

# Practices for Secure Software Report

Table of Contents

￼

￼

￼

￼

￼

￼

￼

￼

￼

￼

￼

￼

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **02/19/23** | **Christina Roki** |  |

## 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

Christina Roki

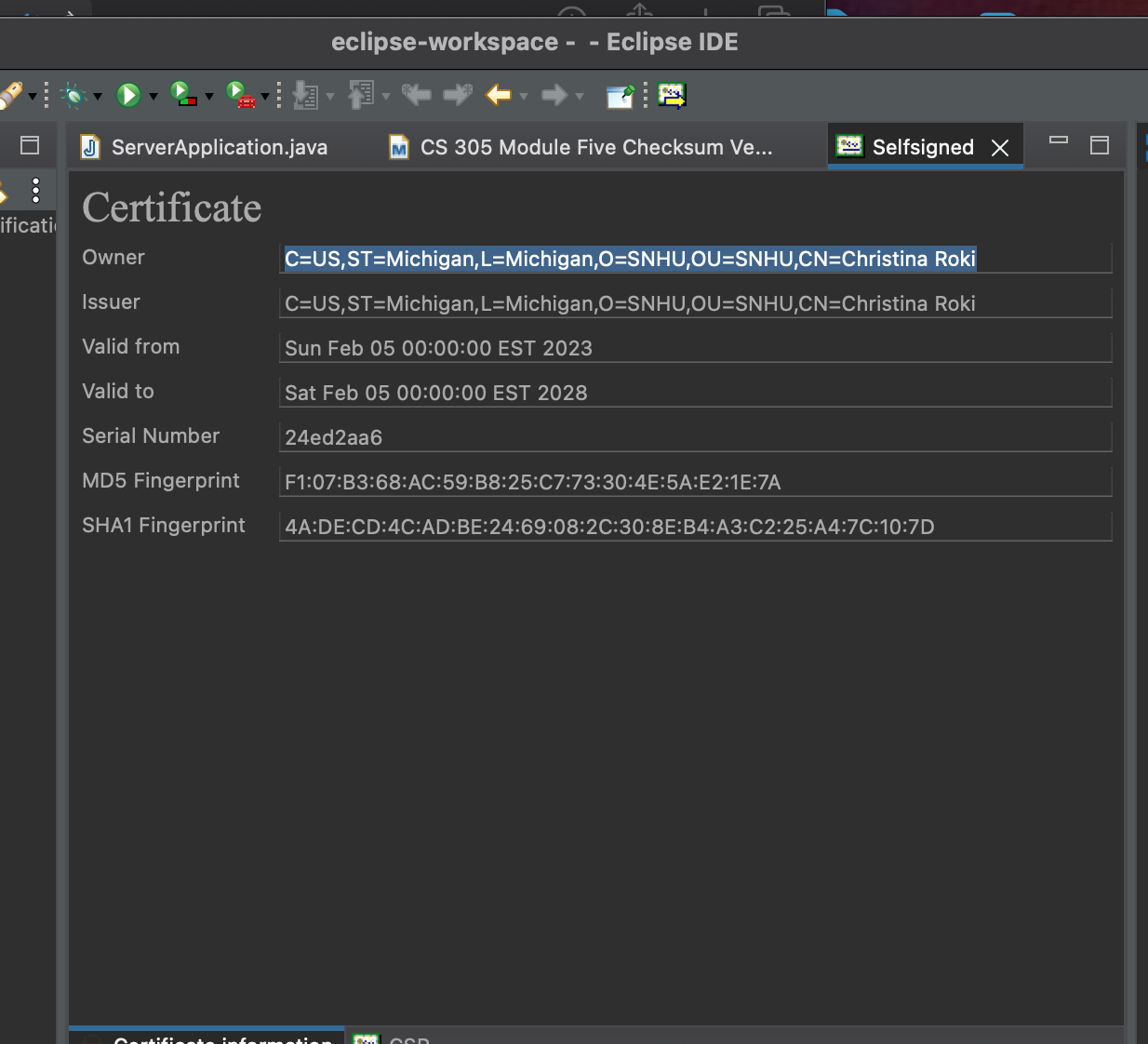
## Algorithm Cipher

As Artemis Finacial is a consulting company that develops individualized plans for their clients, it is agreed that individual files must be protected, even non-active, archived files. With a thorough review of the company’s vulnerabilities, the Advanced Encryption Standard is best recommended. As this is a very well-known cipher—recognized by NIST as FIPS-approved which stands for Federal Information Processing Standards (Morris J. Dworkin et al., 2001). This means it is safe enough even for governmental files, ensuring it will be safe for individual files from Artemis Financial. AES is reliable to go against many security attacks. WinZip Enterprise states brute force attacks are nearly impossible to happen since AES will have 2^256 possible combinations (2021).

