Practices for Secure Software Report

Table of Contents

Document Revision History 3
Client 3
Instructions 3
Developer 4
1. Algorithm Cipher 4
2. Certificate Generation 4
3. Deploy Cipher 4
4. Secure Communications 4
5. Secondary Testing 4
6. Functional Testing 4
7. Summary 4
8. Industry Standard Best Practices 4

Document Revision History

Version	Date	Author	Comments
1.0	[Date]	[Kevin Alexander]	

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
[Kevin Alexander.]

1. Algorithm Cipher

To recommend an appropriate encryption algorithm cipher for Artemis Financial's software application, consider several factors such as security requirements,performance,and industry standards.

Research and Understand Encryption Algorithms:

-Encryption algorithms are mathematical procedures used to convert plaintext data into a secure form(ciphertext) to protect it during transmission or storage.

-Common encryption algorithms include Advanced Encryption Standard(AES),RSA,Triple Data Encryption Standard (3DES),and others.

Consider Security Requirements:

-For a financial institution like Artemis Financial dealing with sensitive client data and financial dealing with sensitive client data and financial information,a strong encryption algorithm is crucial.

-AES is widely considered secure and is recommended for its strength and speed,making it a popular choice for secure communications.

Justify the Recommendation:

-AES(Advanced Encryption Standard) is a symmetric encryption algorithm that uses keys of 128,192,or 256 bits.

-It provides a good balance between security,performance,and implementation complexity, making it suitable for Artemis Financial's needs.

Discuss Hash Functions and Bit Levels:

-AES does not directly involve hash functions,but it operates on a fixed block size of 128 bits.

-Hash functions like SHA-256 can be used in conjunction with AES for additional security in verifying data integrity.

Random Numbers and Key Types:

-AES uses symmetric keys,meaning the same key is used for both encryption and decryption.

-Random numbers play a crucial role in generating secure keys for encryption and decryption processes.

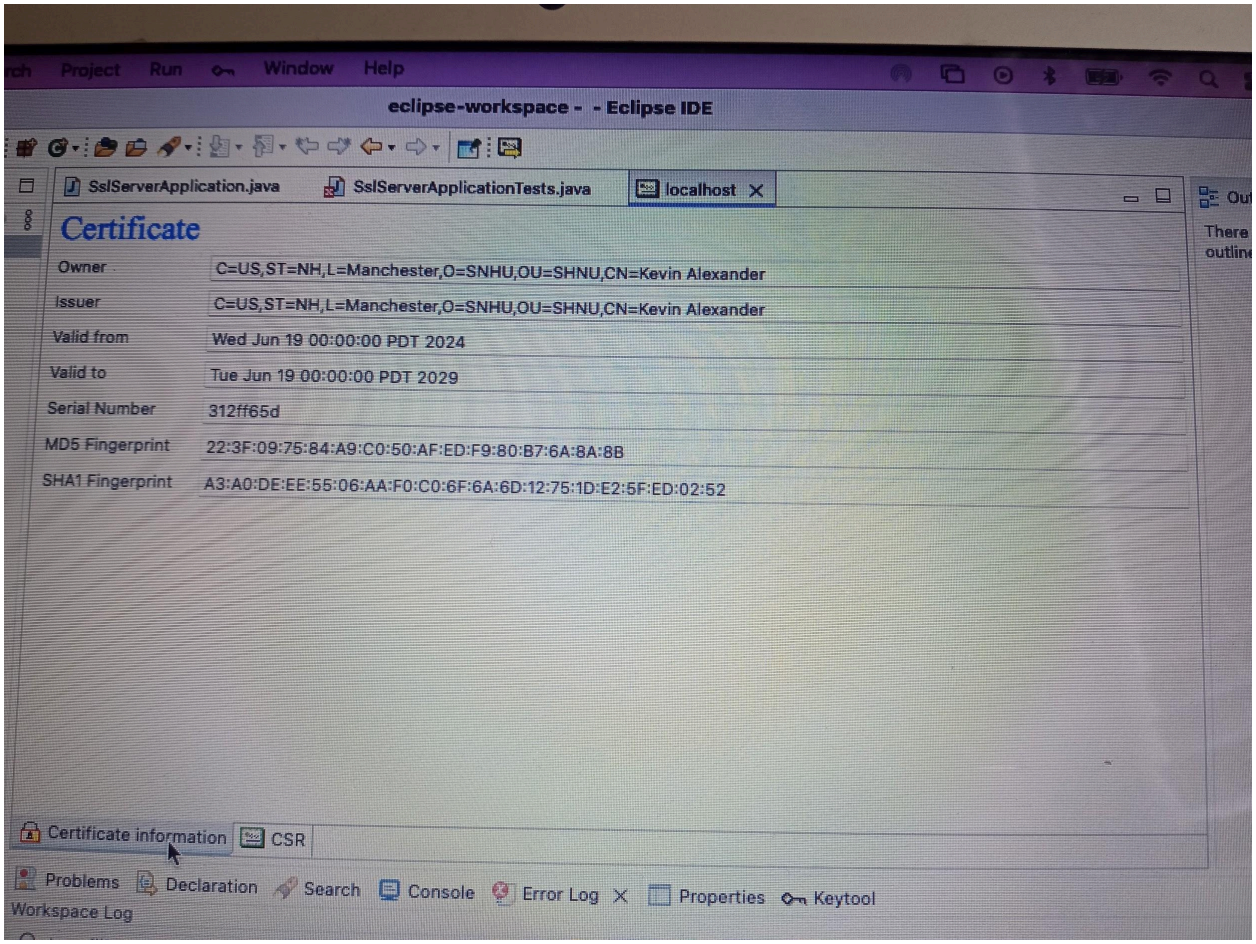
History and Current State of Encryption Algorithms:

