****

# 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** | **8/10/2023** | **Matthew Bartrum** |  |

## 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

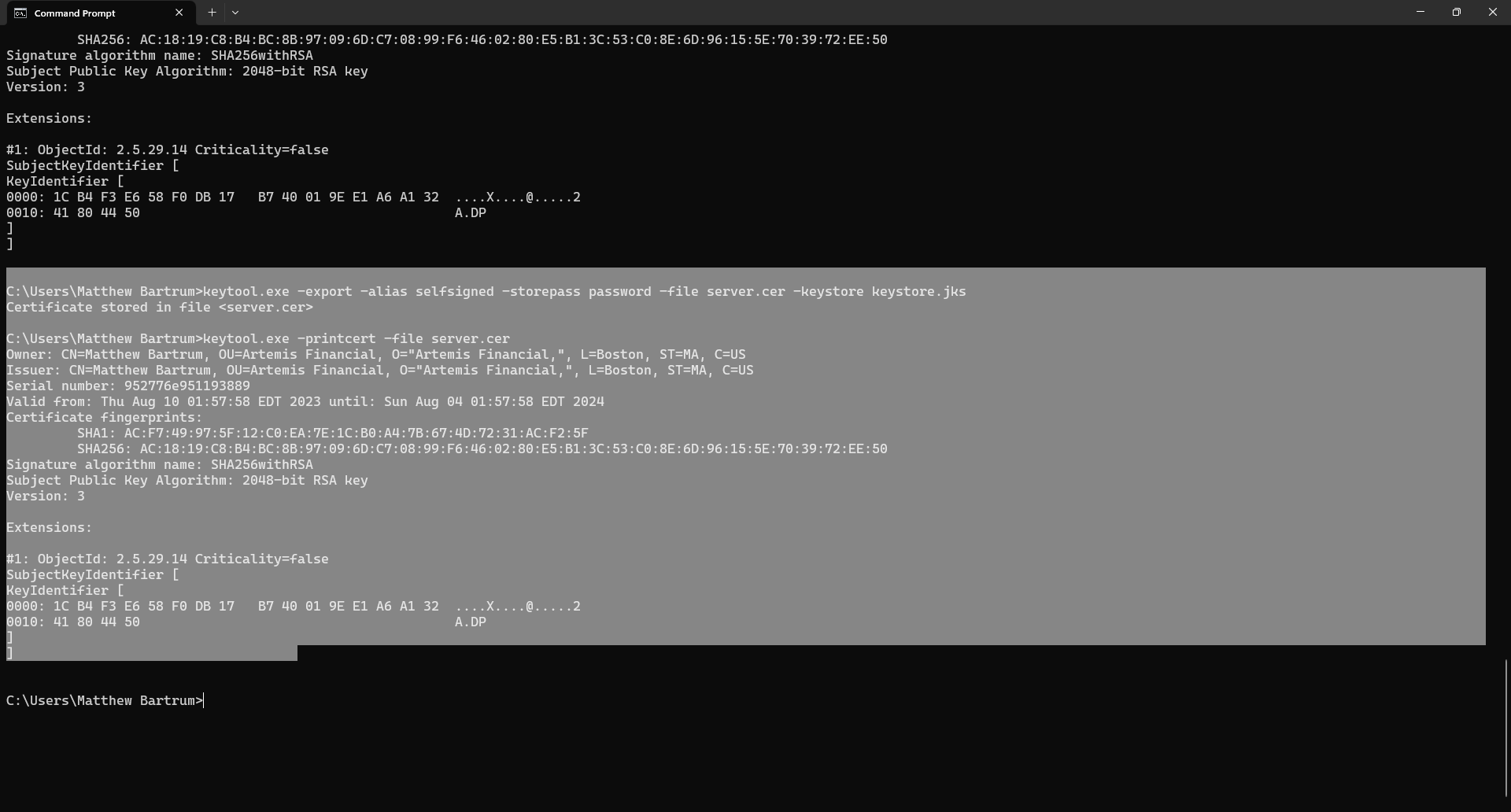
Matthew Bartrum

## Algorithm Cipher

AES will be the cipher algorithm for Artemis Financials. AES is one of the best cipher algorithms and even the government uses it to protect their information. It has three different blocks of cipher which are 128,192. And 256. The different bits represent that amount times it could take to break the system. AES does all symmetric encryption which breaks the code into fix size boxes then it does the crypto operations. With AES it is made to not be cracked because it is the highest bits we have. If someone was able to crack this, we would be in trouble because there are not many ways to fix these issues. With that being said it has been around a long time, and it has yet been cracked. AES finally is symmetrical key which allows for one key that can both encrypt and decrypt messages from the system. Which is very advance for today.