Of course, each cipher will have its own disadvantages and it is fair to say that technology does advance by day. This means that there will be a potential possibility for a quantum computer to decrypt the cipher. Though, in order to be able to encrypt and decrypt the data, both, the sender and receiver, must have access to the same key meaning it is a symmetric key cipher. Further to note, both parties must keep this key very secured. With that being said, AES cipher will be used to secure Artemis Finacial's archive files. This cipher uses multiple methods to stay secure. This includes but not limited to hash functions and rand() selected numbers. Overall, it is confident that AES will be the best choice for set data protections as the advantages weight over the disadvantages given for this company.

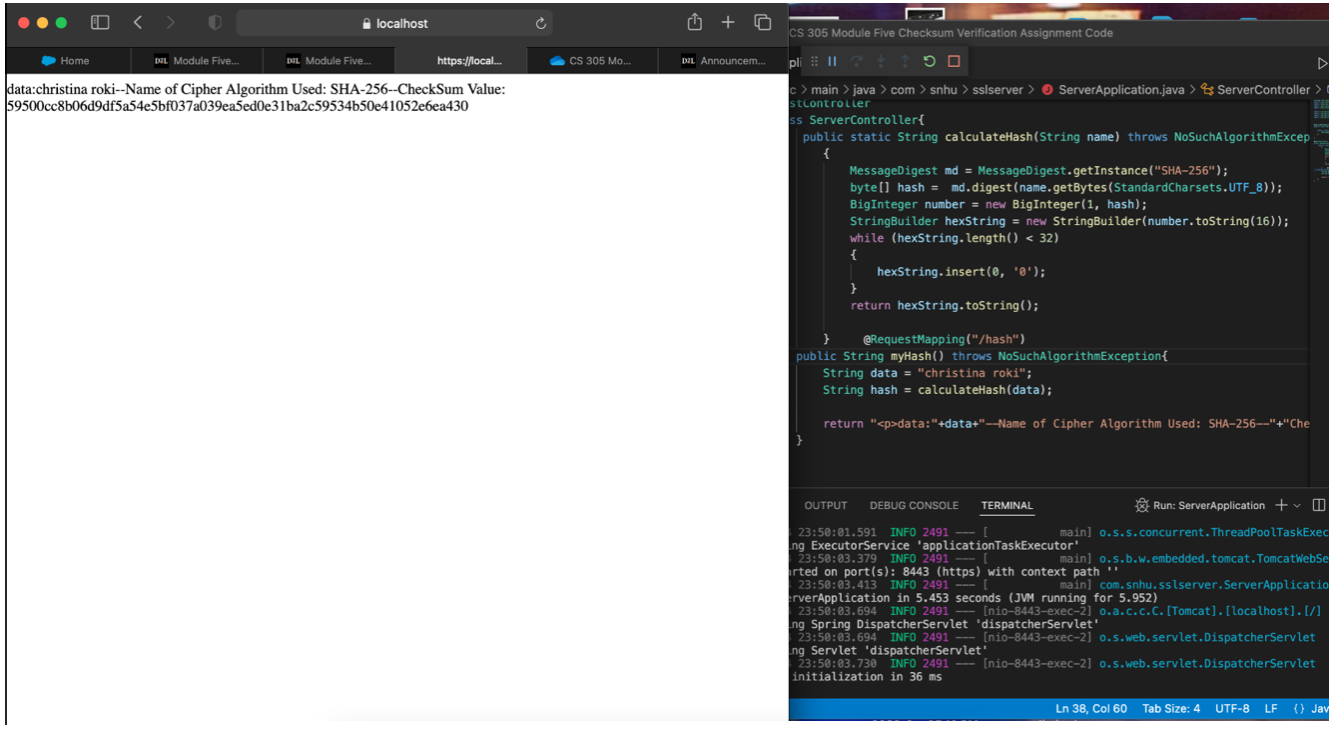
## Certificate Generation

Insert a screenshot below of the CER file.