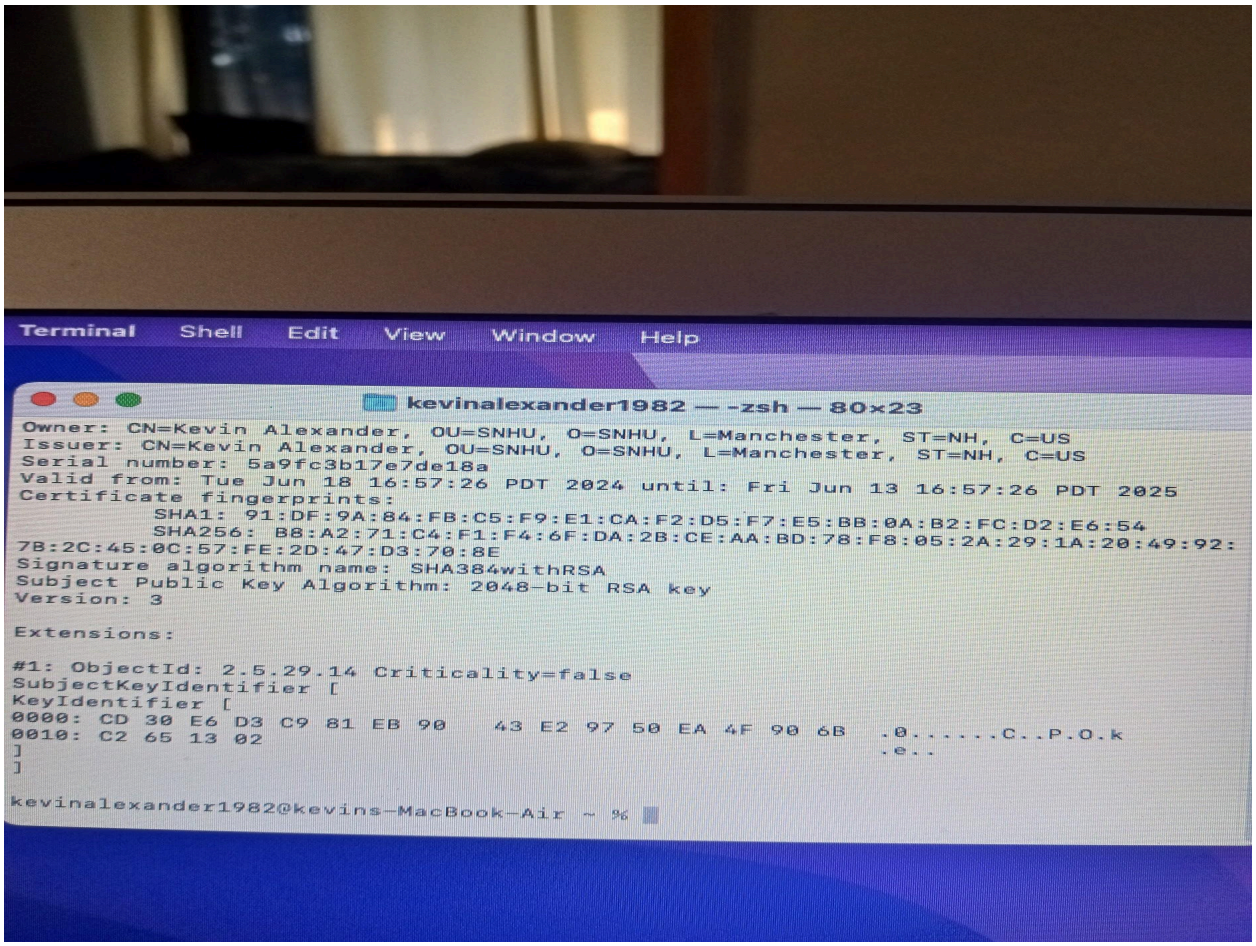
-AES was established as the standard encryption algorithm by the U.S. National Institute of Standards and Technology(NIST) in 2001.

-It has since become one of the most widely used encryption algorithms globally due to its security and efficiency.

Recommending AES as the encryption algorithm cipher for Artemis Financial's software application.you can ensure a high level of security for the company's client data and financial information during data transfers.

