****

# 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** | **4/21/2024** | **Jannatul Ferdush** |  |

## 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

Jannatul Ferdush

## Algorithm Cipher

Artemis Financial needs a super strong way to keep its clients' financial info safe. So, we're picking SHA-256, a really tough encryption method.

SHA-256 takes any input and spits out a fixed-size jumble of letters and numbers. It's like a secret code that's really hard to crack. This code is so tough because it's based on randomness and uses a lot of bits (like tiny pieces of info). With SHA-256, there are so many possible combinations that it's nearly impossible for anyone to guess the right one.

We're also using symmetric keys, like in AES-256, which are basically keys that unlock the code. They're simple and fast because they only need one key to lock and unlock stuff. Even though asymmetric keys are fancier and use two keys, we're sticking with symmetric keys for their speed and ease.

Encryption has been around for ages, evolving over time to keep up with sneaky hackers. Nowadays, it's crucial for keeping our data safe in our digital world.

So, by using SHA-256 and symmetric keys, Artemis Financial can keep its clients' financial data super secure and protect it from prying eyes.

## Certificate Generation

## Generate appropriate self-signed certificates using the Java Keytool, which is used through the command line.

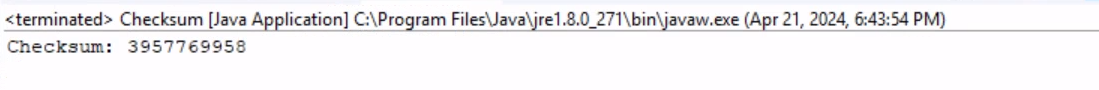
Insert a screenshot below of the CER file.

A computer screen with white text

Description automatically generated

## Deploy Cipher

Insert a screenshot below of the checksum verification.



## Secure Communications

Run the refactored code to verify secure communication by typing https://localhost:8443/hash in a new browser window to demonstrate that the secure communication works successfully.

## Secondary Testing

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

A screenshot of a computer program

Description automatically generated

## Functional Testing

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

A screenshot of a computer code

Description automatically generated

## Summary

We made the app more secure by switching from HTTP to HTTPS. Also, we added some extra security measures in the application.properties file. This makes it harder for hackers to get sensitive information. But remember, even with these changes, the app might still have vulnerabilities. It's important to stay updated on security and keep improving the app's defenses. As technology gets better, hackers might find new ways to attack. So, we need to stay vigilant.

## Industry Standard Best Practices

Industry standard best practices refer to the commonly accepted guidelines, procedures, and techniques that are recognized as effective and efficient in a particular industry. These practices are established based on industry experience, research, regulations, and evolving technologies. Here are some examples of industry standard best practices across various sectors:

1. **Information Security:** Keep important data safe by using strong passwords and encryption.
2. **Software Development:** Write and test code carefully to make sure it works well and doesn't have any mistakes.
3. **Project Management:** Plan projects carefully, make sure everyone knows what they need to do, and check progress regularly.
4. **Quality Assurance:** Test products thoroughly to make sure they work correctly and meet standards.
5. **Data Management:** Keep data safe, accurate, and organized.
6. **Compliance:** Follow the rules and laws that apply to your industry.
7. **Risk Management:** Identify and reduce potential problems before they happen.
8. **Business Continuity:** Have plans in place to keep the business running if something unexpected happens.
9. **Customer Service:** Treat customers well and fix any problems quickly.
10. **Ethical Standards:** Be honest, fair, and respectful in all business activities.