****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc241174976)

[Table of Contents 1](#_Toc1731048788)

[Document Revision History 2](#_Toc1653830012)

[Client 3](#_Toc1372947671)

[Instructions 3](#_Toc250132494)

[Developer 3](#_Toc1033559998)

[1. Algorithm Cipher 4](#_Toc1837427327)

[2. Certificate Generation 4](#_Toc2037629003)

[3. Deploy Cipher 4](#_Toc2131450445)

[4. Secure Communications 5](#_Toc733582547)

[5. Secondary Testing 5](#_Toc1636634350)

[6. Functional Testing 6](#_Toc1300446819)

[7. Summary 7](#_Toc56321460)

[8. Industry Standard Best Practices 7](#_Toc10758866)

[References 8](#_Toc1498912100)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **2/17/2023** | **Kate Doughty** |  |

## 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

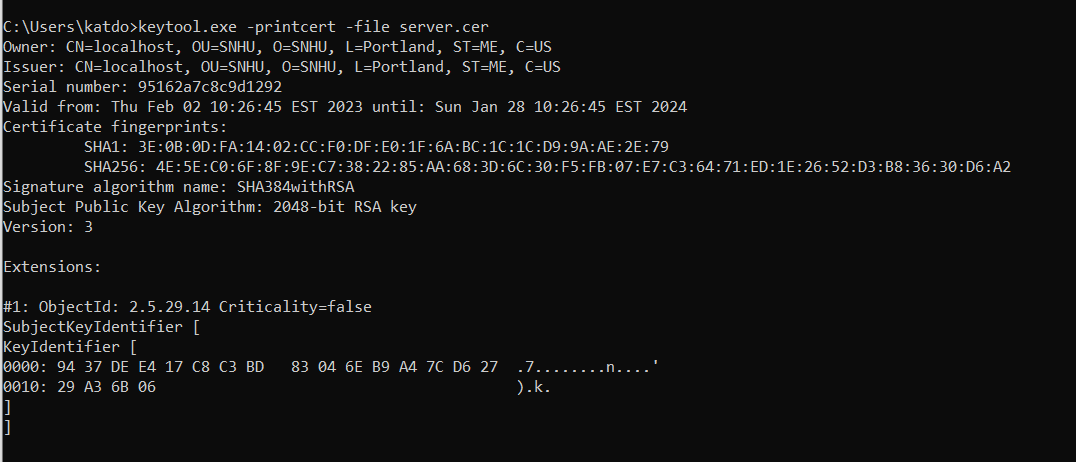
Kate Doughty

## Algorithm Cipher

For Artemis Financial, I recommend SHA-256 for the cipher. SHA-256 is incredibly secure, as it is unlikely for the hash values to be reversed, and it is collision resistant (What Is SHA256, How Does It Work, and Why Is It So Important? - Faisal Khan, 2023). A hash function is an algorithm that translates a message into a hash value, which is a string of letters and numbers that are incomprehensible. Bit levels indicate how many attempts an attacker might need in a brute force attack. The higher the bit level, the more possibilities there are. In this case, randomness equals security. Having random numbers and letters makes it more difficult for attackers to guess, infer, or predict what an encrypted message is. Symmetric encryption uses the same key to decrypt as it uses to encrypt, while asymmetric uses a different key to decrypt (Manico & Detlefsen, 2014). Currently, SHA-256 is one of the most secure ciphers, as it is unfeasible to crack.

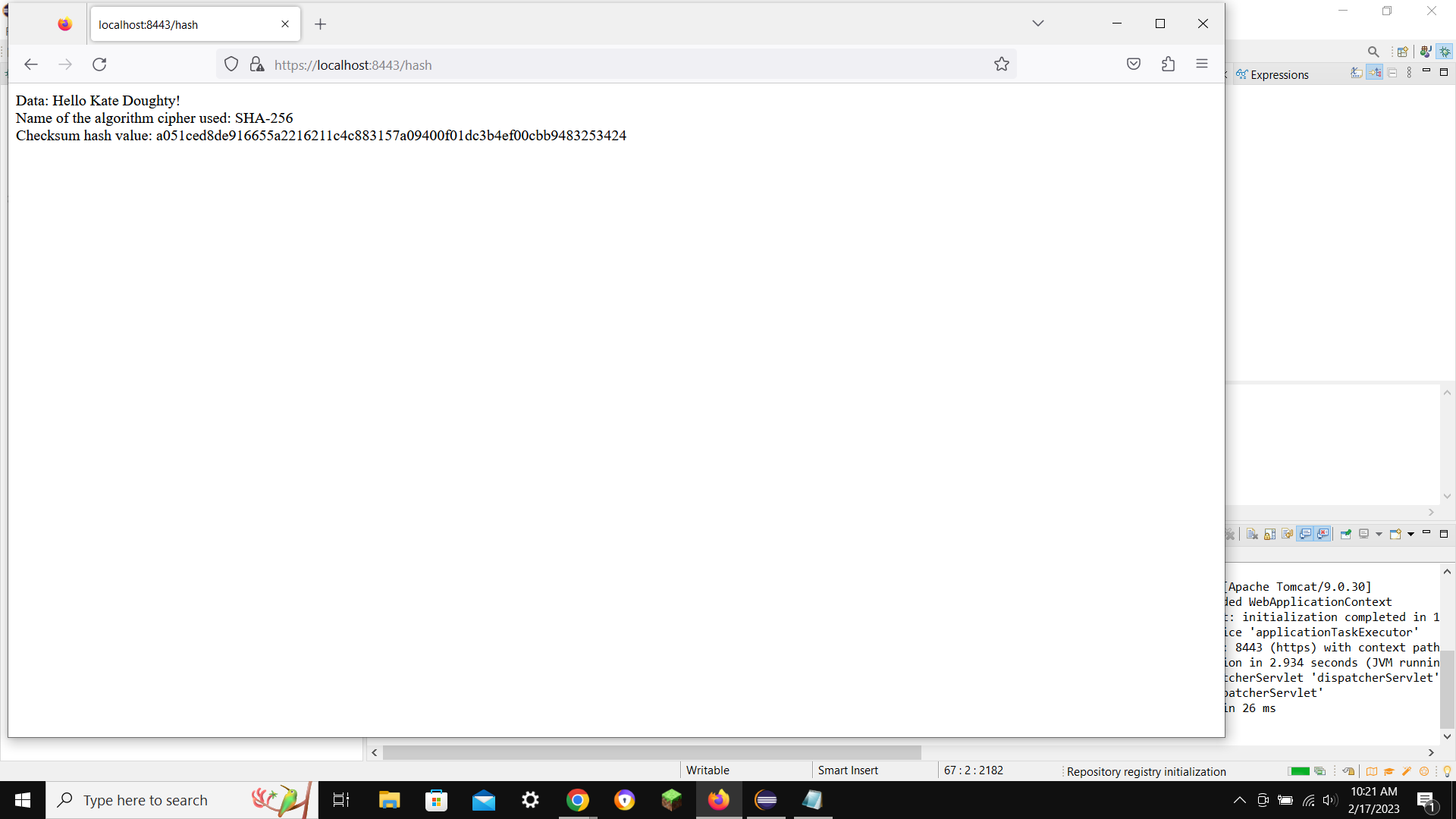
## Certificate Generation

Insert a screenshot below of the CER file.



