecurity*. Security. <https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard>

Jena, B. K. (2023, February 9). *What is AES encryption and how does it work? - simplilearn*. Simplilearn.com. <https://www.simplilearn.com/tutorials/cryptography-tutorial/aes-encryption>

Poggi, N. (2021, June 15). *Types of Encryption: Symmetric or Asymmetric? RSA or AES?*. Prey Blog. <https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes>