GLOBALRAIN

Practices for Secure Software Report

Table of Contents

Document Revision History

Version	Date	Author	Comments
1.0	Oct 16, 2022	Rui Costa	First Commit

Client

ARTEMIS
FINANCIAL

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
Rui Costa

1. Algorithm Cipher

"A hashing algorithm is a mathematical function that garbles data and makes it unreadable. Hashing algorithms are one-way programs, so the text can't be unscrambled and decoded by anyone else." (Hashing Algorithm Overview: Types, Methodologies & Usage | Okta, n.d.) There are four Common hashing; **MD-5, RIPEMD-160, SHA, and Whirlpool.**

MD5 was one of the first algorithms and was developed in 1991. It's not considered today a secure algorithm since it has been discovered how to decode the algorithm. **RIPEMD-160** was developed in 1990 and is still considered secure today since no one has discovered how to decode the algorithm. **Whirlpool** was developed in 2000, and RIPEMD-160 is still considered secure since no one has decoded the algorithm. The United States government created SHA. In 2001, the NSA and NIST developed the successor to the original SHA called SHA 2.

I'm recommending SHA 2 based on the standout features of the algorithm:

- "It produces 224, 256, 384 or 512 bits hash value." (Difference between SHA1 and SHA2 - GeeksforGeeks)
- SHA2 has more improved certificates than SHA1.
- Used widely.
- "Developed by U.S National Security Agency to replace SH1." (Difference between SHA1 and SHA2 - GeeksforGeeks)

"SHA-256 generates an almost-unique 256-bit (32-byte) signature for a text." (Chris Veness, www.movable-type.co.uk, 2002-2017, n.d.) SHA-256 is a one-way cryptographic function and is a fixed size for any size of the source text. Since it's a one-way process, it's difficult to be compromised by a hacker and other malicious users.

Citations:

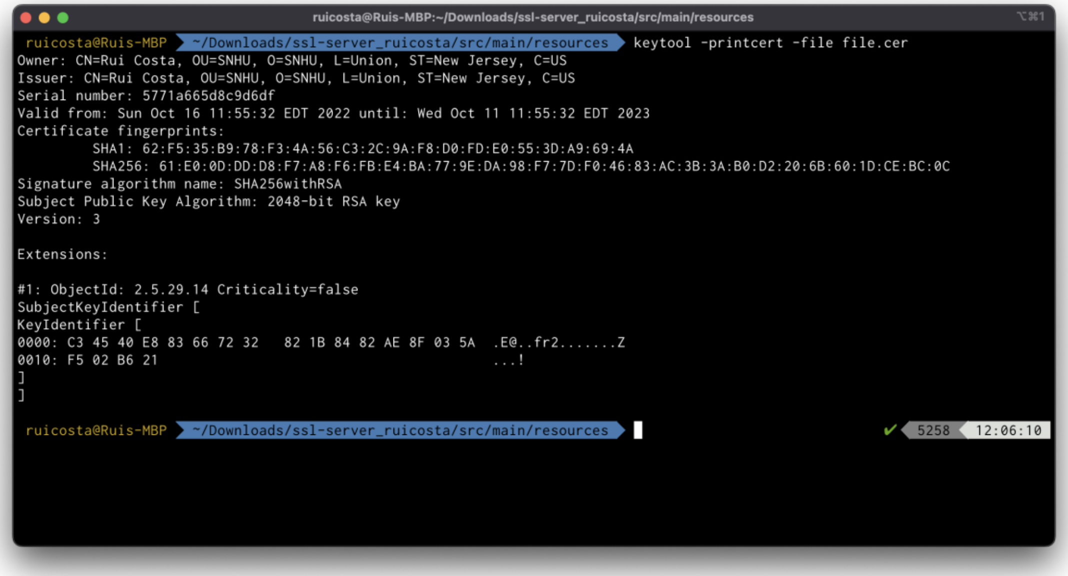
Chris Veness, www.movable-type.co.uk, 2002-2017. (n.d.). *SHA-256 Cryptographic Hash Algorithm implemented in JavaScript | Movable Type Scripts*. Retrieved September 30, 2022, from https://www.movable-type.co.uk/scripts/sha256.html

Hashing Algorithm Overview: Types, Methodologies & Usage | Okta. (n.d.). Okta, Inc. Retrieved September 30, 2022, from https://www.okta.com/identity-101/hashing-algorithms/

Difference between SHA1 and SHA2 - GeeksforGeeks. https://www.geeksforgeeks.org/difference-between-sha1-and-sha2/

