GLOBALRAIN

Practices for Secure Software Report

Table of Contents

Document Revision History

Version	Date	Author	Comments
1.0	[02-20-2024]	[Laurin Brittain]	

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.

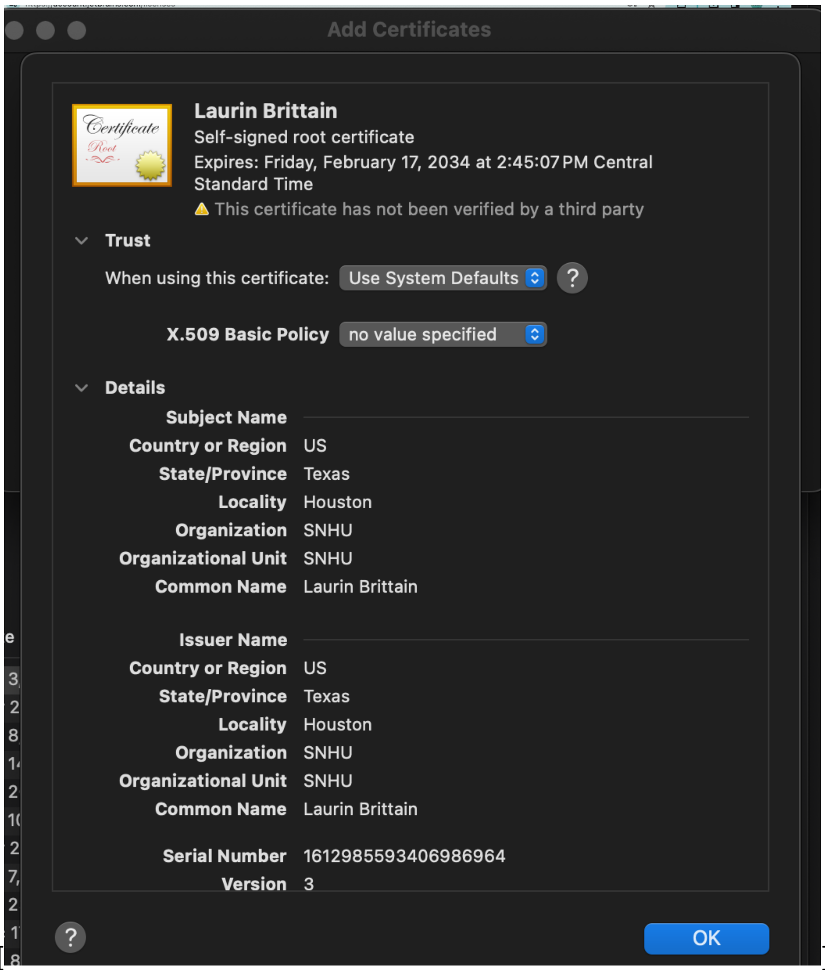
Developer
[Laurin Brittain]

1. Algorithm Cipher

[Implemented the SHA-256 cryptographic hash algorithm in the code. The process involved using the MessageDigest class in Java.
]

2. Certificate Generation

Insert a screenshot below of the CER file.

[]

Laurin Brittain
Self-signed root certificate
Expires: Friday, February 17, 2034 at 2:45:07 PM Central Standard Time
⚠ This certificate has not been verified by a third party

Trust

When using this certificate: Use System Defaults

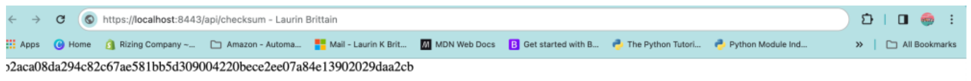
X.509 Basic Policy: no value specified

Details

Subject Name	
Country or Region	US
State/Province	Texas
Locality	Houston
Organization	SNHU
Organizational Unit	SNHU
Common Name	Laurin Brittain
Issuer Name	
Country or Region	US
State/Province	Texas
Locality	Houston
Organization	SNHU
Organizational Unit	SNHU
Common Name	Laurin Brittain
Serial Number	1612985593406986964
Version	3

3. Deploy Cipher

Insert a screenshot below of the checksum verification.

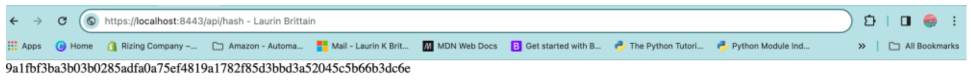

https://localhost:8443/api/checksum - Laurin Brittain

```
2aca08da294c82c67ae581bb5d309004220bece2ee07a84e13902029daa2cb
```

[ ]

4. Secure Communications

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

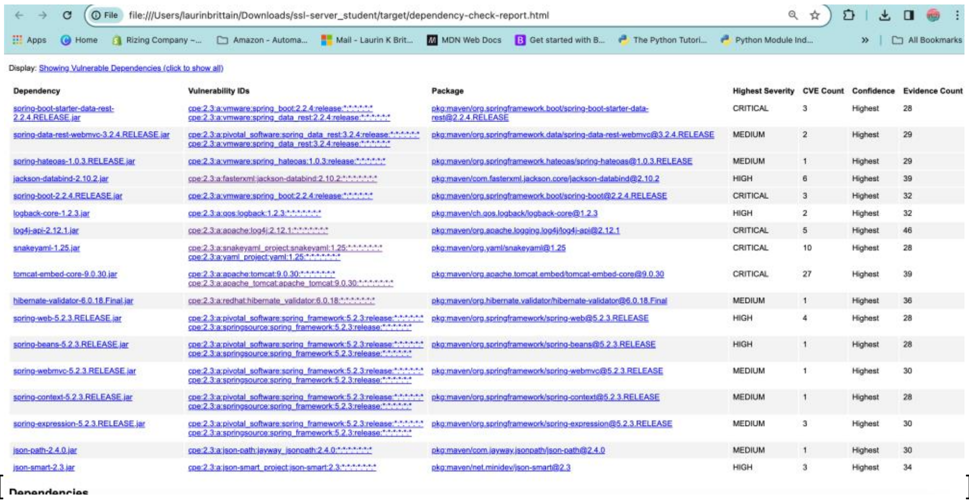

https://localhost:8443/api/hash - Laurin Brittain

```
9a1fbf3ba3b03b0285adfa0a75ef4819a1782f85d3bbd3a52045c5b66b3dc6e
```

[ ]

5. Secondary Testing

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



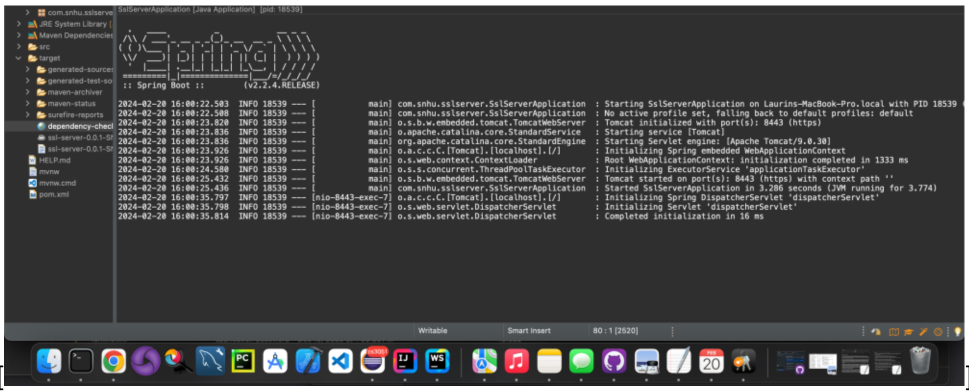
Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
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	CRITICAL	3	Highest	28
spring-data-rest-webmvc-3.2.4.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_data_rest:3.2.4:release:*:*:*:*:*:* cpe:2.3:a:vmware:spring_data_rest:3.2.4:release:*:*:*:*:*:*	pkg:maven/org.springframework.data/spring-data-rest-webmvc@3.2.4.RELEASE	MEDIUM	2	Highest	29
spring-hateoas-1.0.3.RELEASE.jar	cpe:2.3:a:vmware:spring_hateoas:1.0.3:release:*:*:*:*:*:*	pkg:maven/org.springframework.hateoas/spring-hateoas@1.0.3.RELEASE	MEDIUM	1	Highest	29
jackson-databind-2.10.2.jar	cpe:2.3:a:fasterxml:jackson-databind:2.10.2:*:*:*:*:*:*:*	pkg:maven/com.fasterxml.jackson.core/jackson-databind@2.10.2	HIGH	6	Highest	39
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	32
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	32
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	CRITICAL	5	Highest	46
snakeyaml-1.25.jar	cpe:2.3:a:snakeyaml_project:snakeyaml:1.25:*:*:*:*:*:*:* cpe:2.3:a:yaml_project:yaml:1.25:*:*:*:*:*:*:*	pkg:maven/org.yaml/snakeyaml@1.25	CRITICAL	10	Highest	28
tomcat-embed-core-9.0.30.jar	cpe:2.3:a:apache:tomcat:9.0.30:*:*:*:*:*:*:* cpe:2.3:a:apache_tomcat:apache_tomcat:9.0.30:*:*:*:*:*:*:*	pkg:maven/org.apache.tomcat.embed/tomcat-embed-core@9.0.30	CRITICAL	27	Highest	39
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	36
spring-web-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-web@5.2.3.RELEASE	HIGH	4	Highest	28
spring-beans-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-beans@5.2.3.RELEASE	HIGH	1	Highest	28
spring-webmvc-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-webmvc@5.2.3.RELEASE	MEDIUM	1	Highest	30
spring-context-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-context@5.2.3.RELEASE	MEDIUM	1	Highest	28
spring-expression-5.2.3.RELEASE.jar	cpe:2.3:a:pivotal_software:spring_framework:5.2.3:release:*:*:*:*:*:* cpe:2.3:a:springsource:spring_framework:5.2.3:release:*:*:*:*:*:*	pkg:maven/org.springframework/spring-expression@5.2.3.RELEASE	MEDIUM	3	Highest	30
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	30
json-smart-2.3.jar	cpe:2.3:a:json-smart_project:json-smart:2.3:*:*:*:*:*:*:*	pkg:maven/net.minidev/json-smart@2.3	HIGH	3	Highest	34