2. Certificate Generation

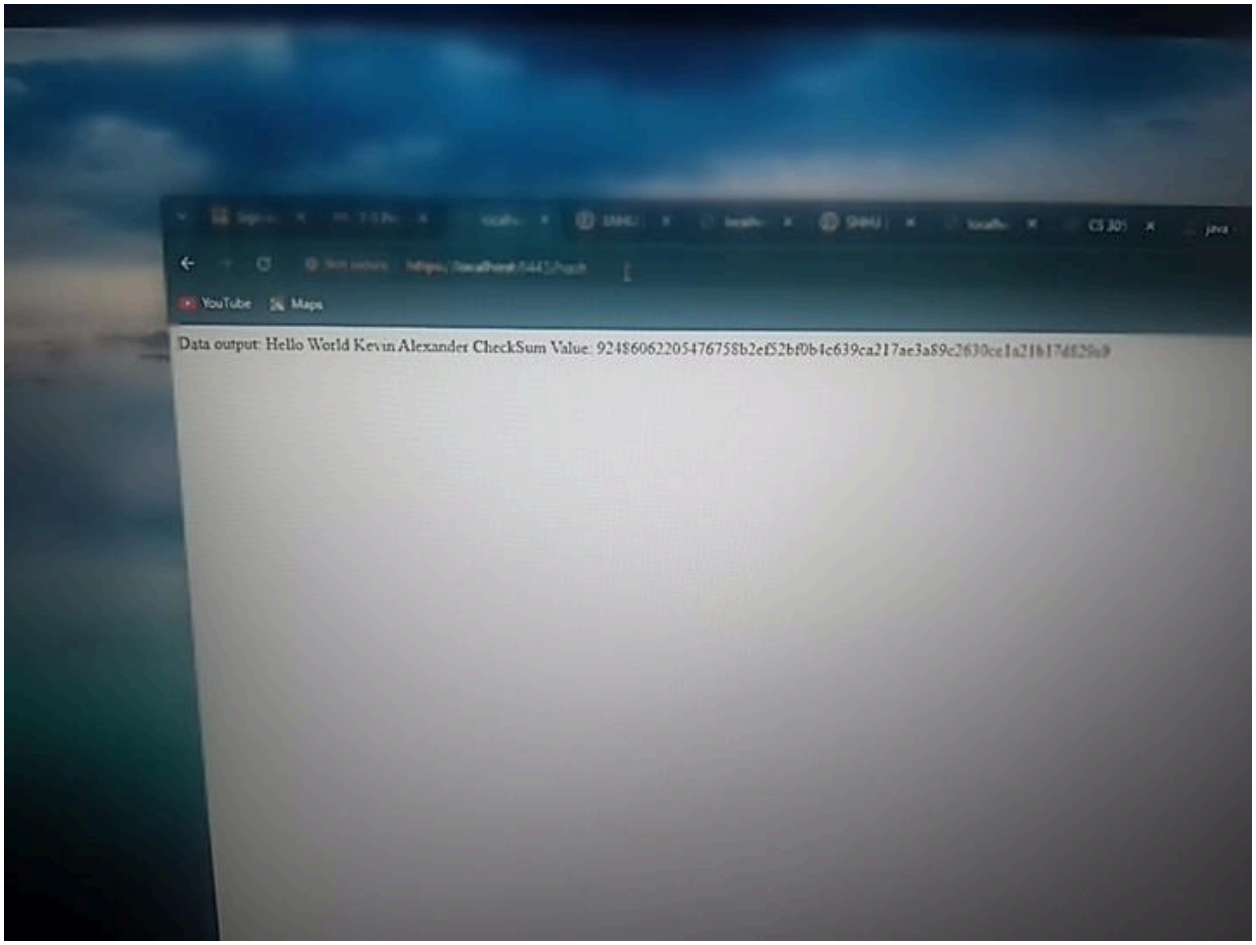

Project Run Window Help
eclipse-workspace - - Eclipse IDE
SslServerApplication.java
SslServerApplicationTests.java
localhost
Certificate
Owner
C=US,ST=NH,L=Manchester,O=SNHU,OU=SHNU,CN=Kevin Alexander
Issuer
C=US,ST=NH,L=Manchester,O=SNHU,OU=SHNU,CN=Kevin Alexander
Valid from
Wed Jun 19 00:00:00 PDT 2024
Valid to
Tue Jun 19 00:00:00 PDT 2029
Serial Number
312ff65d
MD5 Fingerprint
22:3F:09:75:84:A9:C0:50:AF:ED:F9:80:B7:6A:8A:8B
SHA1 Fingerprint
A3:A0:DE:EE:55:06:AA:F0:C0:6F:6A:6D:12:75:1D:E2:5F:ED:02:52
Certificate information
CSR
Problems
Declaration
Search
Console
Error Log
Properties
Keytool
Workspace Log

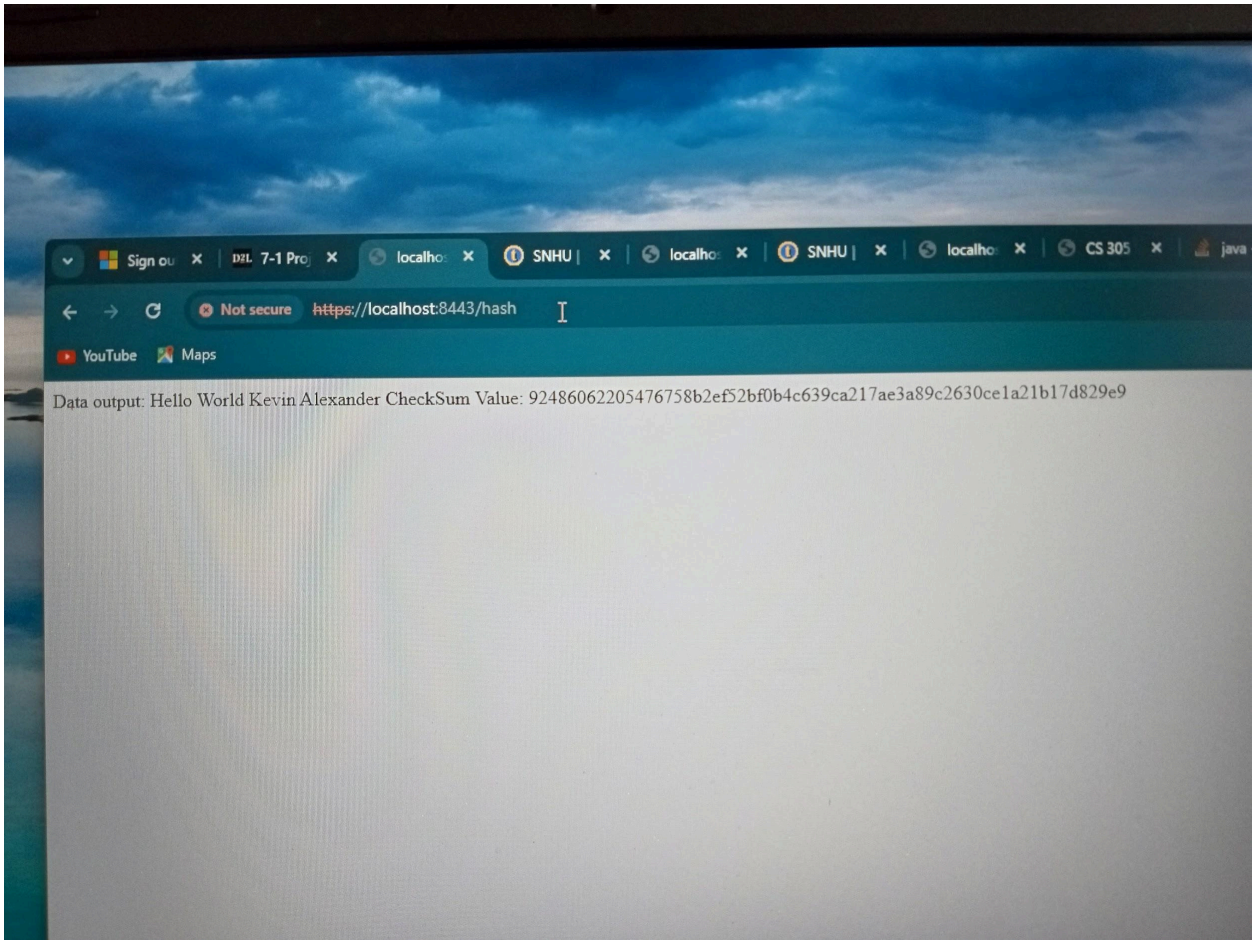


3. Deploy Cipher

Insert a screenshot below of the checksum verification.

[


YouTube
Maps
Data output: Hello World Kevin Alexander CheckSum Value: 9248606220547675 8b2ef52bf0b4c639ca217ae3a89c2630ce1a21b17d529a9