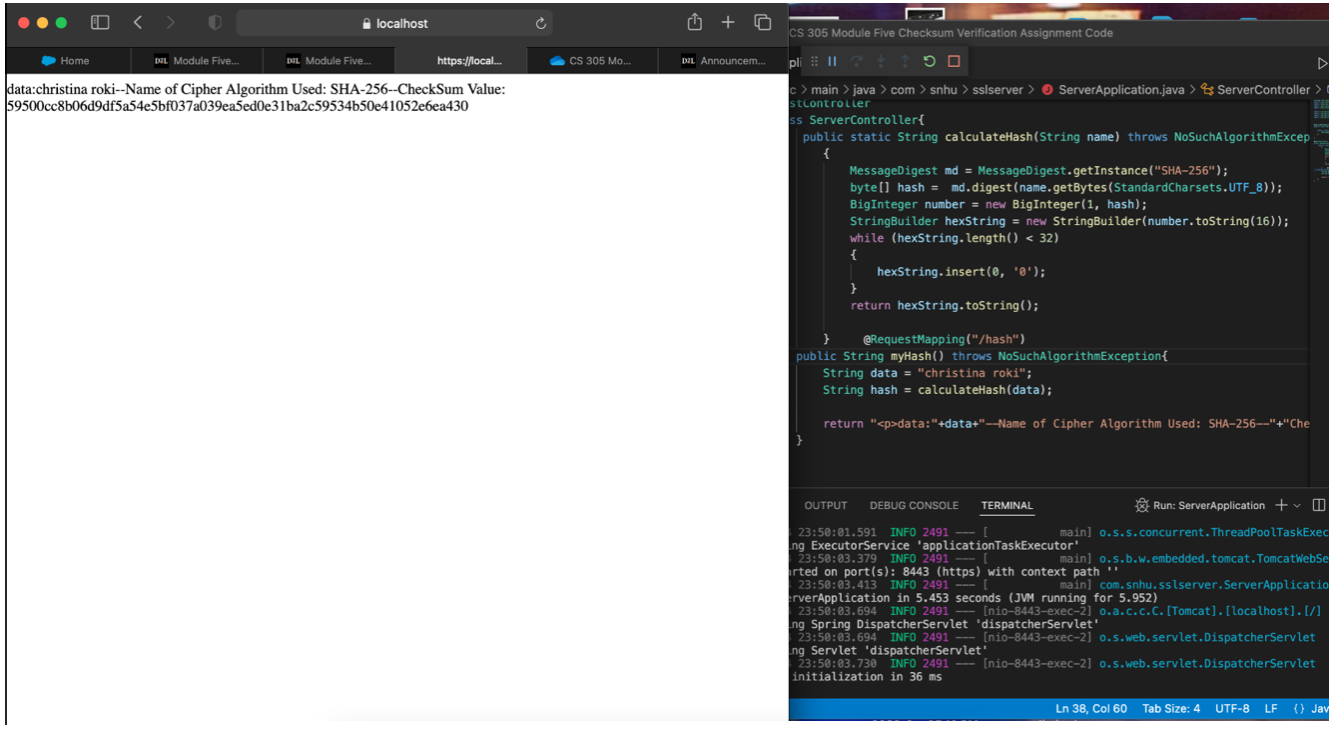
## Deploy Cipher

Insert a screenshot below of the checksum verification.