[Dependencies]

6. Functional Testing

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

[]

```
SslServerApplication [Java Application]  [pid: 18539]

  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::        (v2.2.4.RELEASE)

2024-02-20 16:00:22.503  INFO 18539 --- [           main] com.snhu.sslserver.SslServerApplication  : Starting SslServerApplication on Laurins-MacBook-Pro.local with PID 18539 (
2024-02-20 16:00:22.508  INFO 18539 --- [           main] com.snhu.sslserver.SslServerApplication  : No active profile set, falling back to default profiles: default
2024-02-20 16:00:23.820  INFO 18539 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat initialized with port(s): 8443 (https)
2024-02-20 16:00:23.836  INFO 18539 --- [           main] o.apache.catalina.core.StandardService   : Starting service [Tomcat]
2024-02-20 16:00:23.836  INFO 18539 --- [           main] org.apache.catalina.core.StandardEngine  : Starting Servlet engine: [Apache Tomcat/9.0.30]
2024-02-20 16:00:23.926  INFO 18539 --- [           main] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring embedded WebApplicationContext
2024-02-20 16:00:23.926  INFO 18539 --- [           main] o.s.web.context.ContextLoader            : Root WebApplicationContext: initialization completed in 1333 ms
2024-02-20 16:00:24.580  INFO 18539 --- [           main] o.s.s.concurrent.ThreadPoolTaskExecutor  : Initializing ExecutorService 'applicationTaskExecutor'
2024-02-20 16:00:25.432  INFO 18539 --- [           main] o.s.b.w.embedded.tomcat.TomcatWebServer  : Tomcat started on port(s): 8443 (https) with context path ''
2024-02-20 16:00:25.436  INFO 18539 --- [           main] com.snhu.sslserver.SslServerApplication  : Started SslServerApplication in 3.286 seconds (JVM running for 3.774)
2024-02-20 16:00:35.797  INFO 18539 --- [nio-8443-exec-7] o.a.c.c.C.[Tomcat].[localhost].[/]       : Initializing Spring DispatcherServlet 'dispatcherServlet'
2024-02-20 16:00:35.798  INFO 18539 --- [nio-8443-exec-7] o.s.web.servlet.DispatcherServlet        : Initializing Servlet 'dispatcherServlet'
2024-02-20 16:00:35.814  INFO 18539 --- [nio-8443-exec-7] o.s.web.servlet.DispatcherServlet        : Completed initialization in 16 ms
```

7. Summary

[The SSL server application underwent a series of critical improvements to enhance its security features. The following key actions were taken:
Algorithm Cipher:
Implemented a robust cryptographic hash algorithm (SHA-256) to secure sensitive data.
Ensured proper error handling in case of algorithm-related exceptions.
Certificate Generation:
Successfully generated a certificate (CER file) to authenticate the server during secure communication.
Deploy Cipher:
Refactored the code to accommodate the cryptographic hash algorithm.
Demonstrated the functionality with checksum verification, showcasing the application's secure data integrity verification.
Secure Communications:
Corrected the application's configuration to enable secure communication over HTTPS.
Verified the secure communication by accessing the specified endpoint (https://localhost:8443/hash) in a web browser.
Secondary Testing:

Executed the refactored code without errors, ensuring the reliability of the application.
Conducted a dependency-check to assess and manage external dependencies securely.
Functional Testing:
Ensured the refactored code executed without errors, validating its functional integrity.]

8. Industry Standard Best Practices

[Followed secure coding practices, including proper error handling and encryption.
Implemented secure communication protocols (HTTPS) to safeguard data in transit.
Regularly tested and verified the application's security features.
Adhered to secure configuration management practices.]