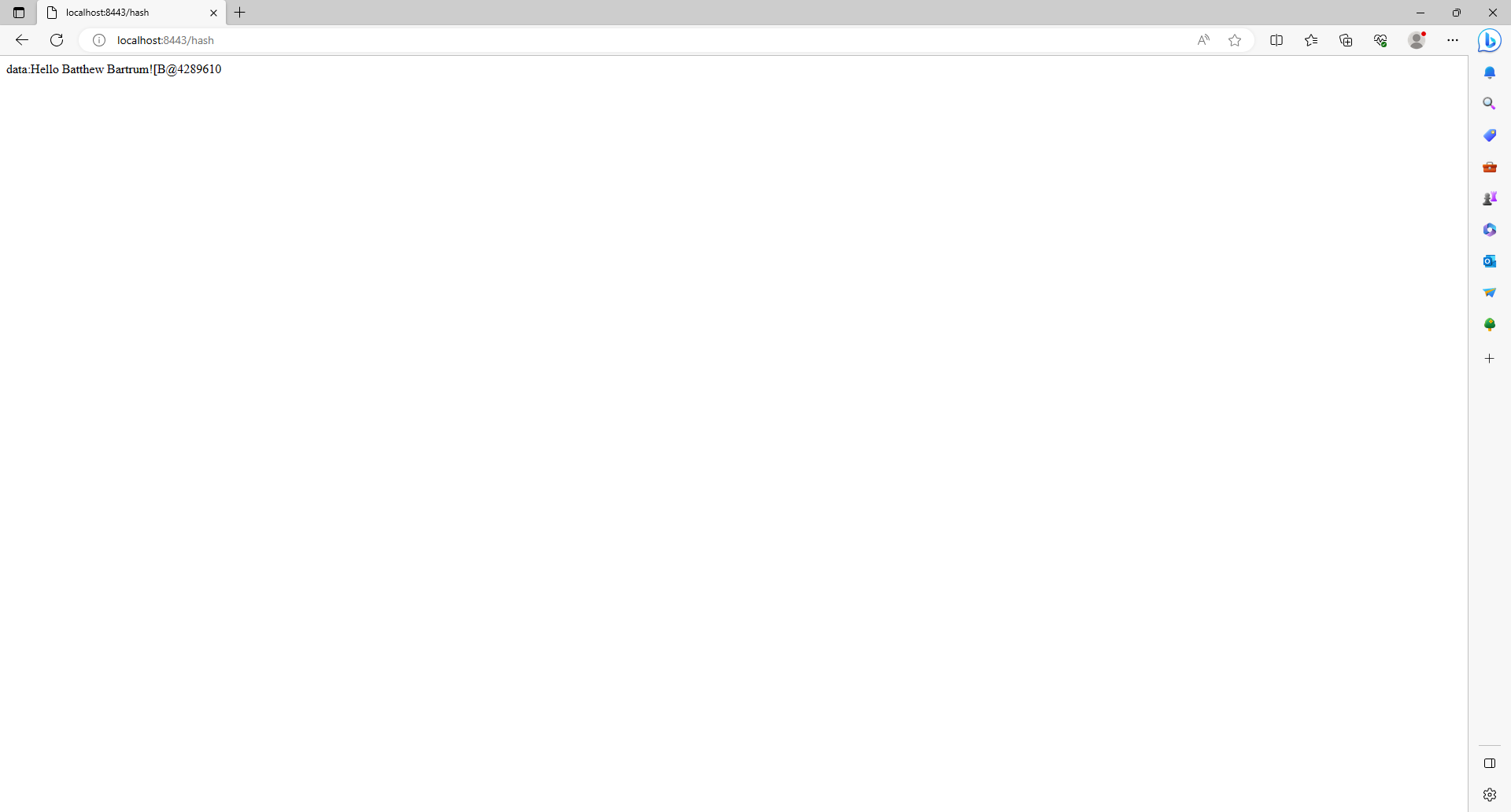
## Certificate Generation

Insert a screenshot below of the CER file.



