****

# 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** | **[October 16]** | **[Steven Cognata]** |  |

## 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

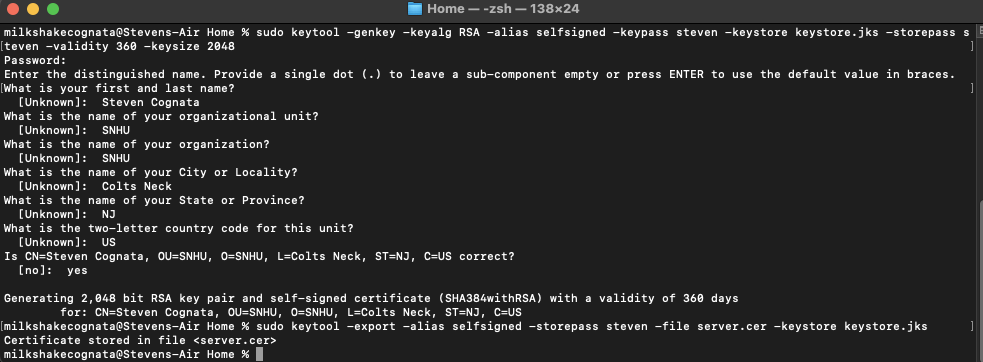
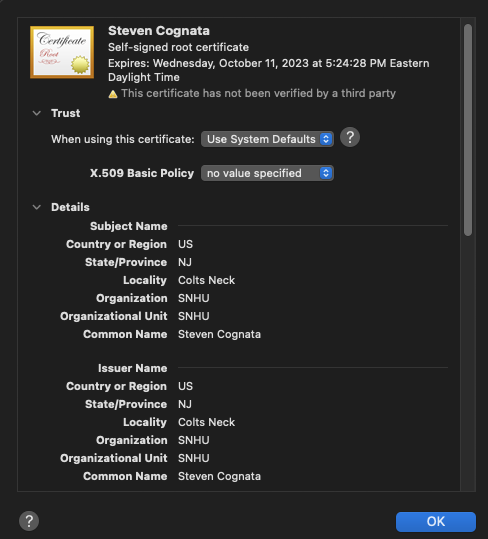
[Steven Cognata]

## Algorithm Cipher

The goal of Artemis Financial is to give plans for clients worldwide. With this goal I would recommend using SHA-256 as the type of encryption method. This cipher protects all data and ensures any third party from intercepting it. It is seen as the standard and it is used by the United States Government, Amazon, and more major companies. It is impossible to crack the key with the current technology we possess right now. It would take years and tons of technology mixed with brute force to even have a small possibility of cracking a SHA-256. This cipher is typically encouraged for most companies with sensitive data so when dealing with finances this is definitely the standard. When dealing with different types of encryption asymmetric keys are seen as the most secure due to the fact that there is 2. (Simplilearn, 2021)

## Certificate Generation

Insert a screenshot below of the CER file.



## Deploy Cipher

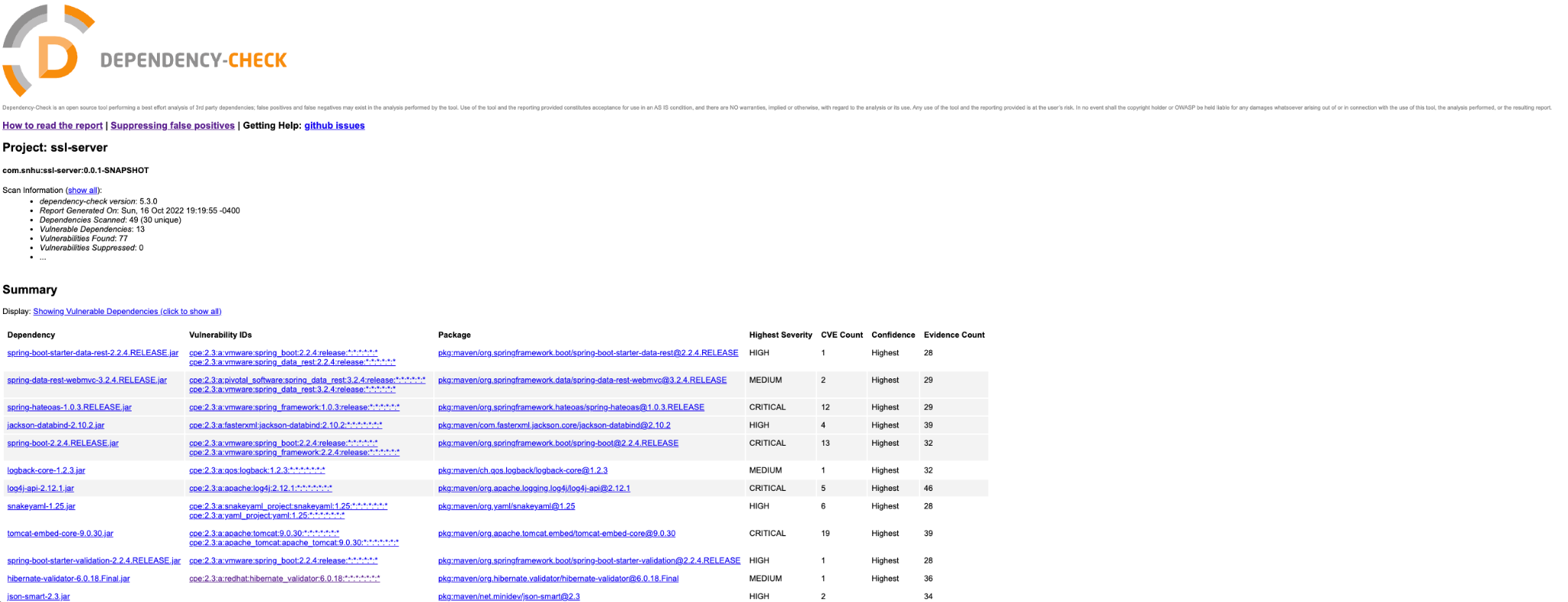
Insert a screenshot below of the checksum verification.

## 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

After reviewing and analyzing the Vulnerability Assessment Process Flow Diagram I came to the conclusion that in order to make this program run properly I needed to implement SHA-256 algorithm because I determined it was the most secure algorithm for what we were using it for. I also added a @RestController and a @RequestMapping controller. As I stated earlier, due to the fact that we are dealing with people's finances we need to make sure we use the most secure cipher out there.

## Industry Standard Best Practices

The industry has many standards and best practices that should be followed in order to keep everything maintained. In reality checking up on the software with dependency checks and things of that nature should happen daily. Bug fix updates should happen often when needed. Lastly, we want to be able to have a future where a company that does not keep up with its competitors will be lost along the way. In order to combat this we must be able to scale the software and have innovation play a part along the way. (Bose, 2021)

References

Bose, S. (2021, February 2). *Coding standards and best practices to follow*. BrowserStack. <https://www.browserstack.com/guide/coding-standards-best-practices>

Simplilearn. (2021, July 13). *What is SHA-256 algorithm: How it works and applications [2022 edition] | Simplilearn*. Simplilearn.com. <https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm>

*What is the strongest hash algorithm?* (n.d.). SG & Singapore Map! Powered by Streetdirectory.com. <https://www.streetdirectory.com/etoday/-ejcluw.html>