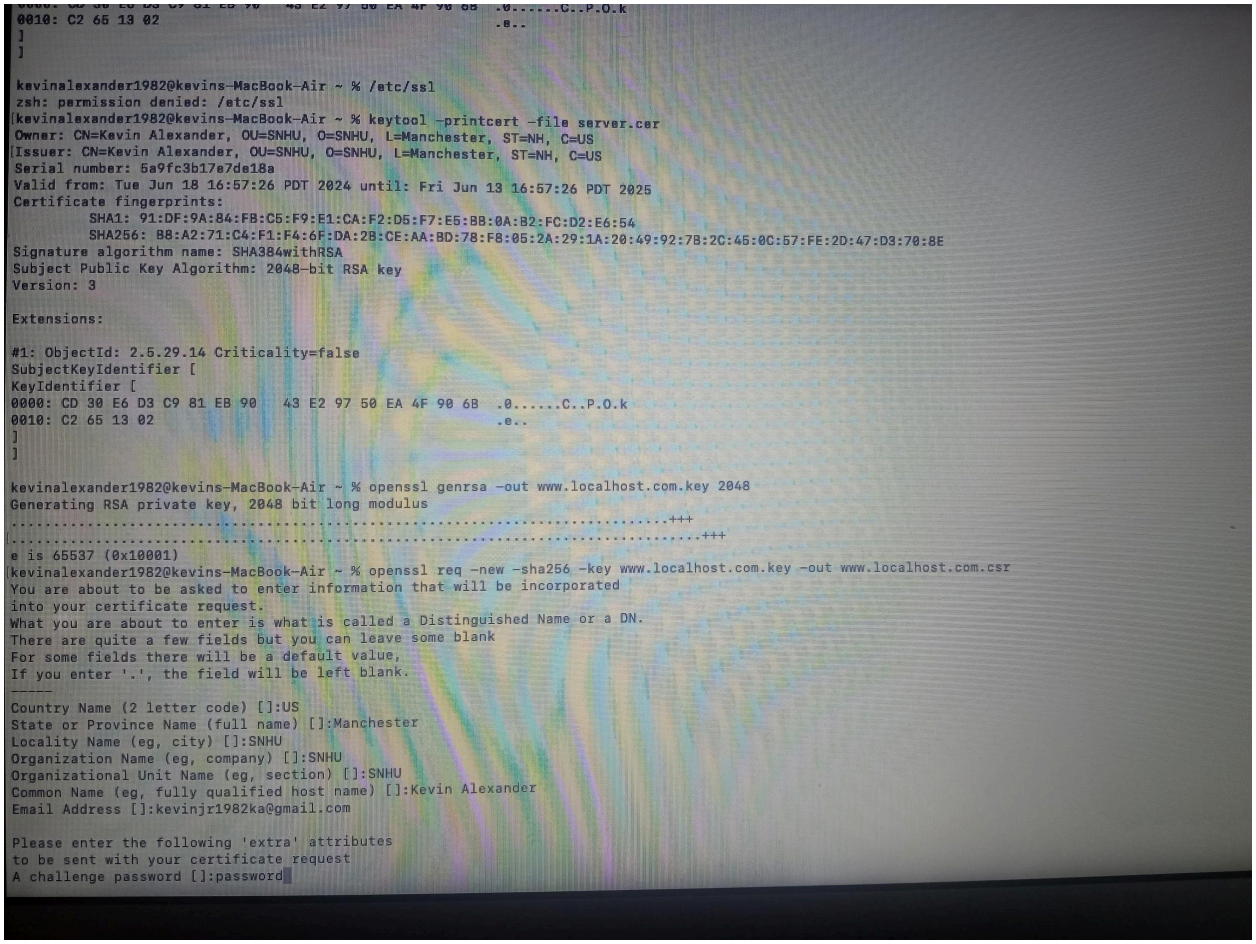
.]

4. Secure Communications

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

[

```
0000: CD 30 E6 D3 C9 81 EB 90   43 E2 97 50 EA 4F 90 68  .0......C..P.O.k
0010: C2 65 13 02                                        .e..
]
]

kevinalexander1982@kevins-MacBook-Air ~ % /etc/ssl
zsh: permission denied: /etc/ssl
kevinalexander1982@kevins-MacBook-Air ~ % keytool -printcert -file server.cer
Owner: CN=Kevin Alexander, OU=SNHU, O=SNHU, L=Manchester, ST=NH, C=US
Issuer: CN=Kevin Alexander, OU=SNHU, O=SNHU, L=Manchester, ST=NH, C=US
Serial number: 5a9fc3b17e7de18a
Valid from: Tue Jun 18 16:57:26 PDT 2024 until: Fri Jun 13 16:57:26 PDT 2025
Certificate fingerprints:
         SHA1: 91:DF:9A:84:F8:C5:F9:E1:CA:F2:D5:F7:E5:B8:0A:82:FC:D2:E6:54
         SHA256: 88:A2:71:C4:F1:F4:6F:DA:2B:CE:AA:BD:78:F8:05:2A:29:1A:20:49:92:78:2C:45:0C:57:FE:2D:47:D3:70:8E
Signature algorithm name: SHA384withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: CD 30 E6 D3 C9 81 EB 90   43 E2 97 50 EA 4F 90 68  .0......C..P.O.k
0010: C2 65 13 02                                        .e..
]
]

kevinalexander1982@kevins-MacBook-Air ~ % openssl genrsa -out www.localhost.com.key 2048
Generating RSA private key, 2048 bit long modulus
.......................................................................+++
.....................................................................+++
e is 65537 (0x10001)
kevinalexander1982@kevins-MacBook-Air ~ % openssl req -new -sha256 -key www.localhost.com.key -out www.localhost.com.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:Manchester
Locality Name (eg, city) []:SNHU
Organization Name (eg, company) []:SNHU
Organizational Unit Name (eg, section) []:SNHU
Common Name (eg, fully qualified host name) []:Kevin Alexander
Email Address []:kevinjr1982ka@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
```