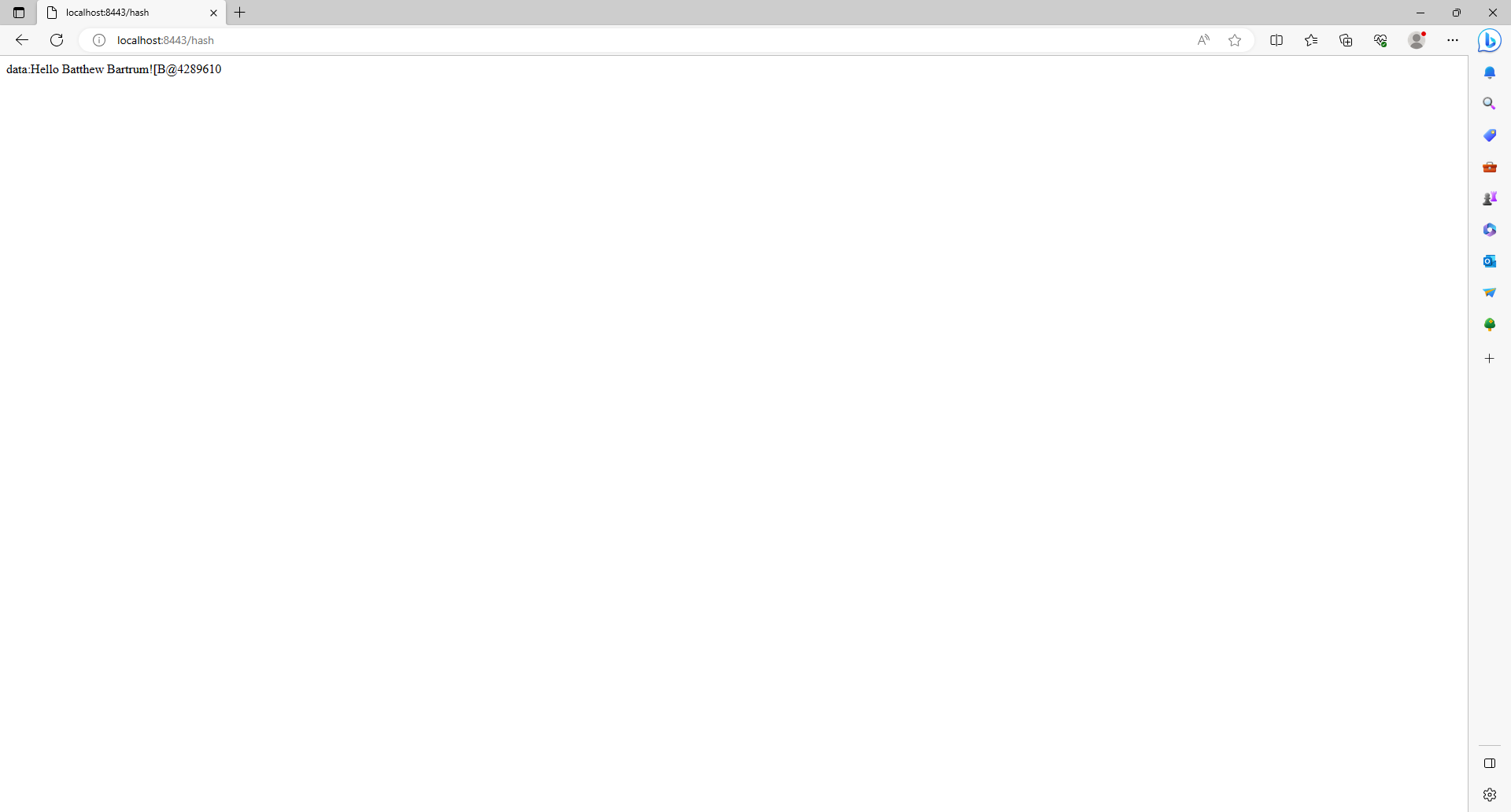
## Deploy Cipher

Insert a screenshot below of the checksum verification.



