

Spring AU '21 – Java Code Quality – Morning Session

Name: Sheik Abudhahir K

Date: 27/01/2021

Secure coding standards

1.CWE – Common Weakness Enumeration

- enumerates design and architectural weaknesses, as well as low-level coding and design errors.
- enables better understanding and management of software weaknesses related to architecture and design
- find weaknesses in source code and operational systems
- category system for software weaknesses and vulnerabilities

eg: CWE category 121 is for stack-based buffer overflows

2.OWASP Top 10 – Open web application security project

- provides a checklist for secure coding practices

Some of top OWASP practices to help you protect against vulnerabilities are

- Security by Design
- Password Management
- Access Control
- Error Handling and Logging
- System Configuration
- Threat Modeling
- Cryptographic Practices
- Input Validation and Output Encoding

3.CERT

- Secure coding standards commonly used for C, C++ and Java
- Guidelines for avoiding coding and implementation errors.
- Encourage programmers to follow a uniform set of rules and guidelines

Risk assessment methodology using failure mode, effects and criticality analysis

Eg: Severity – How serious are the consequences of the rule being ignored

3 levels – (1-Low) (2-medium) (3-high)

Low – eg: denial of service attack, abnormal termination

Medium – eg: data integrity violation, unintentional information disclosure

High – eg: run arbitrary code.

4. SANS 25

- Most dangerous software error – links with CWE
- list of the most widespread and critical errors that can lead to serious vulnerabilities in softwares

Top errors:

CWE	Name
89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
306	Missing Authentication for Critical Function

continue in next page

Starting SonarQube server

It is running in localhost:9000

Login page:

Log In to SonarQube

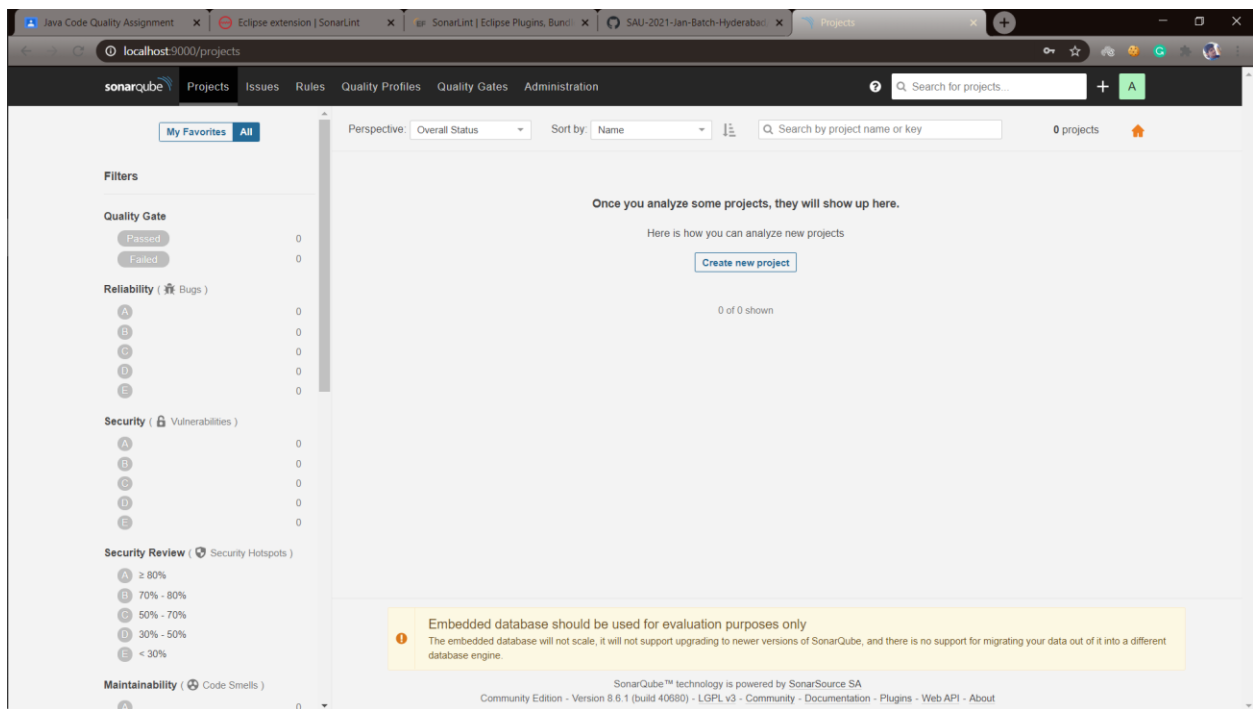
Login

Password

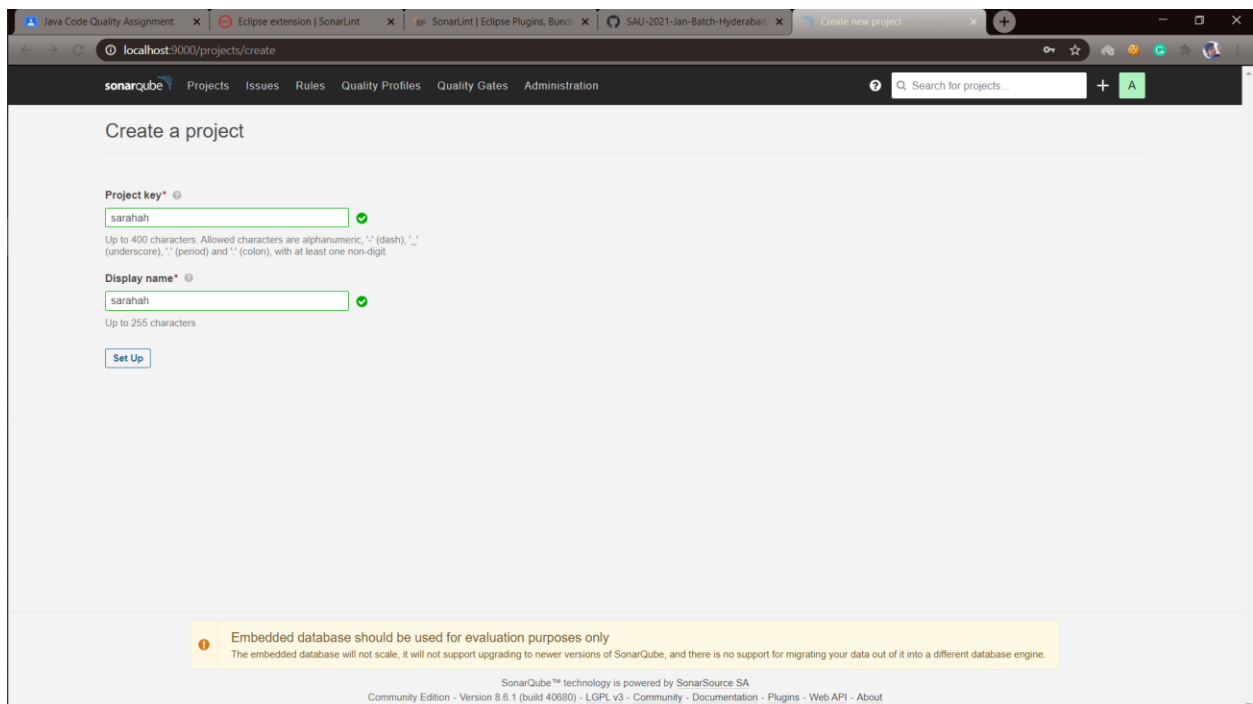
Log in Cancel

SonarQube™ technology is powered by SonarSource SA
L/GPL v3 - Community - Documentation - Plugins

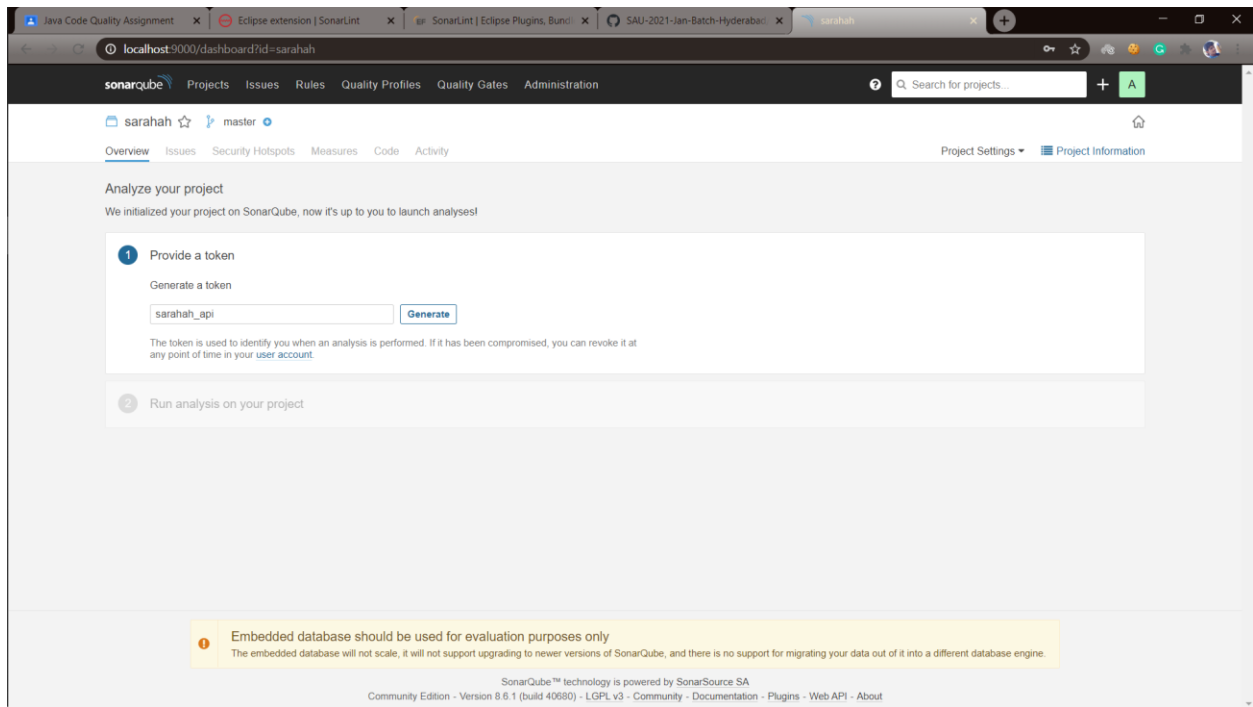
Main page:



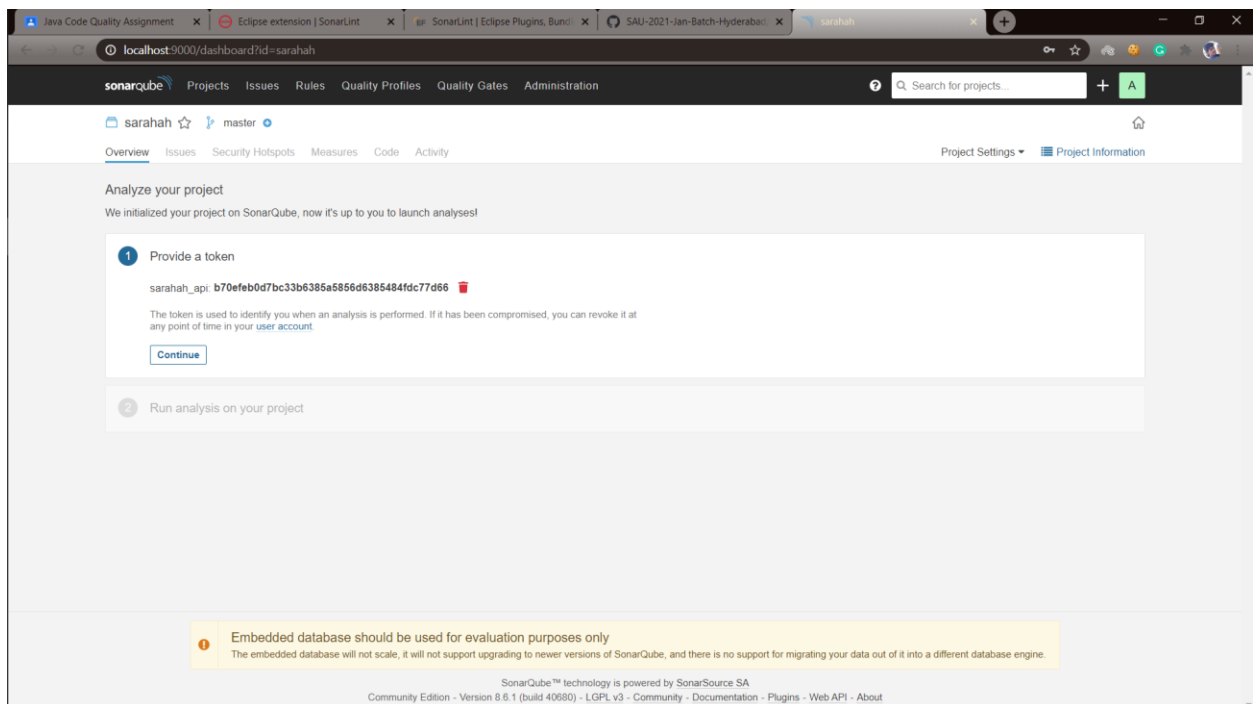
Project creation:



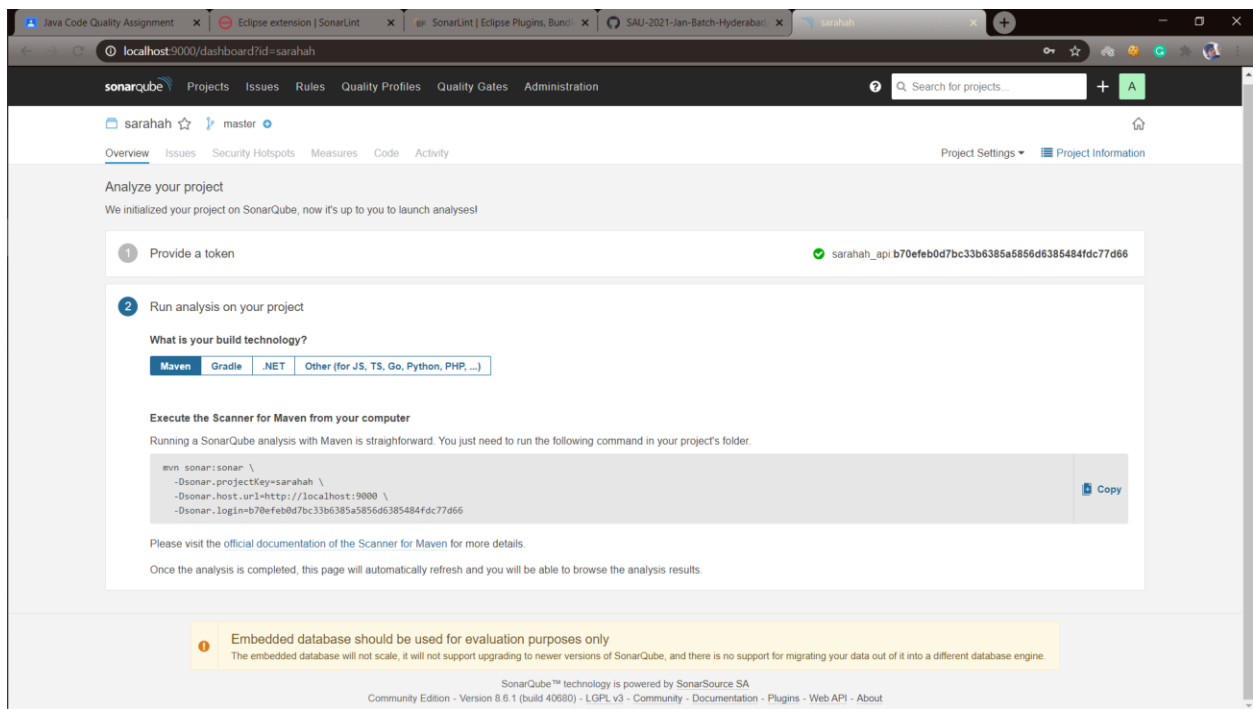
Token generation:



Token generated with the given name



Run analysis on project



sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

sarahah master

Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information

Analyze your project

We initialized your project on SonarQube, now it's up to you to launch analyses!

- 1 Provide a token ✓ sarahah_api b70efeb0d7bc33b6385a5856d6385484fdc77d66
- 2 Run analysis on your project

What is your build technology?

Maven Gradle .NET Other (for J5, TS, Go, Python, PHP, ...)

Execute the Scanner for Maven from your computer

Running a SonarQube analysis with Maven is straightforward. You just need to run the following command in your project's folder.

```
mvn sonar:sonar \
  -Dsonar.projectKey=sarahah \
  -Dsonar.host.url=http://localhost:9000 \
  -Dsonar.login=b70efeb0d7bc33b6385a5856d6385484fdc77d66
```