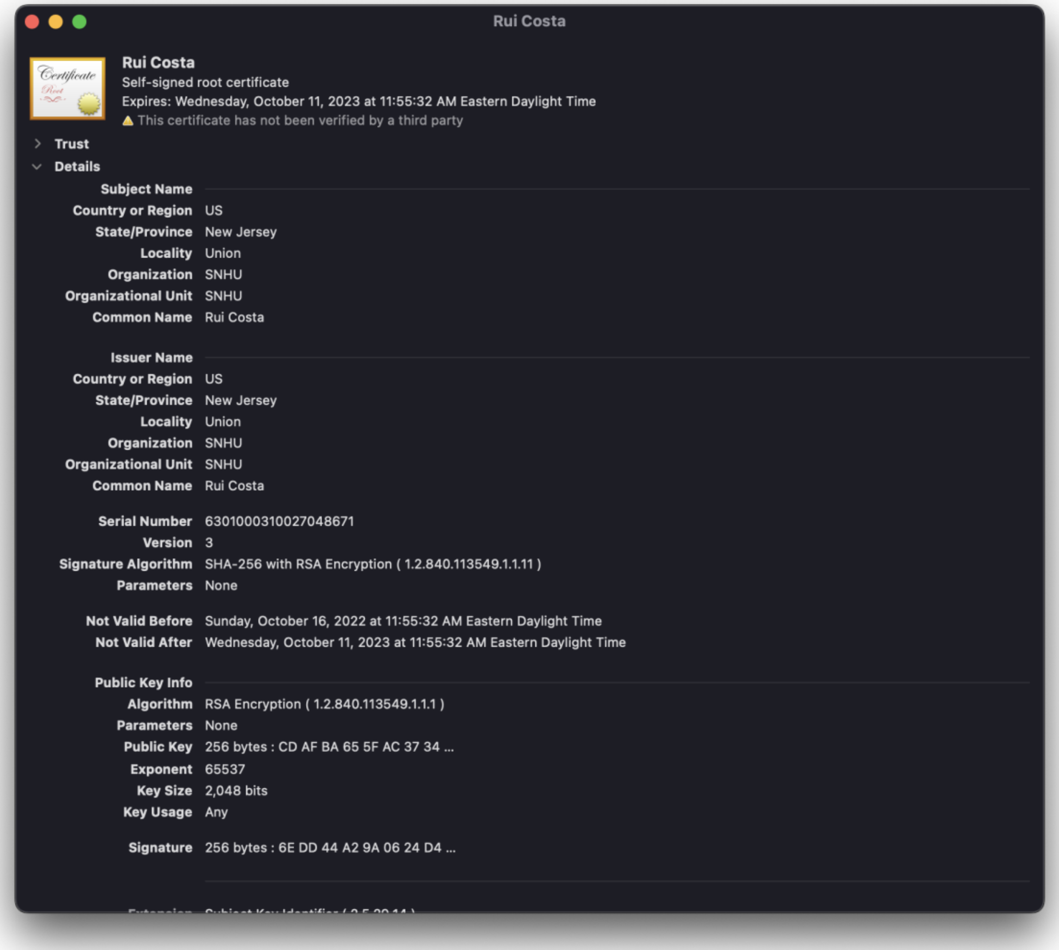
2. Certificate Generation

Insert a screenshot below of the CER file.



ruicosta@Ruis-MBP:~/Downloads/ssl-server_ruicosta/src/main/resources

```
ruicosta@Ruis-MBP  ~/Downloads/ssl-server_ruicosta/src/main/resources  keytool -printcert -file file.cer
Owner: CN=Rui Costa, OU=SNHU, O=SNHU, L=Union, ST=New Jersey, C=US
Issuer: CN=Rui Costa, OU=SNHU, O=SNHU, L=Union, ST=New Jersey, C=US
Serial number: 5771a665d8c9d6df
Valid from: Sun Oct 16 11:55:32 EDT 2022 until: Wed Oct 11 11:55:32 EDT 2023
Certificate fingerprints:
         SHA1: 62:F5:35:B9:78:F3:4A:56:C3:2C:9A:F8:D0:FD:E0:55:3D:A9:69:4A
         SHA256: 61:E0:0D:DD:D8:F7:A8:F6:FB:E4:BA:77:9E:DA:98:F7:7D:F0:46:83:AC:3B:3A:B0:D2:20:6B:60:1D:CE:BC:0C
Signature algorithm name: SHA256withRSA
Subject Public Key Algorithm: 2048-bit RSA key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C3 45 40 E8 83 66 72 32   82 1B 84 82 AE 8F 03 5A  .E@..fr2.......Z
0010: F5 02 B6 21                                        ...!
]
]

ruicosta@Ruis-MBP  ~/Downloads/ssl-server_ruicosta/src/main/resources                 ✔  5258  12:06:10
```



Rui Costa

Rui Costa
Self-signed root certificate
Expires: Wednesday, October 11, 2023 at 11:55:32 AM Eastern Daylight Time
⚠ This certificate has not been verified by a third party

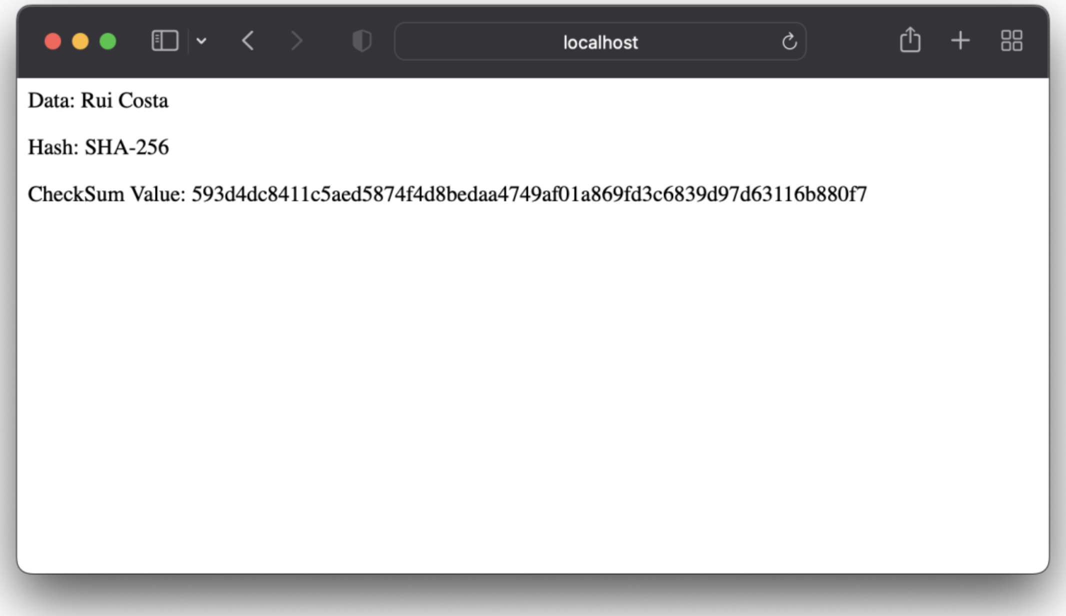
› Trust

⌄ Details

Subject Name	
Country or Region	US
State/Province	New Jersey
Locality	Union
Organization	SNHU
Organizational Unit	SNHU
Common Name	Rui Costa
Issuer Name	
Country or Region	US
State/Province	New Jersey
Locality	Union
Organization	SNHU
Organizational Unit	SNHU
Common Name	Rui Costa
Serial Number	6301000310027048671
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Sunday, October 16, 2022 at 11:55:32 AM Eastern Daylight Time
Not Valid After	Wednesday, October 11, 2023 at 11:55:32 AM Eastern Daylight Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : CD AF BA 65 5F AC 37 34 ...
Exponent	65537
Key Size	2,048 bits
Key Usage	Any
Signature	256 bytes : 6E DD 44 A2 9A 06 24 D4 ...
Extension	Subject Key Identifier (2.5.29.14)

3. Deploy Cipher

Insert a screenshot below of the checksum verification.



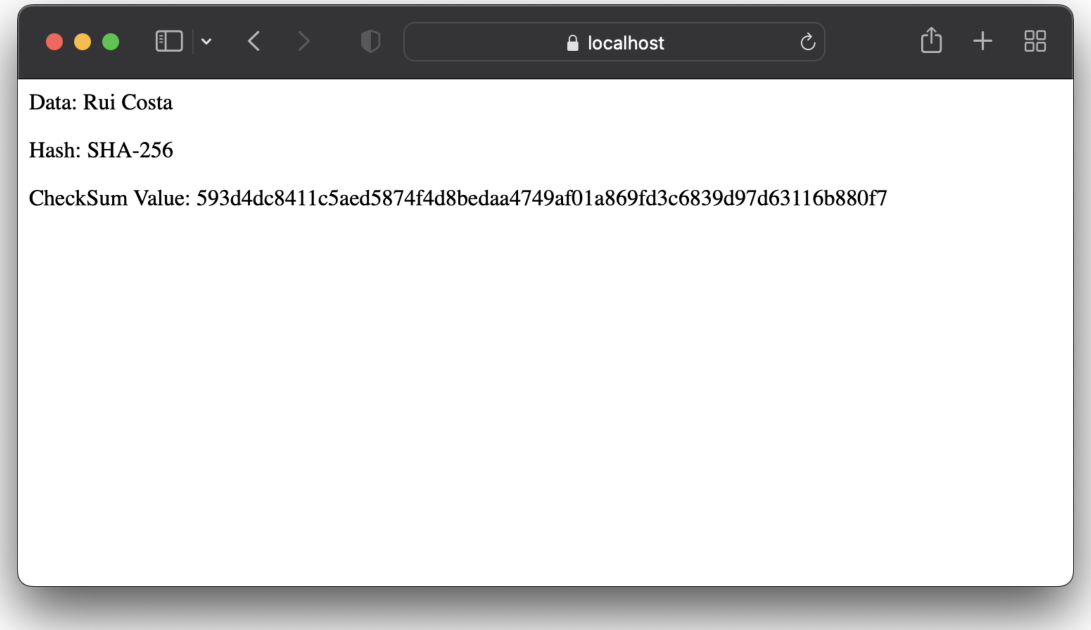
Data: Rui Costa

Hash: SHA-256

CheckSum Value: 593d4dc8411c5aed5874f4d8bedaa4749af01a869fd3c6839d97d63116b880f7

4. Secure Communications

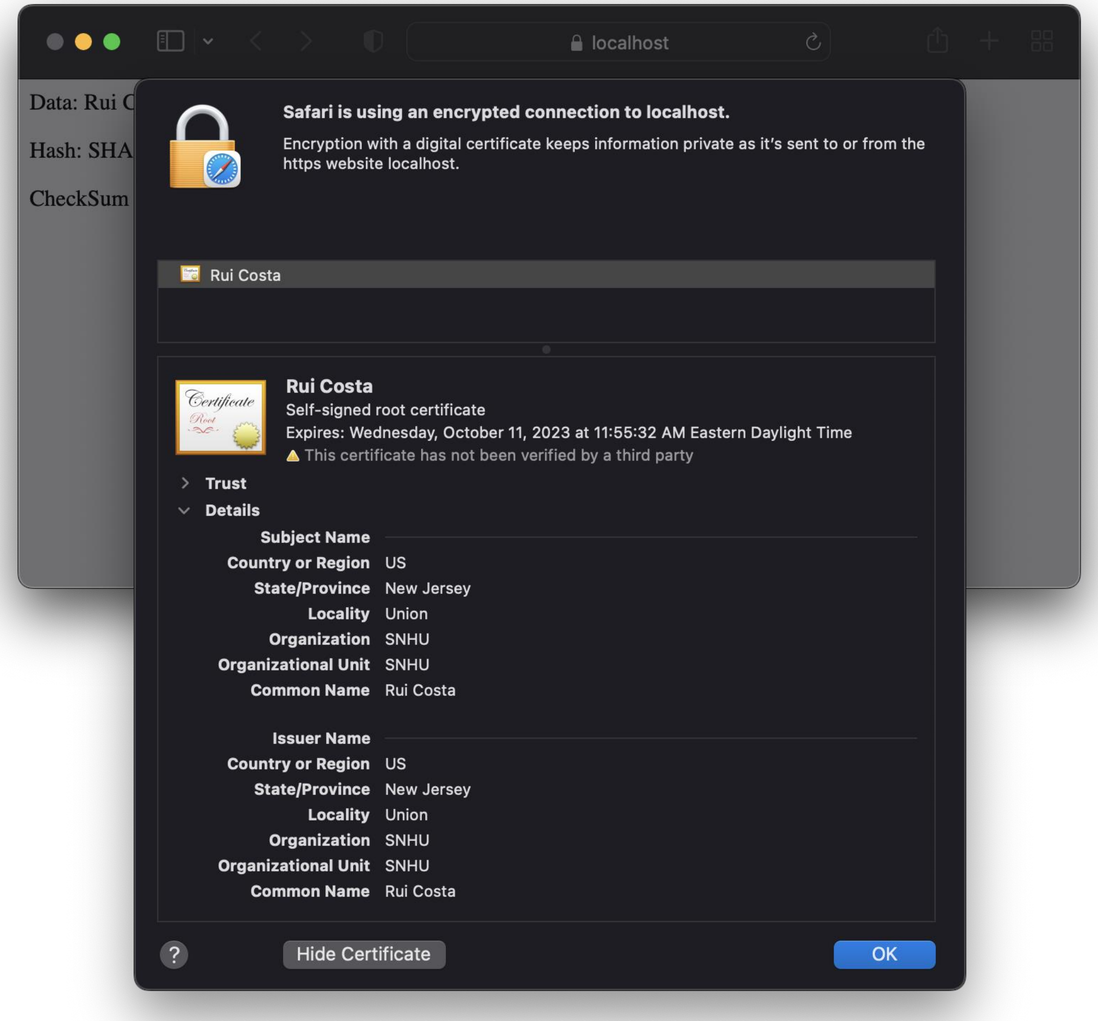
Insert a screenshot below of the web browser that shows a secure webpage.



Data: Rui Costa

Hash: SHA-256

CheckSum Value: 593d4dc8411c5aed5874f4d8bedaa4749af01a869fd3c6839d97d63116b880f7



Safari is using an encrypted connection to localhost.

Encryption with a digital certificate keeps information private as it's sent to or from the https website localhost.

Rui Costa

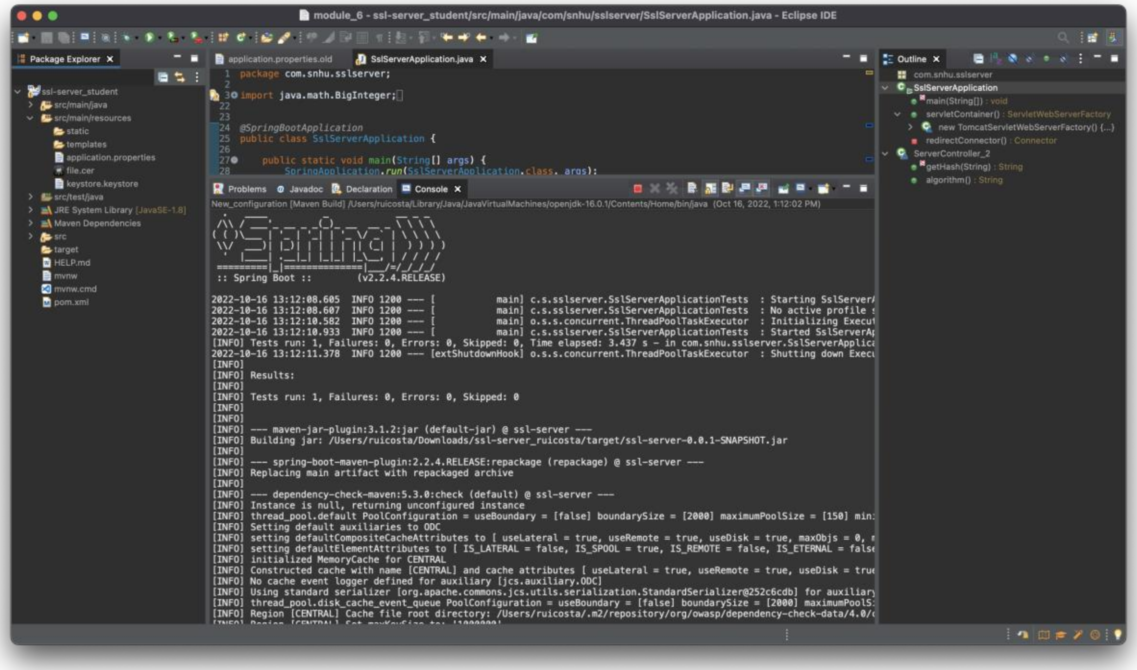
Rui Costa
Self-signed root certificate
Expires: Wednesday, October 11, 2023 at 11:55:32 AM Eastern Daylight Time
⚠ This certificate has not been verified by a third party

› **Trust**
⌄ **Details**

Subject Name	
Country or Region	US
State/Province	New Jersey
Locality	Union
Organization	SNHU
Organizational Unit	SNHU
Common Name	Rui Costa
Issuer Name	
Country or Region	US
State/Province	New Jersey
Locality	Union
Organization	SNHU
Organizational Unit	SNHU
Common Name	Rui Costa

5. Secondary Testing

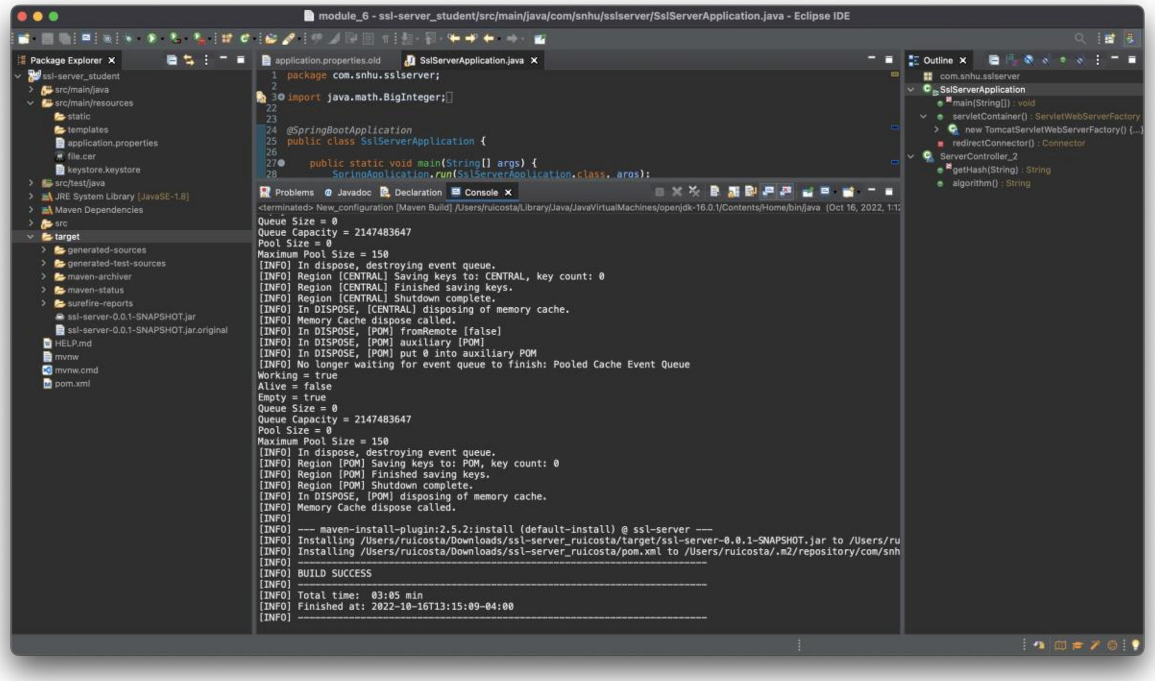
Insert screenshots below of the refactored code executed without errors and the dependency-check report.



module_6 - ssl-server_student/src/main/java/com/snhu/sslserver/SslServerApplication.java - Eclipse IDE

```java
package com.snhu.sslserver;

import java.math.BigInteger;


@SpringBootApplication
public class SslServerApplication {

    public static void main(String[] args) {
        SpringApplication.run(SslServerApplication.class, args);
```