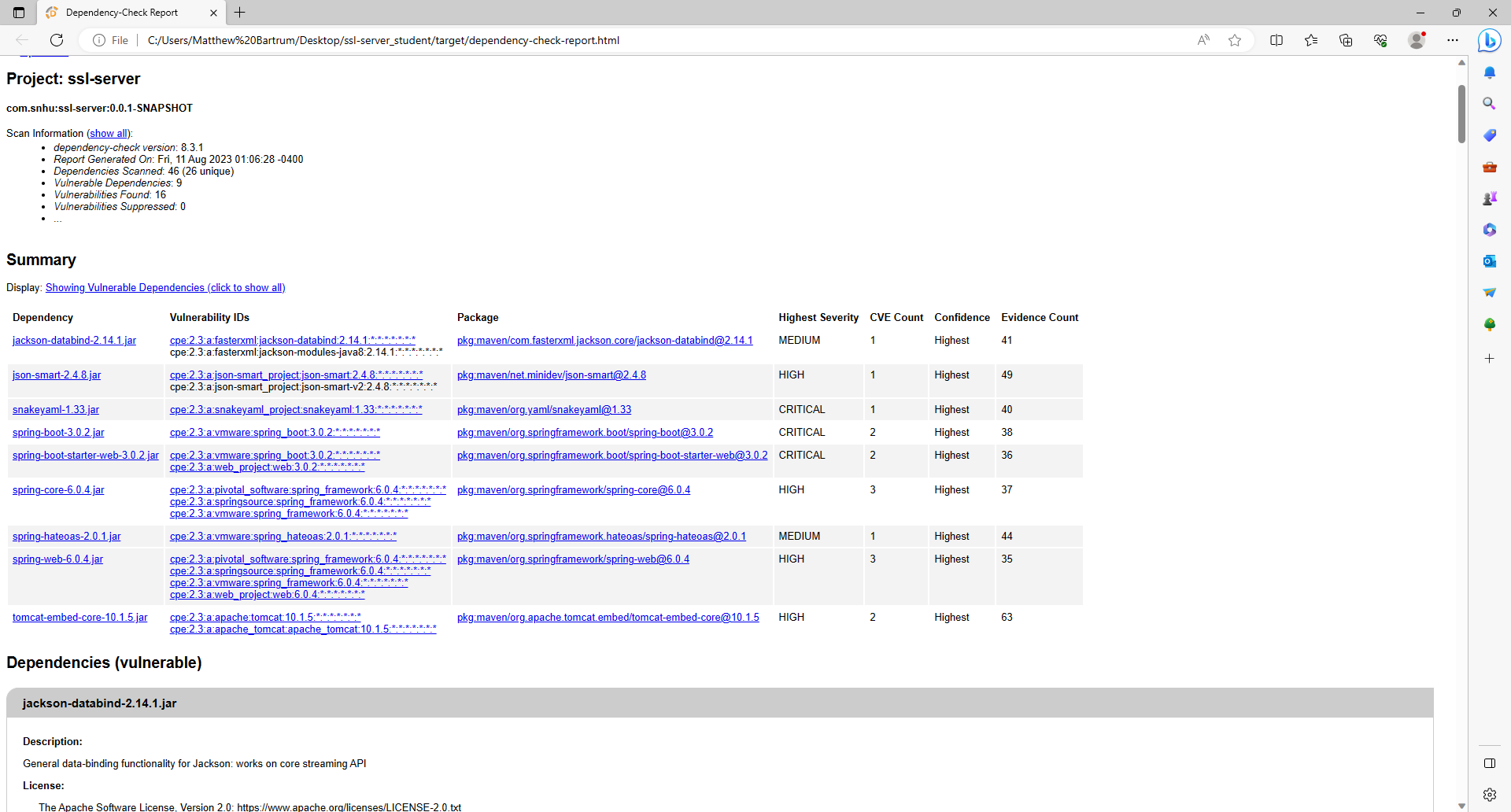
## Secure Communications

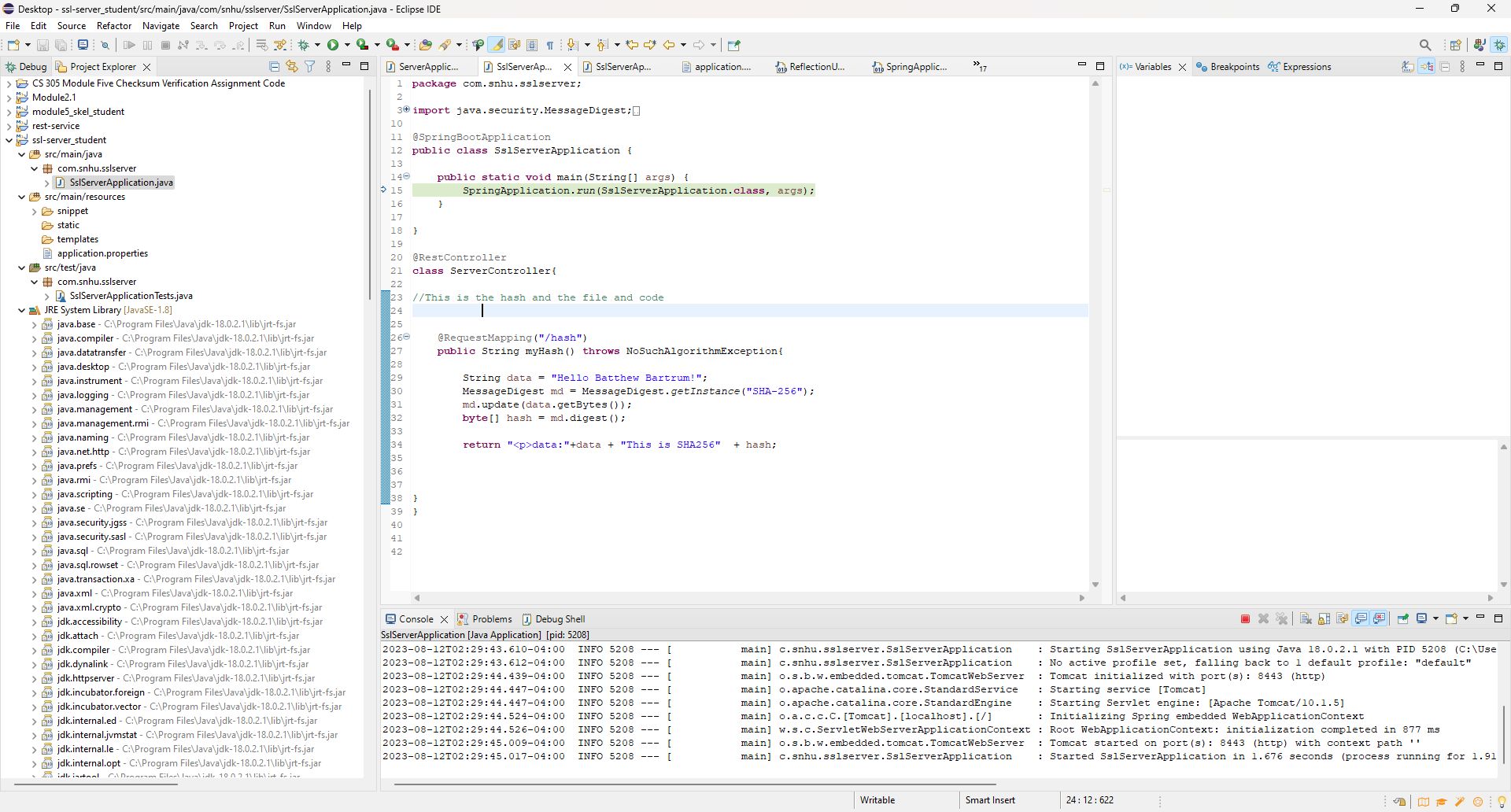
Insert a screenshot below of the web browser that shows a secure webpage.