Copy

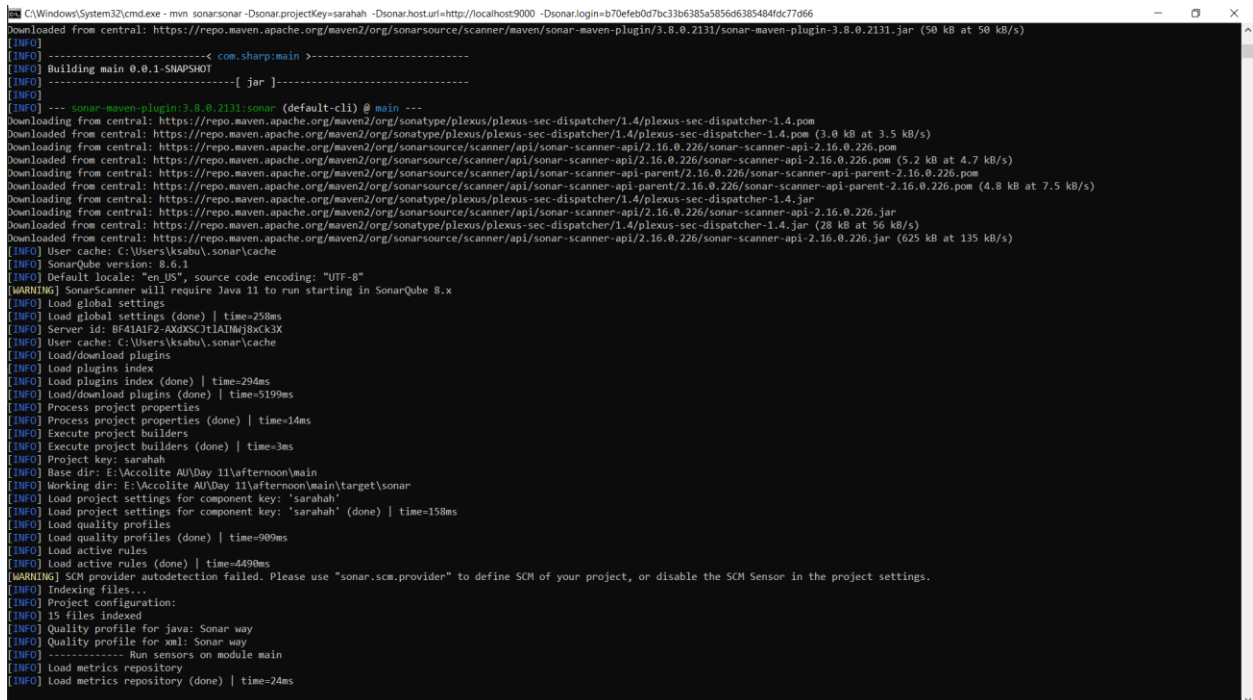
Please visit the official documentation of the Scanner for Maven for more details.

Once the analysis is completed, this page will automatically refresh and you will be able to browse the analysis results.

Embedded database should be used for evaluation purposes only
The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 8.6.1 (build 40680) - LGPL v3 - Community - Documentation - Plugins - Web API - About

