****

# 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** | **12/09/2023** | **Mary Sanders** |  |

## Client



## Developer

Mary Sanders

## Algorithm Cipher

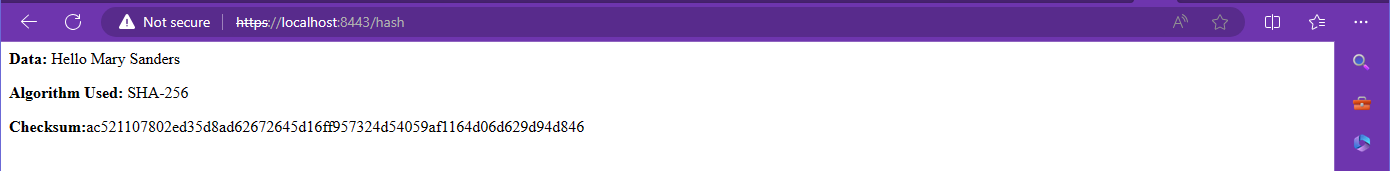
I chose SHA-256, a cryptographic hash function developed by the NSA in 2001. It transforms input messages into fixed-size 256-bit hash values, ensuring irreversibility. This one-way function is widely used for data integrity verification, digital signatures, and password hashing, contributing to digital systems and communications security. SHA-256 is a reliable and widely adopted cryptographic tool, especially suited for financial organizations like Artemis Financial.

Symmetric key algorithms use the same key for encryption and decryption, offering computational efficiency but requiring secure key distribution. On the other hand, asymmetric key algorithms employ a pair of keys—one public and one private—allowing secure communication over open networks but at the cost of increased runtime. The choice between symmetric and asymmetric keys depends on factors like efficiency, key management, and the nature of the communication environment.

Cryptography has a long history that goes back centuries. One example is the treatise Arthashasta written in the 3rd century BCE by Kautilya, an Indian strategist and philosopher. In this manuscript, there is mention of secret messages sent by spies (Sidhpurwala, 2023). Today, encryption is done by computers to protect sensitive data.

## Certificate GenerationA screenshot of a computer screen Description automatically generated

## Deploy Cipher



## 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.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated <?xml version="1.0" encoding="UTF-8"?>

<suppressions xmlns="https://jeremylong.github.io/DependencyCheck/dependency-suppression.1.3.xsd">

<suppress>

<notes><CDATA[

file name: spring-boot-starter-data-rest-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot\-starter\-data\-rest@.\*$</packageUrl>

<cpe>cpe:/a:vmware:spring\_boot</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-boot-starter-data-rest-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot\-starter\-data\-rest@.\*$</packageUrl>

<cpe>cpe:/a:vmware:spring\_data\_rest</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-boot-starter-data-rest-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot\-starter\-data\-rest@.\*$</packageUrl>

<cve>CVE-2022-27772</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-boot-starter-data-rest-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot\-starter\-data\-rest@.\*$</packageUrl>

<cve>CVE-2023-20873</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-boot-starter-data-rest-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot\-starter\-data\-rest@.\*$</packageUrl>

<cve>CVE-2023-20883</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-data-rest-webmvc-3.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.data/spring\-data\-rest\-webmvc@.\*$</packageUrl>

<cpe>cpe:/a:pivotal\_software:spring\_data\_rest</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-data-rest-webmvc-3.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.data/spring\-data\-rest\-webmvc@.\*$</packageUrl>

<cpe>cpe:/a:vmware:spring\_data\_rest</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-data-rest-webmvc-3.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.data/spring\-data\-rest\-webmvc@.\*$</packageUrl>

<vulnerabilityName>CVE-2021-22047</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-data-rest-webmvc-3.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.data/spring\-data\-rest\-webmvc@.\*$</packageUrl>

<vulnerabilityName>CVE-2022-31679</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-hateoas-1.0.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.hateoas/spring\-hateoas@.\*$</packageUrl>

<cpe>cpe:/a:vmware:spring\_hateoas</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-hateoas-1.0.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.hateoas/spring\-hateoas@.\*$</packageUrl>

<cve>CVE-2023-34036</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: jackson-databind-2.10.2.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.fasterxml\.jackson\.core/jackson\-databind@.\*$</packageUrl>

<cpe>cpe:/a:fasterxml:jackson-databind</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: jackson-databind-2.10.2.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.fasterxml\.jackson\.core/jackson\-databind@.\*$</packageUrl>

<cve>CVE-2020-25649</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: jackson-databind-2.10.2.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.fasterxml\.jackson\.core/jackson\-databind@.\*$</packageUrl>

<cve>CVE-2020-25649</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: jackson-databind-2.10.2.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.fasterxml\.jackson\.core/jackson\-databind@.\*$</packageUrl>

<cve>CVE-2020-36518</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: jackson-databind-2.10.2.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.fasterxml\.jackson\.core/jackson\-databind@.\*$</packageUrl>

<cve>CVE-2021-46877</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: jackson-databind-2.10.2.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.fasterxml\.jackson\.core/jackson\-databind@.\*$</packageUrl>

<cve>CVE-2022-42003</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: jackson-databind-2.10.2.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.fasterxml\.jackson\.core/jackson\-databind@.\*$</packageUrl>

<cve>CVE-2022-42004</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: jackson-databind-2.10.2.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.fasterxml\.jackson\.core/jackson\-databind@.\*$</packageUrl>

<cve>CVE-2023-35116</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-boot-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot@.\*$</packageUrl>

<cpe>cpe:/a:vmware:spring\_boot</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-boot-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot@.\*$</packageUrl>

<cve>CVE-2022-27772</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-boot-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot@.\*$</packageUrl>

<cve>CVE-2023-20873</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-boot-2.2.4.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework\.boot/spring\-boot@.\*$</packageUrl>

<cve>CVE-2023-20883</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: logback-core-1.2.3.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/ch\.qos\.logback/logback\-core@.\*$</packageUrl>

<cpe>cpe:/a:qos:logback</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: logback-core-1.2.3.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/ch\.qos\.logback/logback\-core@.\*$</packageUrl>

<cve>CVE-2021-42550</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: logback-core-1.2.3.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/ch\.qos\.logback/logback\-core@.\*$</packageUrl>

<cve>CVE-2023-6378</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: log4j-api-2.12.1.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.logging\.log4j/log4j\-api@.\*$</packageUrl>

<cpe>cpe:/a:apache:log4j</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: log4j-api-2.12.1.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.logging\.log4j/log4j\-api@.\*$</packageUrl>

<cve>CVE-2020-9488</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: log4j-api-2.12.1.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.logging\.log4j/log4j\-api@.\*$</packageUrl>

<cve>CVE-2021-44228</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: log4j-api-2.12.1.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.logging\.log4j/log4j\-api@.\*$</packageUrl>

<cve>CVE-2021-44832</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: log4j-api-2.12.1.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.logging\.log4j/log4j\-api@.\*$</packageUrl>

<cve>CVE-2021-45046</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: log4j-api-2.12.1.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.logging\.log4j/log4j\-api@.\*$</packageUrl>

<cve>CVE-2021-45105</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cpe>cpe:/a:snakeyaml\_project:snakeyaml</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cpe>cpe:/a:yaml\_project:yaml</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2017-18640</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2021-4235</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2022-1471</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2022-25857</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2022-3064</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2022-38749</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2022-38750</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2022-38751</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2022-38752</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: snakeyaml-1.25.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.yaml/snakeyaml@.\*$</packageUrl>

<cve>CVE-2022-41854</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cpe>cpe:/a:apache:tomcat</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cpe>cpe:/a:apache\_tomcat:apache\_tomcat</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2019-17569</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-11996</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-13934</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-13935</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-13943</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-17527</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-1935</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-1938</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-8022</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2020-9484</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2021-24122</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2021-25122</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2021-25329</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2021-30640</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2021-33037</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2021-41079</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2021-43980</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2022-29885</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2022-34305</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2022-42252</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2023-28708</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2023-41080</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2023-42795</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2023-44487</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2023-45648</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: tomcat-embed-core-9.0.30.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.apache\.tomcat\.embed/tomcat\-embed\-core@.\*$</packageUrl>

<cve>CVE-2023-46589</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: hibernate-validator-6.0.18.Final.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.hibernate\.validator/hibernate\-validator@.\*$</packageUrl>

<cpe>cpe:/a:redhat:hibernate\_validator</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: hibernate-validator-6.0.18.Final.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.hibernate\.validator/hibernate\-validator@.\*$</packageUrl>

<cve>CVE-2020-10693</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-web-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-web@.\*$</packageUrl>

<cpe>cpe:/a:pivotal\_software:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-web-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-web@.\*$</packageUrl>

<cpe>cpe:/a:springsource:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-web-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-web@.\*$</packageUrl>

<vulnerabilityName>CVE-2016-1000027</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-web-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-web@.\*$</packageUrl>

<vulnerabilityName>CVE-2020-5421</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-web-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-web@.\*$</packageUrl>

<vulnerabilityName>CVE-2021-22096</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-web-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-web@.\*$</packageUrl>

<vulnerabilityName>CVE-2021-22118</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-beans-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-beans@.\*$</packageUrl>

<cpe>cpe:/a:pivotal\_software:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-beans-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-beans@.\*$</packageUrl>

<cpe>cpe:/a:springsource:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-beans-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-beans@.\*$</packageUrl>

<vulnerabilityName>CVE-2022-22965</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-webmvc-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-webmvc@.\*$</packageUrl>

<cpe>cpe:/a:pivotal\_software:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-webmvc-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-webmvc@.\*$</packageUrl>

<cpe>cpe:/a:springsource:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-webmvc-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-webmvc@.\*$</packageUrl>

<vulnerabilityName>CVE-2021-22060</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-context-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-context@.\*$</packageUrl>

<cpe>cpe:/a:pivotal\_software:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-context-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-context@.\*$</packageUrl>

<cpe>cpe:/a:springsource:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-context-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-context@.\*$</packageUrl>

<vulnerabilityName>CVE-2022-22968</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-expression-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-expression@.\*$</packageUrl>

<cpe>cpe:/a:pivotal\_software:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-expression-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-expression@.\*$</packageUrl>

<cpe>cpe:/a:springsource:spring\_framework</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-expression-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-expression@.\*$</packageUrl>

<vulnerabilityName>CVE-2022-22950</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-expression-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-expression@.\*$</packageUrl>

<vulnerabilityName>CVE-2023-20861</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: spring-expression-5.2.3.RELEASE.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/org\.springframework/spring\-expression@.\*$</packageUrl>

<vulnerabilityName>CVE-2023-20863</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: json-path-2.4.0.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.jayway\.jsonpath/json\-path@.\*$</packageUrl>

<cpe>cpe:/a:json-java\_project:json-java</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: json-path-2.4.0.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.jayway\.jsonpath/json\-path@.\*$</packageUrl>

<cve>CVE-2022-45688</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: json-path-2.4.0.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/com\.jayway\.jsonpath/json\-path@.\*$</packageUrl>

<cve>CVE-2023-5072</cve>

</suppress>

<suppress>

<notes><![CDATA[

file name: json-smart-2.3.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/net\.minidev/json\-smart@.\*$</packageUrl>

<cpe>cpe:/a:json-smart\_project:json-smart</cpe>

</suppress>

<suppress>

<notes><![CDATA[

file name: json-smart-2.3.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/net\.minidev/json\-smart@.\*$</packageUrl>

<vulnerabilityName>CVE-2021-27568</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: json-smart-2.3.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/net\.minidev/json\-smart@.\*$</packageUrl>

<vulnerabilityName>CVE-2021-31684</vulnerabilityName>

</suppress>

<suppress>

<notes><![CDATA[

file name: json-smart-2.3.jar

]]></notes>

<packageUrl regex="true">^pkg:maven/net\.minidev/json\-smart@.\*$</packageUrl>

<vulnerabilityName>CVE-2023-1370</vulnerabilityName>

</suppress>

</suppressions>

![A screenshot of a computer error

Description automatically generated

A screenshot of a computer

Description automatically generated

## Functional Testing

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

A screenshot of a computer

Description automatically generated

## Summary

The process involved systematically strengthening the software application's security through multiple layers. This included implementing robust encryption (SHA-256) for sensitive data, adopting best practices for secure communication via RESTful APIs, introducing HTTPS with SSL/TLS certificates, conducting thorough dependency scans to address vulnerabilities, validating certificates from trusted CAs, and organizing code through refactoring for improved security. Each layer contributes to a fortified defense against potential threats, ensuring data integrity, confidentiality, and compliance with industry standards.

## Industry Standard Best Practices

The use of strong codes, specifically the SHA-256 encryption algorithm, was implemented to protect information considered sensitive. This algorithm is recognized for its effectiveness in securing data.

I used best practices for utilizing RESTful APIs to enhance the secure exchange of information between different parts of the application. This ensures that data shared between components follows standardized and secure protocols.

The application's security was further strengthened by implementing HTTPS, a protocol that encrypts data during transmission. This involved obtaining and deploying a valid SSL/TLS certificate, serving as a digital proof for the security of communication between users and the server.

Comprehensive dependency scans were conducted both before and after making changes to the code. These scans identify and address vulnerabilities in third-party components or libraries, crucial for maintaining a secure application environment.

Sidhpurwala, H. (2023, January 12). A brief history of cryptography. Red Hat. https://www.redhat.com/en/blog/brief-history-cryptography