## Secondary Testing

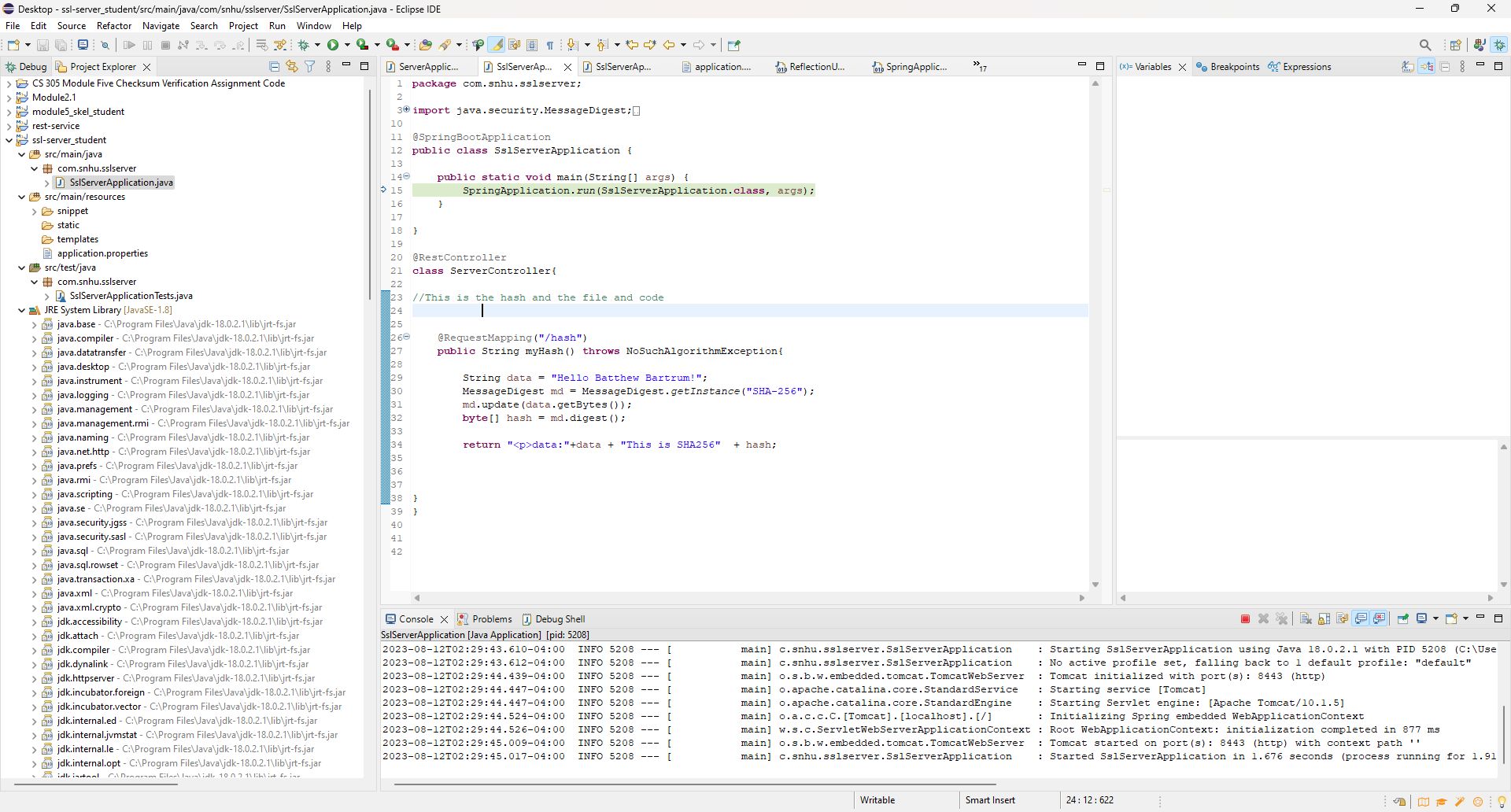
Insert screenshots below of the refactored code executed without errors and the dependency-check report.





## Functional Testing

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



## Summary

In summary, what the system did not have beforehand was a proper security setup dealing with clients signing on. What we did in the first part of the project was develop a plan. We figured out what the mitigation plan should be and how we should handle their program and make it better for them. What we just finished doing was implementing a capability which was adding a single sign on, AES, and SHA256. This is from my research that we felt would be the best thing to fix this problem. Now as we look at the report, we notice that we still need to have additional security in other areas. We would investigate third party CA that could give better security. I would not recommend using something like Java CA and would look for a better one that is easier to use and better to manage. This would cost more, but it will give the company a better structure. We also need to investigate areas that are not being used and to suppress those areas so those errors will not show again.

## Industry Standard Best Practices

What I have done to keep the best practice is always looking at what is the best solution for the current situation. A lot of times we want to choose what is the newest, intstead of what is best. To not let this, happen, we need to do our best due diligence. While doing the research for best practice is learning about single sign on, AES, and SHA. Another best practice is to keep your mind fresh and study what the current market is like and what people are trying out. The best way to help keep the company software safe is good documentation, good comments, and studying the static test report. That report allows us to understand what actual issues are and not.

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?Offer=abt_pubpro_AI-Insider>