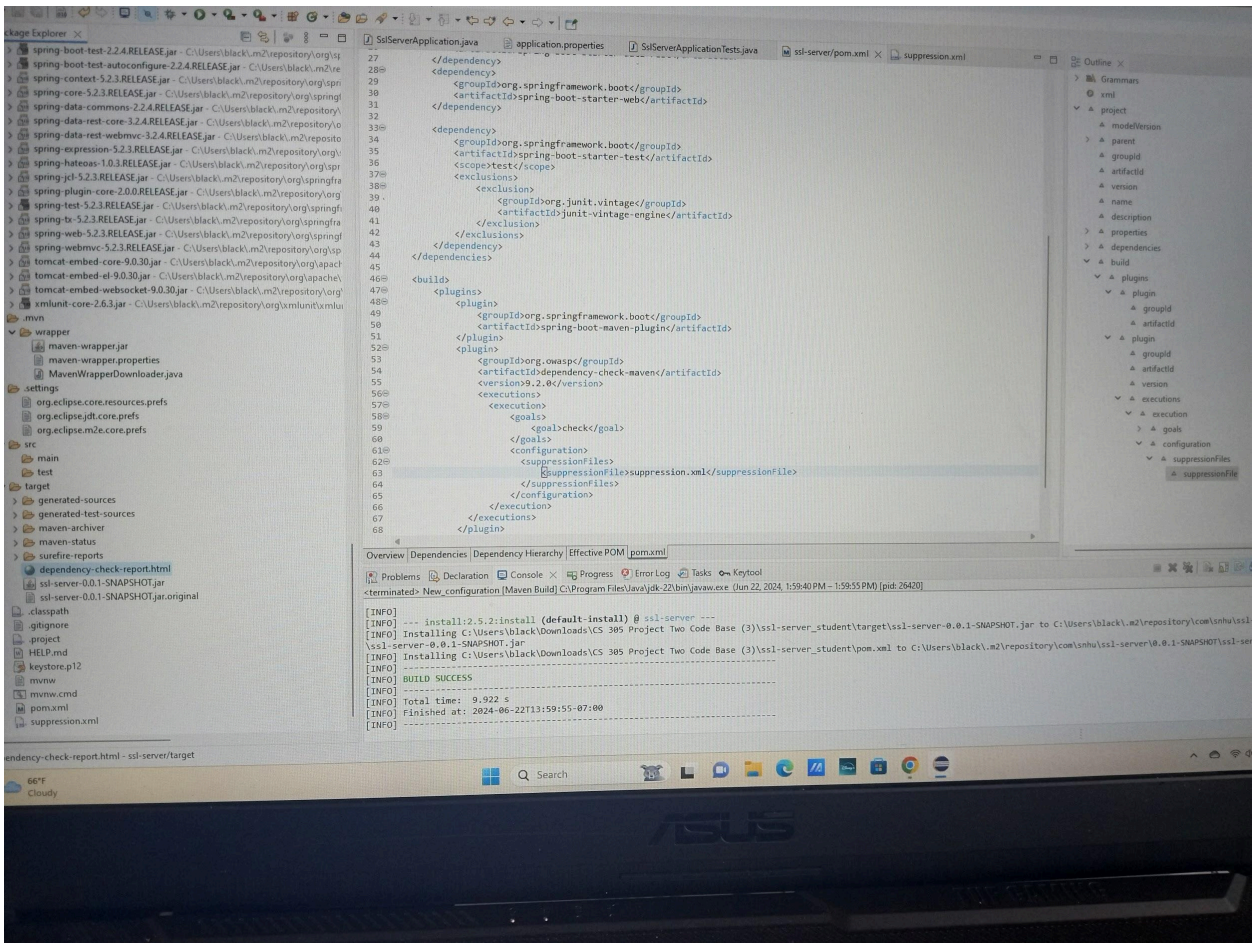
```
0010: C2 65 13 02                                        .e..
]
]

kevinalexander1982@kevins-MacBook-Air ~ % /etc/ssl
zsh: permission denied: /etc/ssl
kevinalexander1982@kevins-MacBook-Air ~ % keytool -printcert -file server.cer
Owner: CN=Kevin Alexander, OU=SNHU, O=SNHU, L=Manchester, ST=NH, C=US
Issuer: CN=Kevin Alexander, OU=SNHU, O=SNHU, L=Manchester, ST=NH, C=US
Serial number: 5a9fc3b17e7de18a
Valid from: Tue Jun 18 16:57:26 PDT 2024 until: Fri Jun 13 16:57:26 PDT 2025
Certificate fingerprints:
         SHA1: 91:DF:9A:84:FB:C5:F9:E1:CA:F2:D5:F7:E5:BB:0A:B2:FC:D2:E6:54
         SHA256: B8:A2:71:C4:F1:F4:6F:DA:2B:CE:AA:BD:78:F8:05:2A:29:1A:20:49:92:7B:2C:45:0C:57:FE:2D:47:D3:70:8E
Signature algorithm name: SHA384withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: CD 30 E6 D3 C9 81 EB 90   43 E2 97 50 EA 4F 90 6B  .0......C..P.O.k
0010: C2 65 13 02                                        .e..
]
]

kevinalexander1982@kevins-MacBook-Air ~ % openssl genrsa -out www.localhost.com.key 2048
Generating RSA private key, 2048 bit long modulus
.......................................................................+++
.......................................................................+++
e is 65537 (0x10001)
kevinalexander1982@kevins-MacBook-Air ~ % openssl req -new -sha256 -key www.localhost.com.key -out www.localhost.com.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:Manchester
Locality Name (eg, city) []:SNHU
Organization Name (eg, company) []:SNHU
Organizational Unit Name (eg, section) []:SNHU
Common Name (eg, fully qualified host name) []:Kevin Alexander
Email Address []:kevinjr1982ka@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password
```

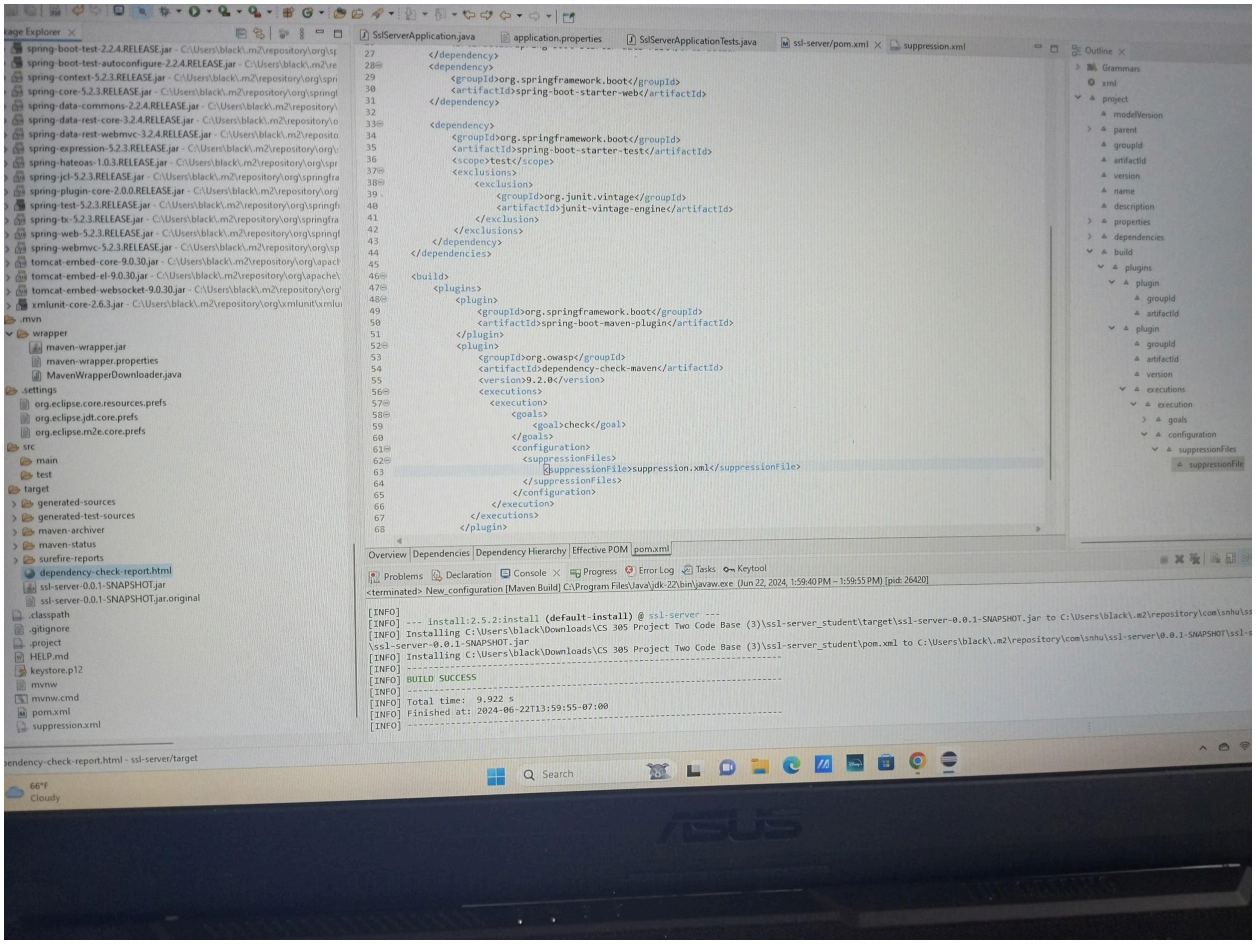
]