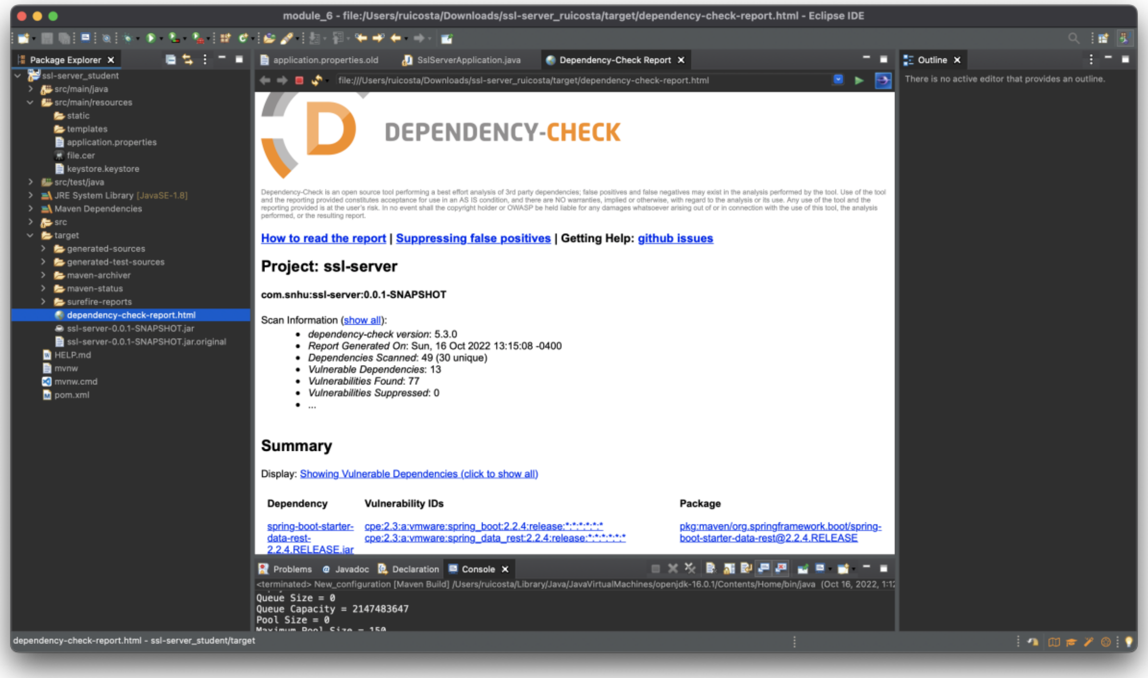
```
New_configuration [Maven Build] /Users/ruicosta/Library/Java/JavaVirtualMachines/openjdk-16.0.1/Contents/Home/bin/java  (Oct 16, 2022, 1:12:02 PM)
  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::        (v2.2.4.RELEASE)

2022-10-16 13:12:08.605  INFO 1200 --- [           main] c.s.sslserver.SslServerApplicationTests  : Starting SslServerA
2022-10-16 13:12:08.607  INFO 1200 --- [           main] c.s.sslserver.SslServerApplicationTests  : No active profile s
2022-10-16 13:12:10.582  INFO 1200 --- [           main] o.s.s.concurrent.ThreadPoolTaskExecutor  : Initializing Execut
2022-10-16 13:12:10.933  INFO 1200 --- [           main] c.s.sslserver.SslServerApplicationTests  : Started SslServerAp
[INFO] Tests run: 1, Failures: 0, Errors: 0, Skipped: 0, Time elapsed: 3.437 s - in com.snhu.sslserver.SslServerApplica
2022-10-16 13:12:11.378  INFO 1200 --- [extShutdownHook] o.s.s.concurrent.ThreadPoolTaskExecutor  : Shutting down Execu
[INFO]
[INFO] Results:
[INFO]
[INFO] Tests run: 1, Failures: 0, Errors: 0, Skipped: 0
[INFO]
[INFO]
[INFO] --- maven-jar-plugin:3.1.2:jar (default-jar) @ ssl-server ---
[INFO] Building jar: /Users/ruicosta/Downloads/ssl-server_ruicosta/target/ssl-server-0.0.1-SNAPSHOT.jar
[INFO]
[INFO] --- spring-boot-maven-plugin:2.2.4.RELEASE:repackage (repackage) @ ssl-server ---
[INFO] Replacing main artifact with repackaged archive
[INFO]
[INFO] --- dependency-check-maven:5.3.0:check (default) @ ssl-server ---
[INFO] Instance is null, returning unconfigured instance
[INFO] thread_pool.default PoolConfiguration = useBoundary = [false] boundarySize = [2000] maximumPoolSize = [150] min:
[INFO] Setting default auxiliaries to ODC
[INFO] setting defaultCompositeCacheAttributes to [ useLateral = true, useRemote = true, useDisk = true, maxObjs = 0, m
[INFO] setting defaultElementAttributes to [ IS_LATERAL = false, IS_SPOOL = true, IS_REMOTE = false, IS_ETERNAL = false
[INFO] initialized MemoryCache for CENTRAL
[INFO] Constructed cache with name [CENTRAL] and cache attributes [ useLateral = true, useRemote = true, useDisk = true
[INFO] No cache event logger defined for auxiliary [jcs.auxiliary.ODC]
[INFO] Using standard serializer [org.apache.commons.jcs.utils.serialization.StandardSerializer@252c6cdb] for auxiliary
[INFO] thread_pool.disk_cache_event_queue PoolConfiguration = useBoundary = [false] boundarySize = [2000] maximumPoolS:
[INFO] Region [CENTRAL] Cache file root directory: /Users/ruicosta/.m2/repository/org/owasp/dependency-check-data/4.0/c
[INFO] Region [CENTRAL] Set maxKeySize to: '1000000'
```