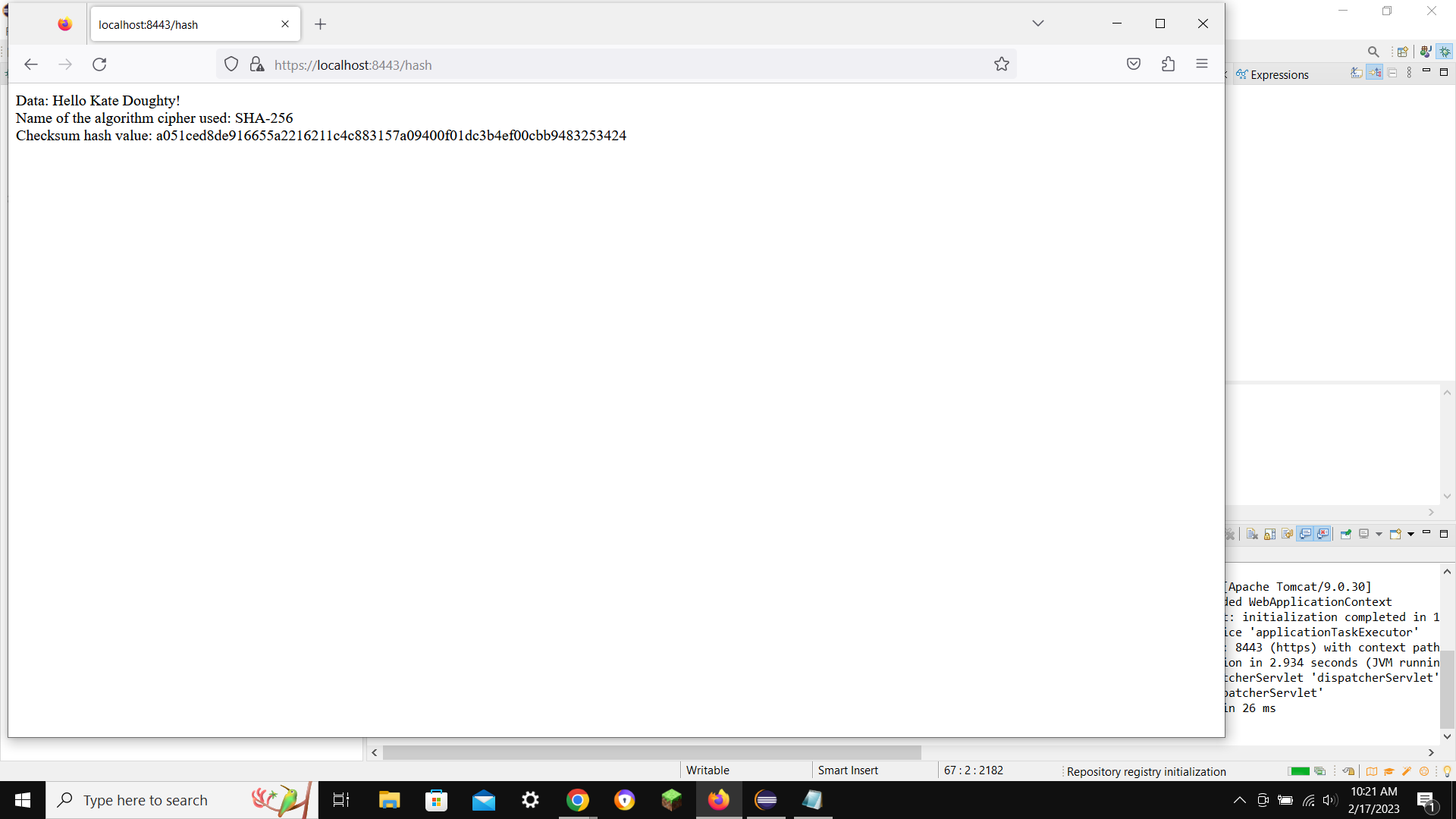
## Deploy Cipher

Insert a screenshot below of the checksum verification.



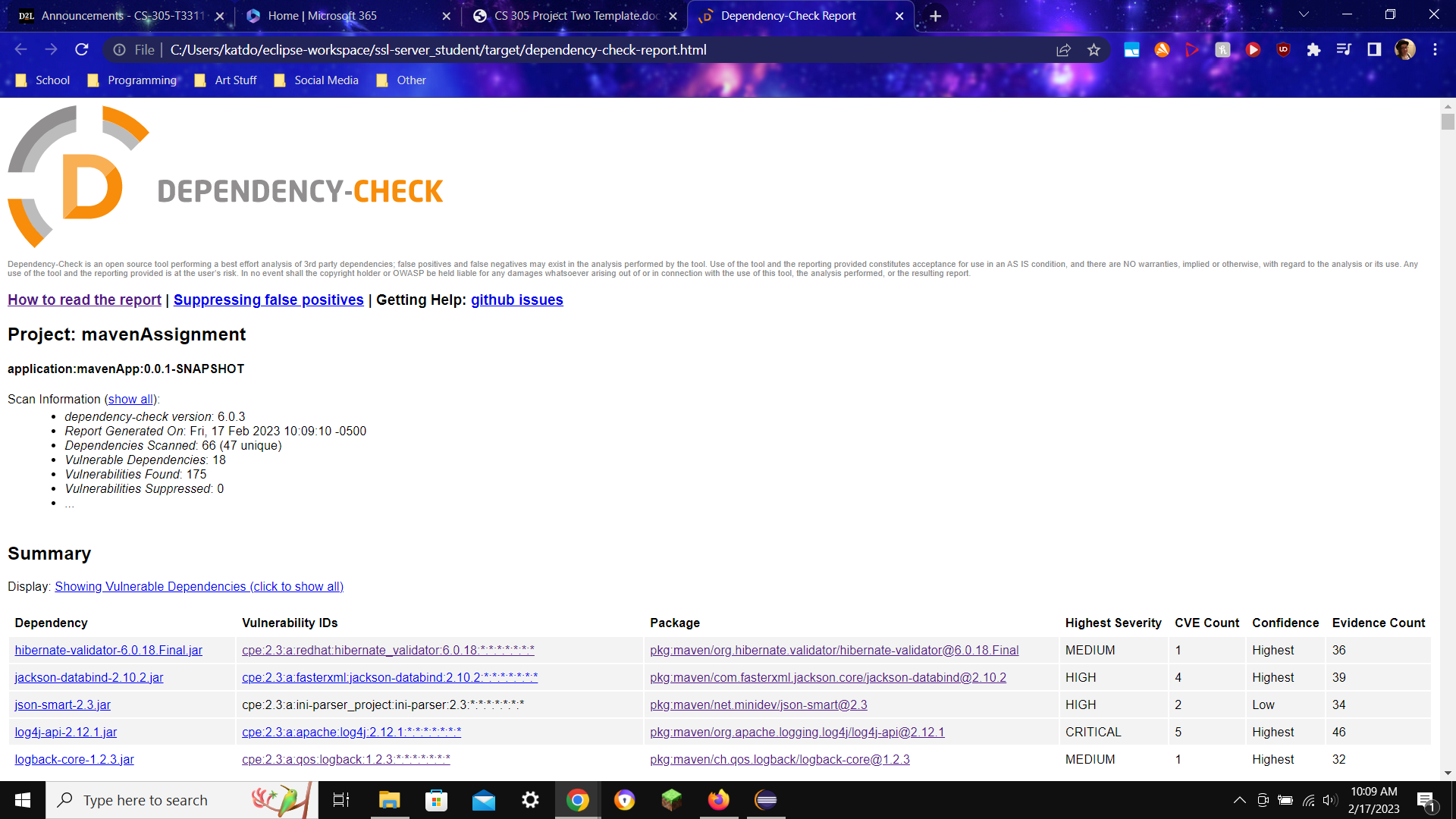
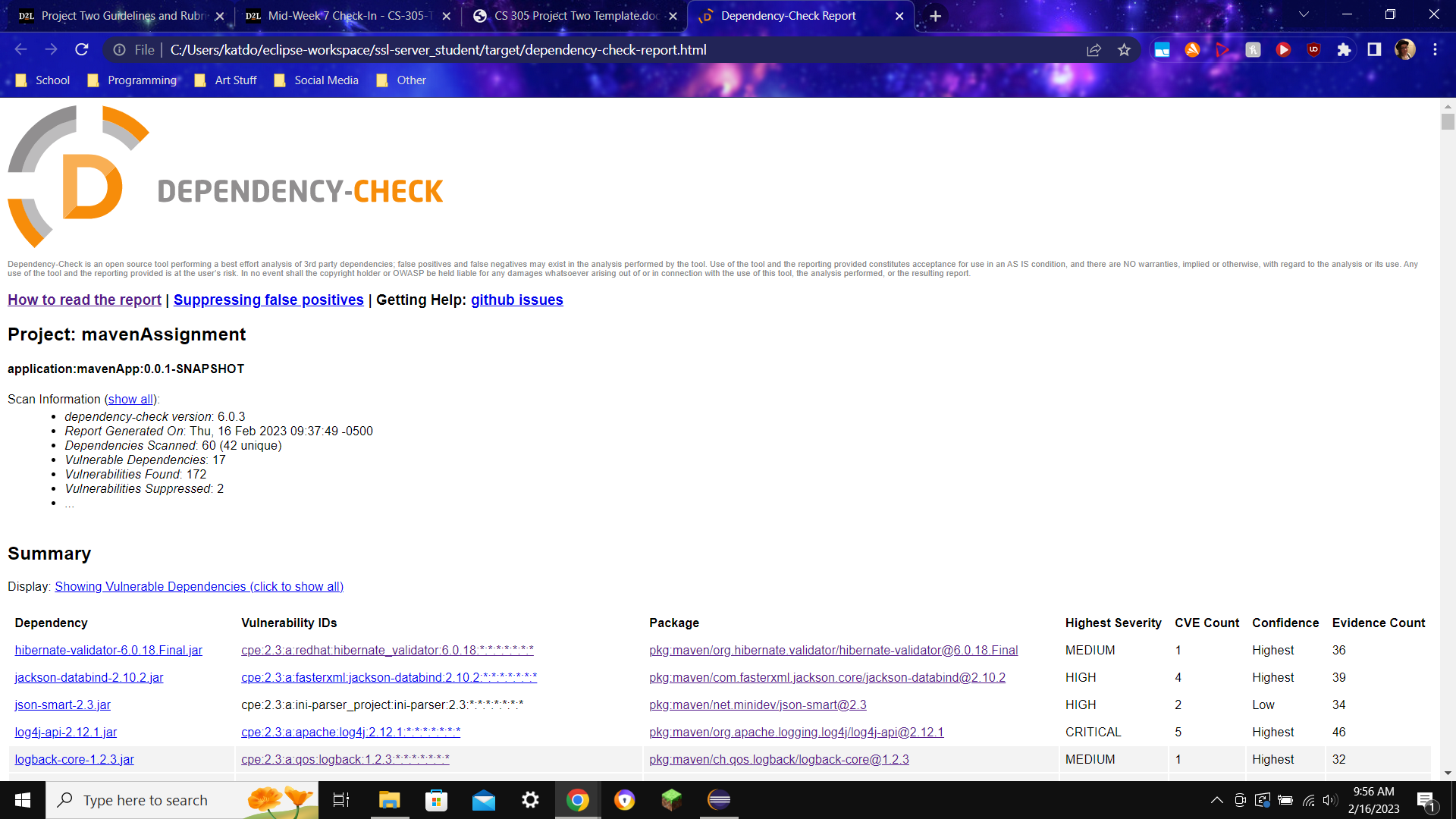
## Secure Communications

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



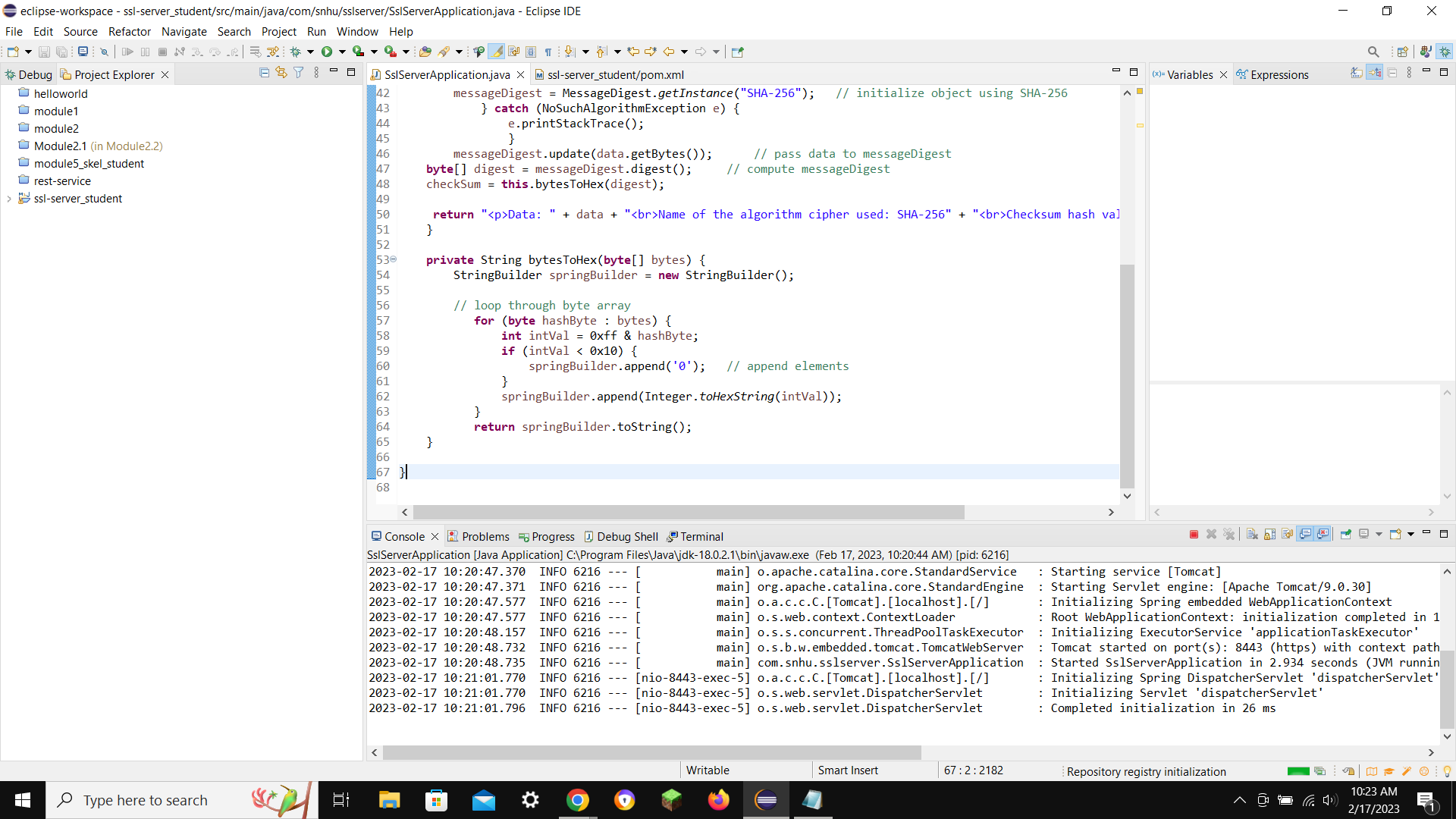
## Secondary Testing

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



## Functional Testing

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



## Summary

The first step I took for adding security was generating self-signed certificates, which allow the use of HTTPS, as secure communication and safety on the website are important for the business’ security and reputation. After, I added the security cipher and made sure it worked properly, which is important to scramble and shield user data. Finally, I performed a dependency check to make sure there were no vulnerabilities showing up that cannot be fixed.

## Industry Standard Best Practices

I did my best to keep the program clear and easy to follow, with proper white space and indentations, as well as following the standard naming conventions. I also commented summaries of my additions, so that other programmers can follow my work.

## References

Manico, J., & Detlefsen, A. (2014, September). *Iron-Clad Java [Book]*. O’Reilly Online Learning; McGraw Hill Computing. <https://learning.oreilly.com/library/view/iron-clad-java/9780071835886/?sso_link=yes&sso_link_from=SNHU>

*What is SHA256, how does it work, and why is it so important? - Faisal Khan*. (2023, January 2). Faisal Khan; <https://www.facebook.com/faisalkhanpaymentconsultant>. <https://faisalkhan.com/knowledge-hub/resources-and-references/what-is-sha256-how-does-it-work-and-why-is-it-so-important/>