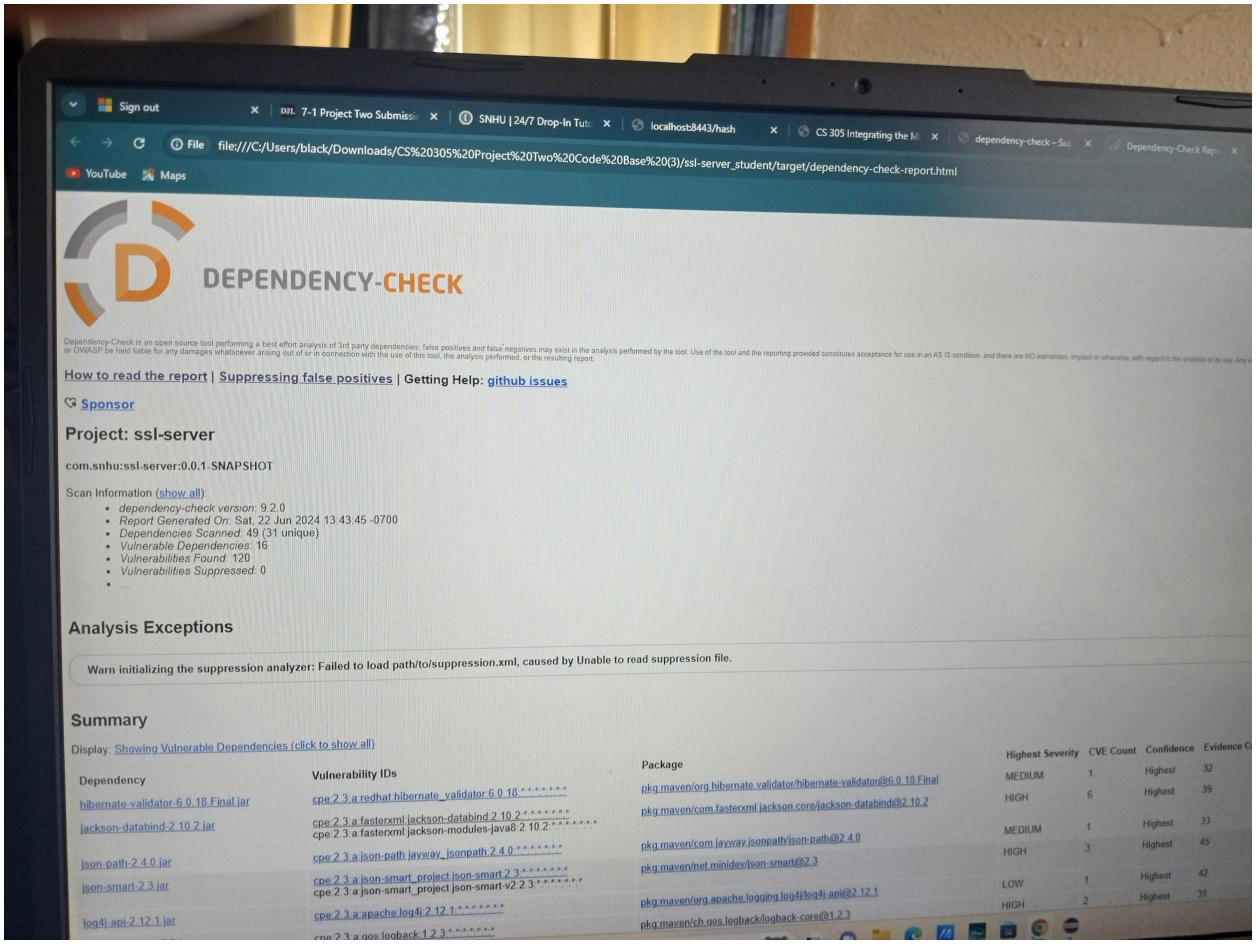
5. Secondary Testing

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

[


SslServerApplication.java
application.properties
SslServerApplicationTests.java
ssl-server/pom.xml
suppression.xml
Overview
Dependencies
Dependency Hierarchy
Effective POM
pom.xml
Problems
Declaration
Console
Progress
Error Log
Tasks
Keytool
[INFO] --- install:2.5.2:install (default-install) @ ssl-server ---
[INFO] Installing C:\Users\black\Downloads\CS 305 Project Two Code Base (3)\ssl-server_student\target\ssl-server-0.0.1-SNAPSHOT.jar to C:\Users\black\.m2\repository\com\snhu\ssl
\ssl-server-0.0.1-SNAPSHOT.jar
[INFO] Installing C:\Users\black\Downloads\CS 305 Project Two Code Base (3)\ssl-server_student\pom.xml to C:\Users\black\.m2\repository\com\snhu\ssl-server\0.0.1-SNAPSHOT\ssl-ser
[INFO] BUILD SUCCESS
[INFO] Total time: 9.922 s
[INFO] Finished at: 2024-06-22T13:59:55-07:00


SslServerApplication.java
application.properties
SslServerApplicationTests.java
ssl-server/pom.xml
suppression.xml
Overview
Dependencies
Dependency Hierarchy
Effective POM
pom.xml
Problems
Declaration
Console
Progress
Error Log
Tasks
Keytool
[INFO] --- install:2.5.2:install (default-install) @ ssl-server ---
[INFO] Installing C:\Users\black\Downloads\CS 305 Project Two Code Base (3)\ssl-server_student\target\ssl-server-0.0.1-SNAPSHOT.jar
[INFO] Installing C:\Users\black\Downloads\CS 305 Project Two Code Base (3)\ssl-server_student\pom.xml
[INFO] --
[INFO] BUILD SUCCESS
[INFO] --
[INFO] Total time: 9.922 s
[INFO] Finished at: 2024-06-22T13:59:55-07:00
[INFO] --