module_6 - ssl-server_student/src/main/java/com/snhu/sslserver/SslServerApplication.java - Eclipse IDE

```java
package com.snhu.sslserver;

import java.math.BigInteger;


@SpringBootApplication
public class SslServerApplication {

    public static void main(String[] args) {
        SpringApplication.run(SslServerApplication.class, args);
```

```
<terminated> New_configuration [Maven Build] /Users/ruicosta/Library/Java/JavaVirtualMachines/openjdk-16.0.1/Contents/Home/bin/java  (Oct 16, 2022, 1:1
Queue Size = 0
Queue Capacity = 2147483647
Pool Size = 0
Maximum Pool Size = 150
[INFO] In dispose, destroying event queue.
[INFO] Region [CENTRAL] Saving keys to: CENTRAL, key count: 0
[INFO] Region [CENTRAL] Finished saving keys.
[INFO] Region [CENTRAL] Shutdown complete.
[INFO] In DISPOSE, [CENTRAL] disposing of memory cache.
[INFO] Memory Cache dispose called.
[INFO] In DISPOSE, [POM] fromRemote [false]
[INFO] In DISPOSE, [POM] auxiliary [POM]
[INFO] In DISPOSE, [POM] put 0 into auxiliary POM
[INFO] No longer waiting for event queue to finish: Pooled Cache Event Queue
Working = true
Alive = false
Empty = true
Queue Size = 0
Queue Capacity = 2147483647
Pool Size = 0
Maximum Pool Size = 150
[INFO] In dispose, destroying event queue.
[INFO] Region [POM] Saving keys to: POM, key count: 0
[INFO] Region [POM] Finished saving keys.
[INFO] Region [POM] Shutdown complete.
[INFO] In DISPOSE, [POM] disposing of memory cache.
[INFO] Memory Cache dispose called.
[INFO]
[INFO] --- maven-install-plugin:2.5.2:install (default-install) @ ssl-server ---
[INFO] Installing /Users/ruicosta/Downloads/ssl-server_ruicosta/target/ssl-server-0.0.1-SNAPSHOT.jar to /Users/ru
[INFO] Installing /Users/ruicosta/Downloads/ssl-server_ruicosta/pom.xml to /Users/ruicosta/.m2/repository/com/snh
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  03:05 min
[INFO] Finished at: 2022-10-16T13:15:09-04:00
[INFO] ------------------------------------------------------------------------
```


module_6 - file:/Users/ruicosta/Downloads/ssl-server_ruicosta/target/dependency-check-report.html - Eclipse IDE
Package Explorer
application.properties.old
SslServerApplication.java
Dependency-Check Report
Outline
There is no active editor that provides an outline.
file:///Users/ruicosta/Downloads/ssl-server_ruicosta/target/dependency-check-report.html
DEPENDENCY-CHECK
dependency-check-report.html - ssl-server_student/target

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

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

Project: ssl-server

com.snhu:ssl-server:0.0.1-SNAPSHOT

Scan Information (show all):

- *dependency-check version*: 5.3.0
- *Report Generated On*: Sun, 16 Oct 2022 13:15:08 -0400
- *Dependencies Scanned*: 49 (30 unique)
- *Vulnerable Dependencies*: 13
- *Vulnerabilities Found*: 77
- *Vulnerabilities Suppressed*: 0
- ...

Summary

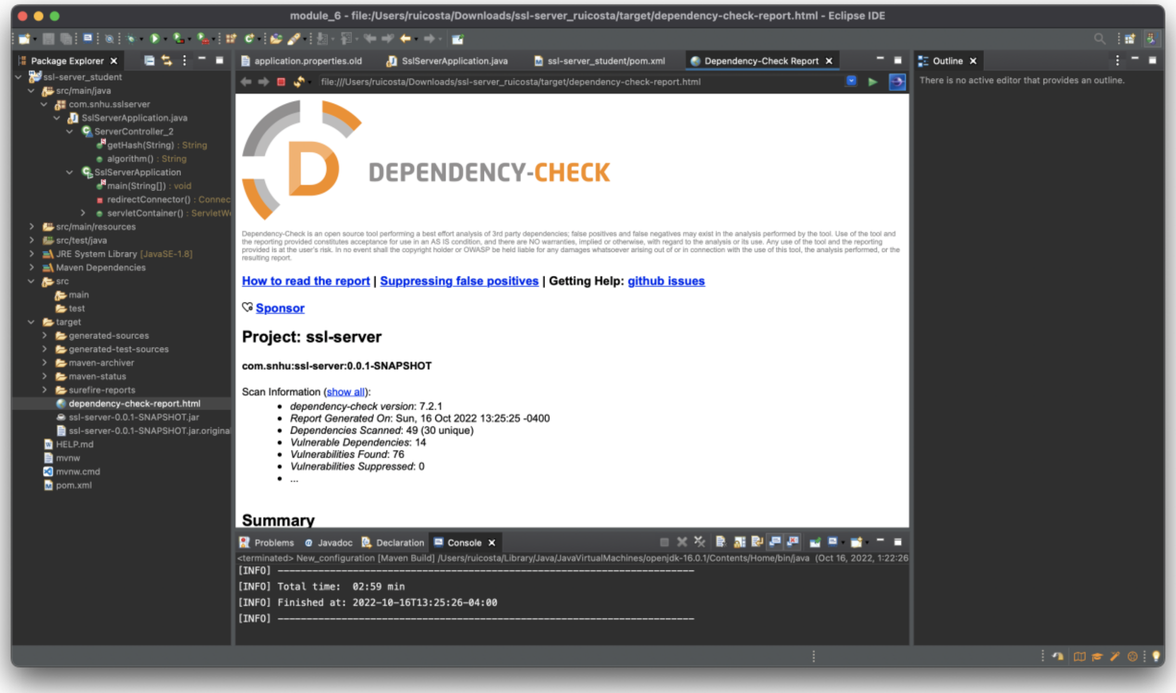
Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package
spring-boot-starter-data-rest-2.2.4.RELEASE.jar	cpe:2.3:a:vmware:spring_boot:2.2.4:release:*:*:*:*:* cpe:2.3:a:vmware:spring_data_rest:2.2.4:release:*:*:*:*:*	pkg:maven/org.springframework.boot/spring-boot-starter-data-rest@2.2.4.RELEASE

```
<terminated> New_configuration [Maven Build] /Users/ruicosta/Library/Java/JavaVirtualMachines/openjdk-16.0.1/Contents/Home/bin/java  (Oct 16, 2022, 1:1
Queue Size = 0
Queue Capacity = 2147483647
Pool Size = 0
Maximum Pool Size = 150
```