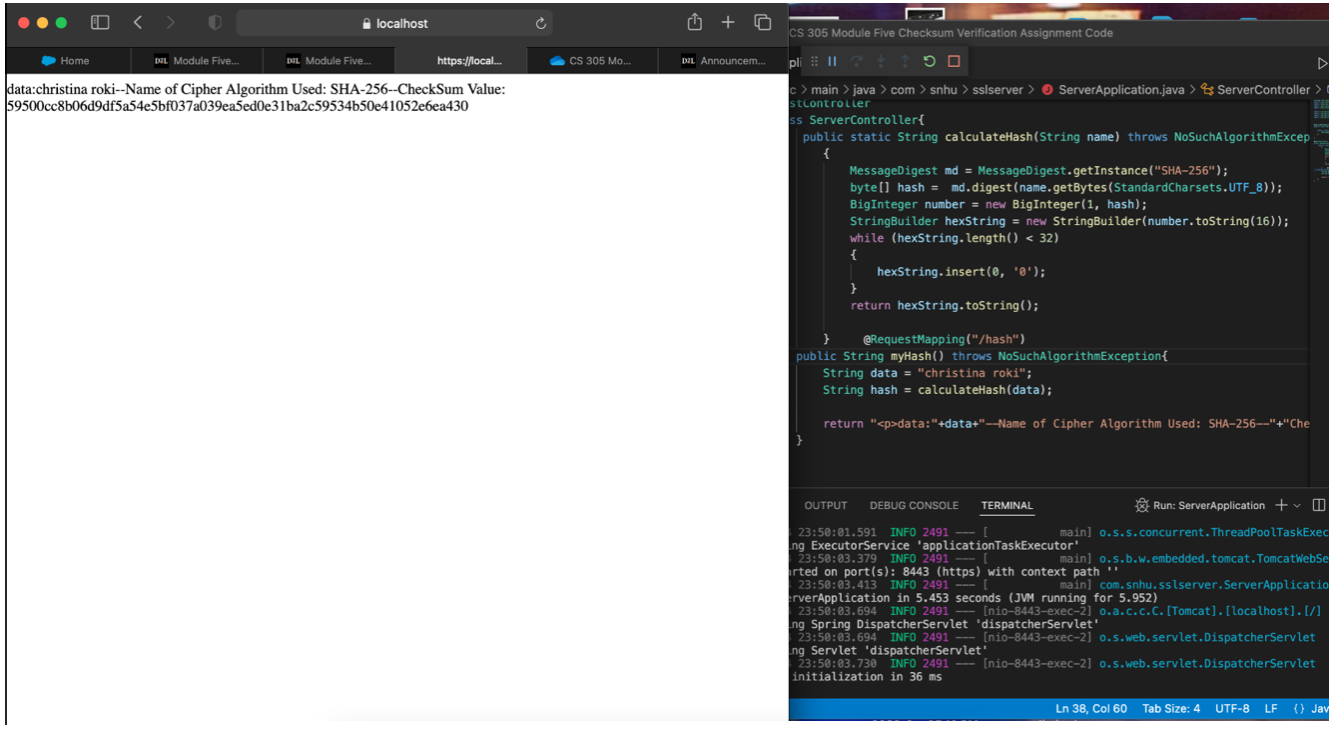
## Secure Communications

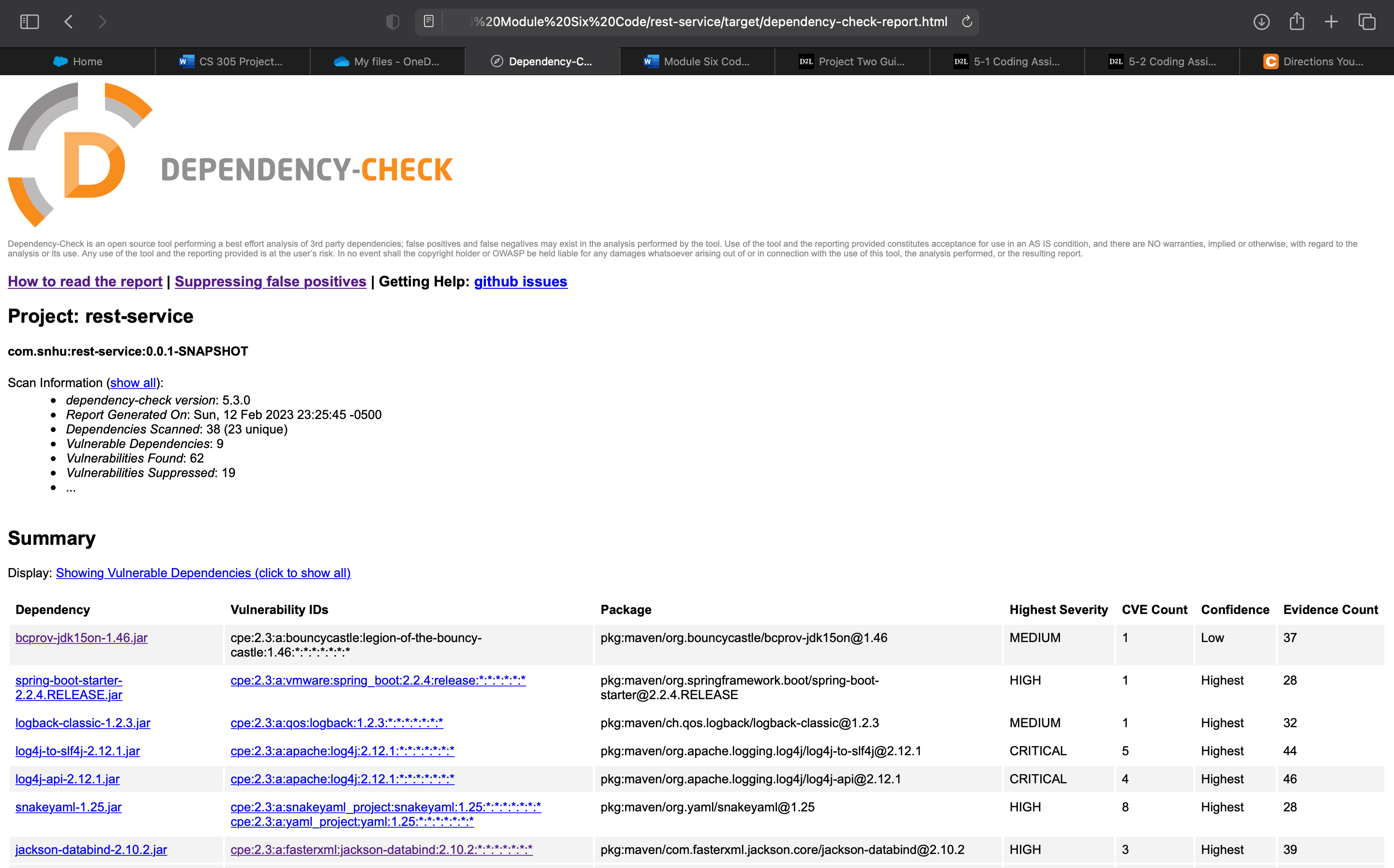
Insert a screenshot below of the web browser that shows a secure webpage.