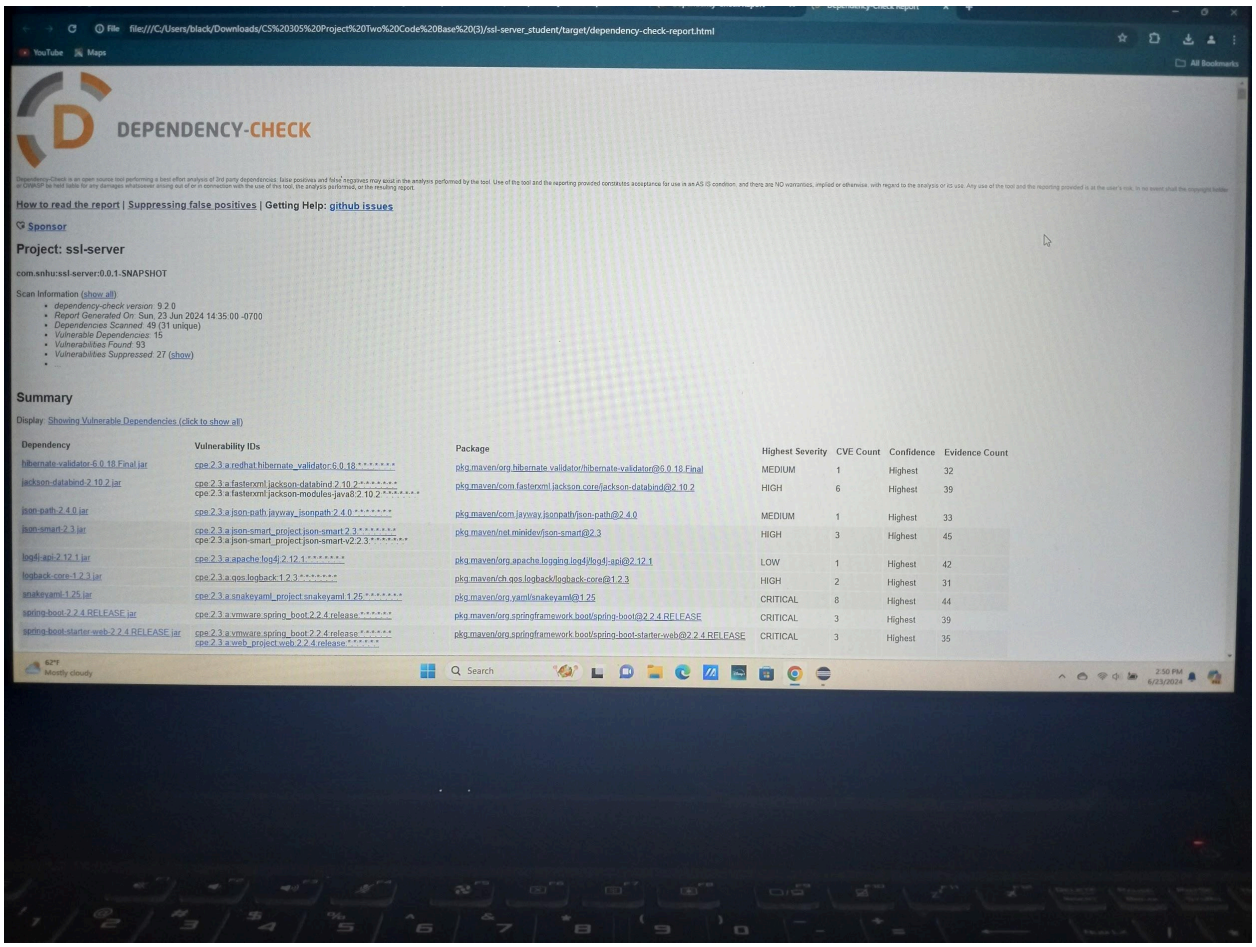


]

6. Functional Testing

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

[



DEPENDENCY-CHECK

How to read the report | Suppressing false positives | Getting Help: github issues

Sponsor

Project: ssl-server

com.snhu:ssl-server:0.0.1-SNAPSHOT

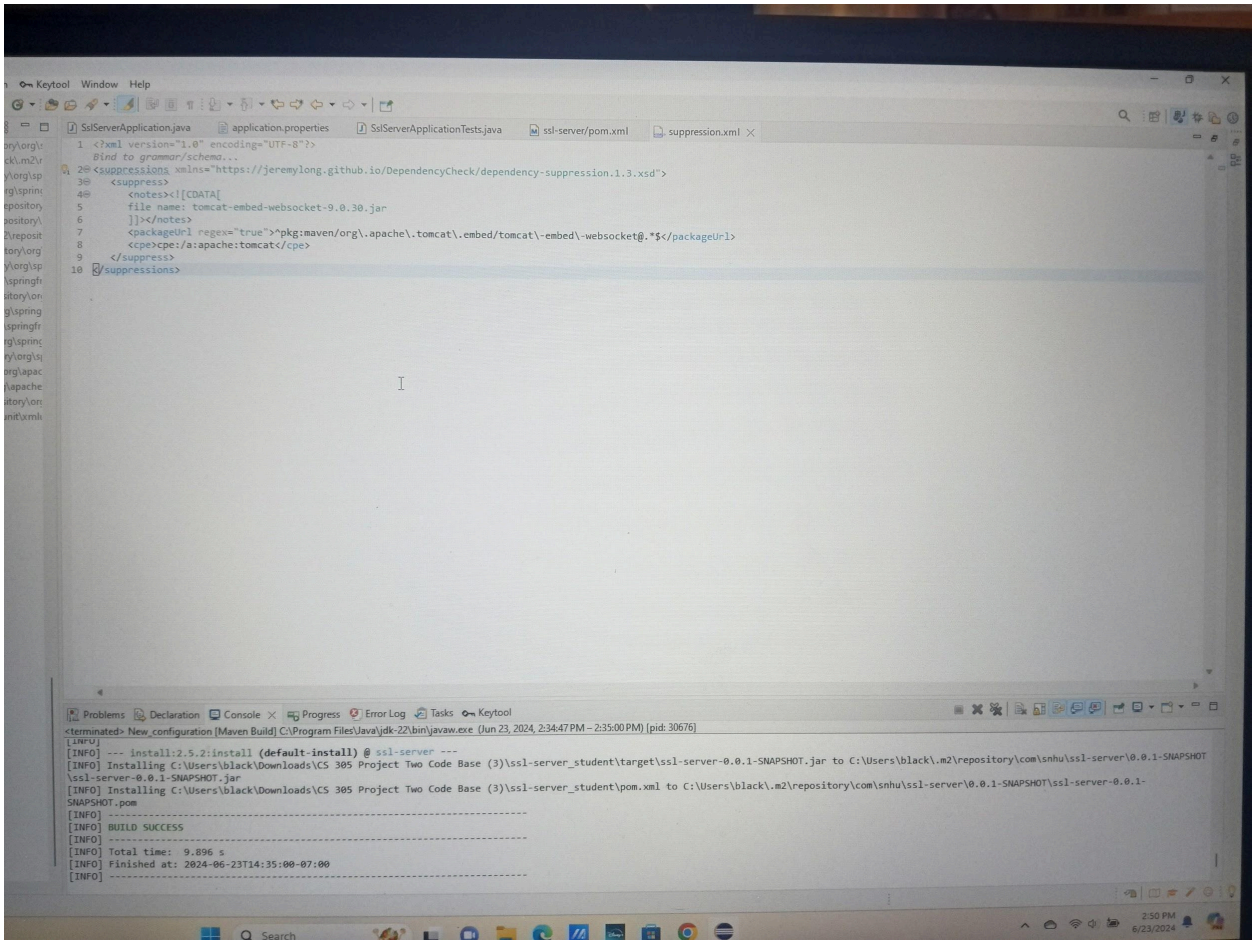
Scan Information (show all)