6. Functional Testing

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


module_6 - file:/Users/ruicosta/Downloads/ssl-server_ruicosta/target/dependency-check-report.html - Eclipse IDE
Package Explorer
application.properties.old
SslServerApplication.java
ssl-server_student/pom.xml
Dependency-Check Report
Outline
There is no active editor that provides an outline.
file:///Users/ruicosta/Downloads/ssl-server_ruicosta/target/dependency-check-report.html
DEPENDENCY-CHECK

Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

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*: 7.2.1
- *Report Generated On*: Sun, 16 Oct 2022 13:25:25 -0400
- *Dependencies Scanned*: 49 (30 unique)
- *Vulnerable Dependencies*: 14
- *Vulnerabilities Found*: 76
- *Vulnerabilities Suppressed*: 0
- ...

Summary

```
<terminated> New_configuration [Maven Build] /Users/ruicosta/Library/Java/JavaVirtualMachines/openjdk-16.0.1/Contents/Home/bin/java  (Oct 16, 2022, 1:22:26
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  02:59 min
[INFO] Finished at: 2022-10-16T13:25:26-04:00
[INFO] ------------------------------------------------------------------------
```

7. Summary

The areas of Security reviewed and addressed:

a. Input Validation (Secure input and Representations): Artemis Finacial's web-based application requires users to authenticate to gain access to their respective portfolios and services provided by Artemis Financial. Failure to conduct proper input validation will leave Artemis Financial vulnerable to cross-site scripting attacks and Structured language injections. XSS and SQL injection are among the most dangerous attacks. "XSS is a client-side vulnerability that targets other application users, while SQL injection is a server-side vulnerability that targets the application's database" (What Is Cross-site Scripting (XSS) and How to Prevent It? | Web Security Academy, n.d.).
b. APIs (Secure API's Interactions): Artemis Finacial's web-based application uses RESTful APIs. "Application programming interface (API) security refers to the practice of preventing or mitigating attacks on APIs. APIs work as the backend framework for mobile and web applications. Therefore, it is critical to protect the sensitive data they transfer. (What Is API Security?, n.d.)" Since the APIS sensitive customer information, security mitigations must be in place to prevent attacks or vulnerabilities.
c. Cryptography (Secure Distributed Composting): Since Artemis Financial is working with sensitive customer data, data should be secured in transit and at rest. This prevents eavesdropping on communications and access to data residing on disk since communications will be encrypted. The Java Cryptography Architecture (JCA) and The Java Cryptography Extension (JCE) will also be used to provide a security framework.
d. Client/Server (Secure Distributed Composing): Client/Server composes the communication between the customer and the web application's backend. The security of Client/Server communications is vital to a secure platform. Items such as authentication, encryption, and monitoring must be considered to have secure Client/Server communications.
e. Code Error (Secure Error Handling): Error handling should correctly use secure exceptions often missed during software design. These and other considerations need to be considered to mitigate future threats.
f. Code Quality (Secure Coding practices/patterns): Code quality is vital to having a secure and reliable platform. The code must be rigorously tested, and software engineers must include unit tests. Code quality also requires software engineers to document and comment on their code properly, allowing other software engineers to understand the logic quickly. This process will help mitigate errors as well as troubleshoot new errors.
g. Encapsulation (Secure Data Structures): "Encapsulation is an important feature that allows a programmer to control access to components of a class. Used properly, encapsulation can enhance program security. (Encapsulation CS2 C++.)"Data and its functions must be encapsulated appropriately to ensure an application's operations are secure against vulnerabilities.

Citations and References

Financial Sector Cybersecurity. (n.d.). Center for Strategic and International Studies. Retrieved September 18, 2022, from https://www.csis.org/programs/strategic-technologies-program/archives/cybersecurity-and-governance/financial-sector

IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High. (n.d.). IBM India News Room. Retrieved September 18, 2022, from https://in.newsroom.ibm.com/IBM-Report-Cost-of-Data-Breach-2022

Six most common cyber attacks. (2019, February 15). IT Governance USA Blog. Retrieved September 18, 2022, from https://www.itgovernanceusa.com/blog/six-most-common-cyber-attacks

What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy. (n.d.). Retrieved September 18, 2022, from https://portswigger.net/web-security/cross-site-scripting

What Is API Security? (n.d.). Fortinet. Retrieved September 18, 2022, from https://www.fortinet.com/resources/cyberglossary/api-security

“Encapsulation CS2 C++.” *Security Injection: Encapsulation - CS2 C++*, https://cisserv1.towson.edu/~cyber4all/modules/nanomodules/Encapsulation-CS2_C++.html.

8. Industry Standard Best Practices

We recommend using a trusted Certificate Authorities which was not used in this report.

"The primary advantage of using certificates from a CA is that **the identity of the certificate holder is verified by a trusted third party**."(Benefits of Self-signed and CA-signed Digital Certificates, n.d.) We know the benefits of a TLS; all traffic is encrypted. However, to trust the certificate from the respective domain, we use the CA. The CA validates the identity of the certificate holder.

Citations:

Benefits of Self-signed and CA-signed Digital Certificates. (n.d.). Retrieved October 3, 2022, from https://www.ibm.com/docs/en/b2b-integrator/5.2?topic=certficates-benefits-self-signed-ca-signed-digital-certificates