****

# Practices for Secure Software Report

Table of Contents

[Practices for Secure Software Report 1](#_Toc127715291)

[Document Revision History 3](#_Toc127715292)

[Client 3](#_Toc127715293)

[Instructions 3](#_Toc127715294)

[Developer 4](#_Toc127715295)

[1. Algorithm Cipher 4](#_Toc127715296)

[2. Certificate Generation 4](#_Toc127715297)

[3. Deploy Cipher 5](#_Toc127715298)

[4. Secure Communications 5](#_Toc127715299)

[5. Secondary Testing 8](#_Toc127715300)

[6. Functional Testing 10](#_Toc127715301)

[7. Summary 13](#_Toc127715302)

[8. Industry Standard Best Practices 13](#_Toc127715303)

## Document Revision History

| **Version** | **Date** | **Author** | **Comments** |
| --- | --- | --- | --- |
| **1.0** | **02/17/2023** | **Sarah Schmidt** | **Research and incorporate the best algorithm cipher** |
| **1.0** | **02/18/2023** | **Sarah Schmidt** | **Create certificate, and run checksum** |
| **1.0** | **02/19/2023** | **Sarah Schmidt** | **Run dependency report write summary and complete assignment** |

## 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

Sarah Schmidt

## Algorithm Cipher

Artemis Financial is a company that works around the world with business partners, the US government, and individuals. Java Security Standard Algorithm gives a great list of names of practices to keep and which Algorithm Cipher to use. My recommendation is that we use SHA 256. This algorithm has been around for a long time and there’s a reason why. SHA-256 allows information to be protected from potential hackers. SHA-256 is the most recommended cipher to use for financial companies. The hash algorithm function of SHA-256 is that it uses Cryptographic hash algorithms. This uses hashes to be unique and irreversible. So, to think, if we have a large number of hashes, the program creates a smaller chance of getting hacked into. (Google Help) The encryption of the SHA-256 is by the number of combinations within the encryption. Using random numbers makes it harder to find out how to get into the encryption. Symmetric keys will use a single key that needs to be shared with people who need the message. While asymmetric encryption will have a public key and a private key to encrypt and decrypt the message. (global ssl) Encryptions go back 100 years without the knowledge of computers, it wasn’t until the early 2000s that the Advanced Encryption Standard was made. This is the most standardized encryption people use because it is known to be the best based on the symmetric encryption it uses. (Sidhpurwala) I also find it interesting that most computers have their own encryption now. Obviously, some people still use some sort of third-party protection, but Apple has its own protection on its devices.

## Certificate Generation

Insert a screenshot below of the CER file.

Text

Description automatically generated

## Deploy Cipher

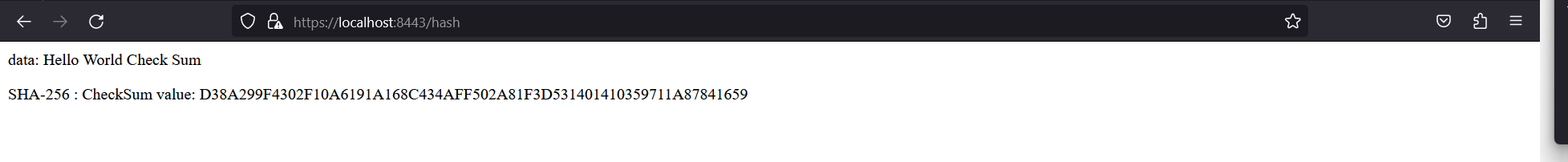
Insert a screenshot below of the checksum verification.

Graphical user interface, text, application

Description automatically generated

## Secure Communications

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



I did just about everything to try to get HTTPS. The issue I believe lies in the permissions and having to pay for a CA. I changed my settings on google chrome. I have added the certificate manually. I exported the certificate from the local host to import it into the certificate areas. I tried Firefox, and windows explorer as well. Nothing works. My code as you will see in step 4, will show that there are no errors.

**Graphical user interface, text, application, email

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

**A screenshot of a computer

Description automatically generated with medium confidence**

## Secondary Testing

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

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

[Dependency Check](file:///C:\Users\sarah\eclipse-workspace\CS%20305%20Project%20Two%20Code%20Base.zip_expanded\ssl-server_student\target\dependency-check-report.html)

Graphical user interface, text, application, email

Description automatically generated

## Functional Testing

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

Text

Description automatically generated

Chart, scatter chart

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated

## Summary

The summary of Project 2 is that we were able to create a self-certificate, add it into the project along with creating a .p12. I used the SHA-256 encryption because it is known to be a financially acceptable AES. I was able to address the areas of security by working on code quality, APIs. I was able to have a checksum report that was executed without any coding errors. In the future there will be additional items that Artemis Financial may need. This would include log-in verification, double authentication and much more. The need for software security is at its highest with how technology is so important today. It is important to maintain software security withing a business’s web application because if there were any attacks, it makes the company liable and could ruin their reputation and yours. A major issue that I ran into while working through this report is that we will need to update a lot of items with today’s standards. Meaning there will be a lot of maintenance on the web application.

## Industry Standard Best Practices

By using best practices, a software developer can help limit the number of cyber-attacks, data breaches, and any other security threat that may arise. If you are applying best coding practices then you can have a better understanding of data privacy and security regulations, helping reduce the risk of negative impacts on web applications like breached data and financial risk.

By using the best coding practices, you will ensure that guidelines, techniques, and procedures are in your software application that will keep the web application secure from any cyber-attacks. Applying industry standard best practices for secure coding is important because it will maintain software security and also help protect the company that you are working for.

Resources

Awati, R., & Loshin, P. (2021, September 1). *What is a Certificate Authority (CA)?* Security. Retrieved February 17, 2023, from <https://www.techtarget.com/searchsecurity/definition/certificate-authority#:~:text=They%20help%20secure%20the%20internet,be%20trusted%20with%20their%20data>.

Help, G. (2023). *SHA-256 algorithm: Definition*. Google Ads Help. Retrieved February 17, 2023, from <https://support.google.com/google-ads/answer/9004655?hl=en#:~:text=SHA%2D256%20stands%20for%20Secure,will%20create%20the%20same%20hash>.

Oracle, D. (2017). *Java Security Standard Algorithm Names*. Docs Oracle. Retrieved February 17, 2023, from <https://docs.oracle.com/javase/9/docs/specs/security/standard-names.html#cipher-algorithm-names>

Sidhpurwala, H. (2023, January 12). *A brief history of cryptography*. Red Hat - We make open source technologies for the enterprise. Retrieved February 17, 2023, from <https://www.redhat.com/en/blog/brief-history-cryptography>

ssl, global. (2021, June 14). *Symmetric vs. asymmetric encryption - what are differences?* SSL2BUY Wiki - Get Solution for SSL Certificate Queries. Retrieved February 17, 2023, from <https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences#:~:text=Symmetric%20encryption%20uses%20a%20single,and%20decrypt%20messages%20when%20communicating>.