## Secondary Testing

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

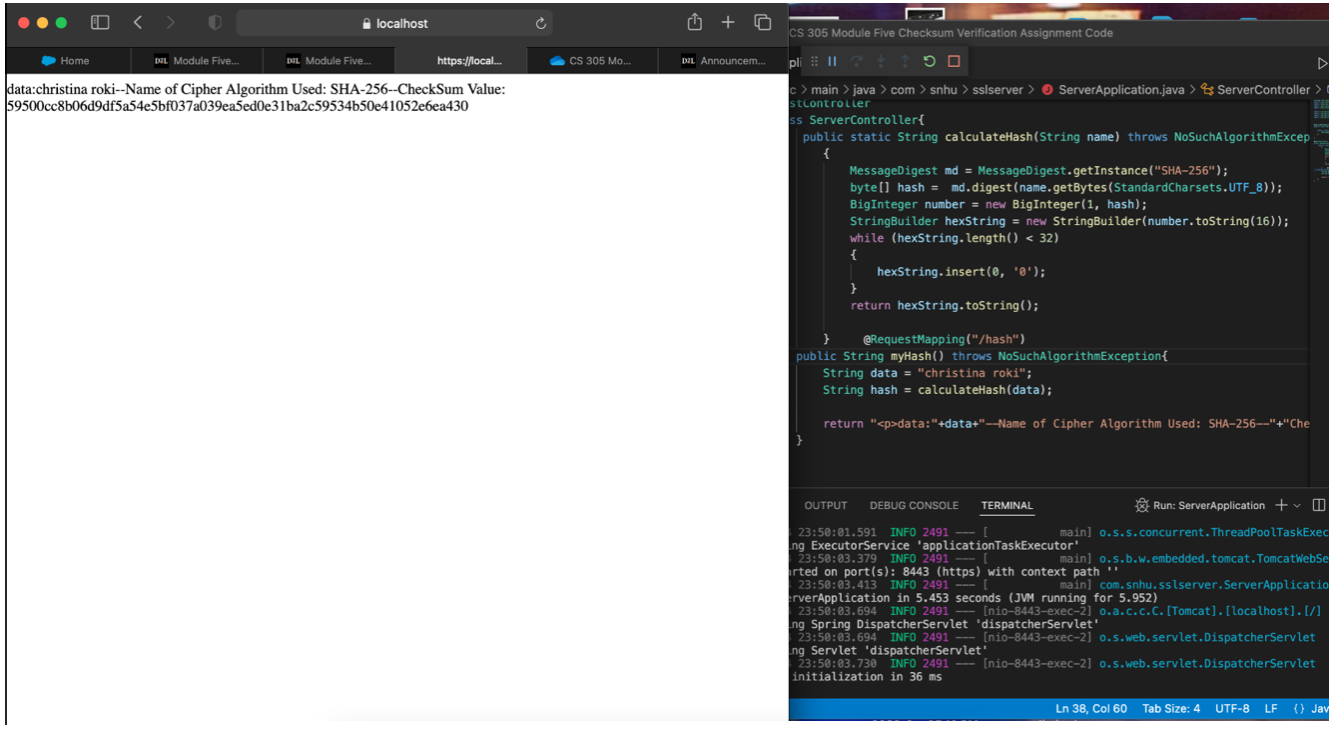




There was a total of 8 vulnerable dependencies found from the dependency-check report before reconfiguration. To start off, Bouncy Castle Crypto package has a timing issue that puts up the risk of certain attacks. Eventually, the Information Security Group released a paper stating the algorithms that were created from these timing issues (AlFardan & Paterson, 2013). There was also a vulnerability with Spring Boot; however, this only affected certain versions. Another version-issued vulnerable package was in log-back core that allowed attackers to modify configurations. Apache Log4j API was vulnerable to a middleman attack that gave the attacker the opportunity to leak any log messages. Luckily, this was fixed with newer versions. There was another version error with SnakeYAML. In the Jackson Databind, there was a potential data integrity issue which NetApp mentioned was resolved in newer versions (2021). Core Tomcat also had a vulnerability where certain data were processed incorrectly in specific versions. Lastly, there was another version specific error with Hibernate Validator which caused a bug in messages.

## Functional Testing

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



## Summary

The sender encrypts the communication before sending it, and the recipient must decode the message before processing it. The process of encrypting and decrypting data is known as "public key encryption." One or more of the communicating parties must have a means of demonstrating to the other that they are, in fact, who they say they are for public key encryption to allow secure communication. This verification is given by SSL, which demands that at least one party submit a digital certificate during the connection's first negotiation before any encrypted data is sent. This action is referred to as "handshaking."

## Industry Standard Best Practices

Embedded systems are used in a variety of sectors as computers becomes more prevalent, including industrial systems, crucial infrastructure, private and public environments, as well as portable and wearable applications. These systems' ability to store, access, and transmit private, delicate, or even crucial information is essential to their performance. As a result, a crucial issue that must be taken into account during the design of those devices is the confidentiality and integrity of their resources and services.

**References**

Dworkin, M. J., Barker, E. B., Nechvatal, J. R., Foti, J., Bassham, L. E., Roback, E., & Jr., J. F. D. (2021, March 1). *Advanced encryption standard (AES)*. NIST. Retrieved January 29, 2023, from <https://www.nist.gov/publications/advanced-encryption-standard-aes>

Blog, W. Z. (2021, October 22). *Articles*. WinZip Enterprise Blog. Retrieved January 29, 2023, from <https://winzip.com/blog/enterprise/aes-encryption-explained/>

AlFardan, N. J., & Paterson, K. G. (2013, February 27). Lucky Thirteen: Breaking the TLS and DTLS record protocols. Retrieved February 13, 2023, from <http://isg.rhul.ac.uk/tls/TLStiming.pdf>

*CVE-2020-25649 fasterxml Jackson Databind vulnerability in Netapp Products: Netapp product security*. CVE-2020-25649 FasterXML Jackson Databind Vulnerability in NetApp Products | NetApp Product Security. (n.d.). Retrieved February 12, 2023, from <https://security.netapp.com/advisory/ntap-20210108-0007/>