- *dependency-check version*: 9.2.0
- *Report Generated On*: Sun, 23 Jun 2024 14:35:00 -0700
- *Dependencies Scanned*: 49 (31 unique)
- *Vulnerable Dependencies*: 15
- *Vulnerabilities Found*: 93
- *Vulnerabilities Suppressed*: 27 (show)

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
hibernate-validator-6.0.18.Final.jar	cpe:2.3:a:redhat:hibernate_validator:6.0.18:*:*:*:*:*:*:*	pkg:maven/org.hibernate.validator/hibernate-validator@6.0.18.Final	MEDIUM	1	Highest	32
jackson-databind-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:* cpe:2.3:a:fasterxml:jackson-modules-java8:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	6	Highest	39
json-path-2.4.0.jar	cpe:2.3:a:json-path:jayway_jsonpath:2.4.0:*:*:*:*:*:*:*	pkg:maven/com.jayway.jsonpath/json-path@2.4.0	MEDIUM	1	Highest	33
json-smart-2.3.jar	cpe:2.3:a:json-smart_project:json-smart:2.3:*:*:*:*:*:*:* cpe:2.3:a:json-smart_project:json-smart-v2:2.3:*:*:*:*:*:*:*	pkg:maven/net.minidev/json-smart@2.3	HIGH	3	Highest	45
log4j-api-2.12.1.jar	cpe:2.3:a:apache:log4j:2.12.1:*:*:*:*:*:*:*	pkg:maven/org.apache.logging.log4j/log4j-api@2.12.1	LOW	1	Highest	42
logback-core-1.2.3.jar	cpe:2.3:a:qos:logback:1.2.3:*:*:*:*:*:*:*	pkg:maven/ch.qos.logback/logback-core@1.2.3	HIGH	2	Highest	31
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.25	CRITICAL	8	Highest	44
spring-boot-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot@2.2.4.RELEASE	CRITICAL	3	Highest	39
spring-boot-starter-web-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:*:* cpe:2.3:a:web_project:web:2.2.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-web@2.2.4.RELEASE	CRITICAL	3	Highest	35



.]

7. Summary

Software development and Security Practices:

-Validation:This likely refers to input validation,which is a crucial security measure to ensure that data entered by users is safe and does not pose a threat to the system. Proper validation helps prevent common security vulnerabilities like injection attacks.

-Secure Representations:This could relate to using secure data formats or representations to transmit and store data securely. It might involve techniques like using encrypted data formats or secure serialization methods.

-API Secure Interactions:Focuses on securing interactions between different components of an API,ensuring that data exchange is done in a secure and authenticated manner to prevent unauthorized

access or data breaches.

-Code Review:Involves a thorough examination of the codebase to identify and rectify any potential security vulnerabilities, bugs,or inefficiencies. Code reviews are essential for maintaining code quality and security standards.

- Models Cryptography Encryption Use:This suggests the use of cryptographic techniques like encryption to secure sensitive data. Proper encryption helps protect data confidentiality and integrity, especially during data transmission and storage.

-Controllers Architecture Review:Refers to reviewing the architecture and design of controllers within the software system to ensure they are implemented securely and efficiently.

-Client/Server Secure Architecture: Emphasizes the importance of designing a secure architecture for client-server interactions,ensuring that communication between clients and servers is protected from security threats.

-Code Error Secure Error Handling:Highlights the significance of implementing secure error handling mechanisms in the codebase to prevent information leakage and maintain system integrity in case of errors or exceptions.

-Data Access Summary of Findings with Mitigation Plan:Suggests conducting an assessment of data access mechanisms,identifying any vulnerabilities or weaknesses,and devising a plan to mitigate these issues effectively.

-Code Quality Secure Coding:Stresses the importance of maintaining high code quality standards while following secure coding practices to minimize security risks and ensure the reliability of the software.

Services Code Review:Indicates the need for reviewing the code related to services within the system to identify and address any security or quality issues.

8. Industry Standard Best Practices

A.To maintain the software application's existing security using industry standard best practices for secure coding,you can consider implementing the following measures:

-Regularly updating software components and libraries to address known security vulnerabilities.

-Implementing secure coding practices such as input validation,output encoding, and proper error handling to prevent common security issues like injection attacks.

-Using encryption for sensitive data at rest and in transit.

-Implementing access controls and authentication mechanisms to ensure that only authorized users can access the application and its data.

-Conducting regular security assessments,such as penetration testing and code reviews,to identify and address potential security weaknesses.

B.The value of applying industry standard best practices for secure coding to the company's overall well-being includes:

-Mitigating the risk of security breaches,data leaks,and other cyber threats that could result in financial losses,reputational damage,and legal liabilities.

-Enhancing customer trust and confidence in the company's products and services by demonstrating a commitment to security and privacy.

-Ensuring compliance with industry regulations and standards related to data protection and information security.

-Improving the overall quality and reliability of the software application by reducing the likelihood of security-related issues that could impact performance and functionally.