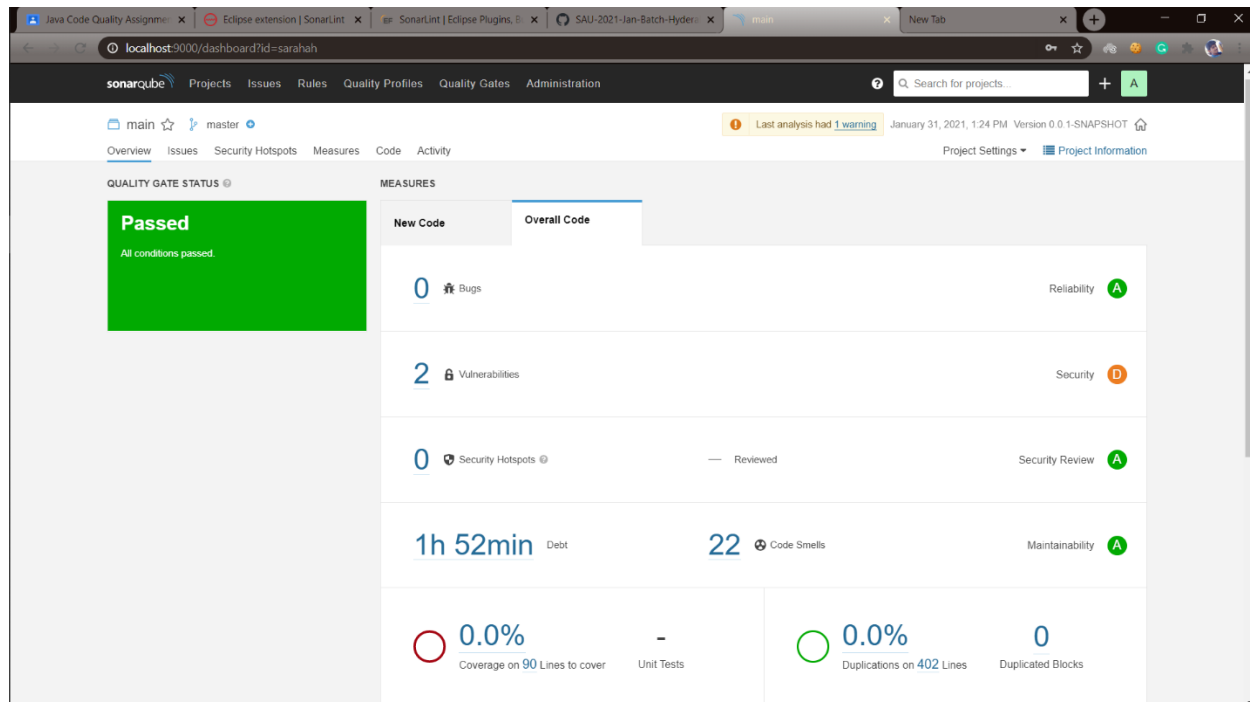
Command Running



```
C:\Windows\System32\cmd.exe - mvn sonar:sonar -Dsonar.projectKey=sarahah -Dsonar.host.url=http://localhost:9000 -Dsonar.login=b70efeb0d7bc33b6385a5856d6385484fdc77d66
Downloaded from central: https://repo.maven.apache.org/maven2/org/sonarsource/scanner/maven/sonar-maven-plugin/3.8.0.2131/sonar-maven-plugin-3.8.0.2131.jar (50 kB at 50 kB/s)
[INFO] -----< com.sharp:main -----
[INFO] Building main 0.0.1-SNAPSHOT
[INFO] -----[ jar ]-----
[INFO] --- sonar-maven-plugin:3.8.0.2131:sonar (default-cli) @ main ---
Downloaded from central: https://repo.maven.apache.org/maven2/org/sonatype/plexus/plexus-sec-dispatcher/1.4/plexus-sec-dispatcher-1.4.pom (3.0 kB at 3.5 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/sonatype/plexus/plexus-sec-dispatcher/1.4/plexus-sec-dispatcher-1.4.jar (28 kB at 56 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/sonarsource/scanner/api/sonar-scanner-api/2.16.0.226/sonar-scanner-api-2.16.0.226.pom (5.2 kB at 4.7 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/sonarsource/scanner/api/sonar-scanner-api-parent/2.16.0.226/sonar-scanner-api-parent-2.16.0.226.pom (4.8 kB at 7.5 kB/s)
Downloaded from central: https://repo.maven.apache.org/maven2/org/sonarsource/scanner/api/sonar-scanner-api-parent/2.16.0.226/sonar-scanner-api-parent-2.16.0.226.jar (625 kB at 135 kB/s)
[INFO] User cache: C:\Users\ksabu\.sonar\cache
[INFO] SonarQube version: 8.6.1
[INFO] Default locale: "en_US", source code encoding: "UTF-8"
[WARNING] SonarScanner will require Java 11 to run starting in SonarQube 8.x
[INFO] Load global settings
[INFO] Load global settings (done) | time=258ms
[INFO] Server id: BF41A1F2-AxDXcJt1AIWj8xck3X
[INFO] User cache: C:\Users\ksabu\.sonar\cache
[INFO] Load/download plugins
[INFO] Load plugins index
[INFO] Load plugins index (done) | time=294ms
[INFO] Load/download plugins (done) | time=5199ms
[INFO] Process project properties
[INFO] Process project properties (done) | time=14ms
[INFO] Execute project builders
[INFO] Execute project builders (done) | time=3ms
[INFO] Project key: sarahah
[INFO] Base dir: E:\Accolite AU\Day 11\afternoon\main
[INFO] Working dir: E:\Accolite AU\Day 11\afternoon\main\target\sonar
[INFO] Load project settings for component key: 'sarahah'
[INFO] Load project settings for component key: 'sarahah' (done) | time=158ms
[INFO] Load quality profiles
[INFO] Load quality profiles (done) | time=909ms
[INFO] Load active rules
[INFO] Load active rules (done) | time=4490ms
[WARNING] SCM provider autodetection failed. Please use "sonar.scm.provider" to define SCM of your project, or disable the SCM Sensor in the project settings.
[INFO] Indexing files...
[INFO] Project configuration:
[INFO] 15 files indexed
[INFO] Quality profile for java: Sonar way
[INFO] Quality profile for xml: Sonar way
[INFO] ----- Run sensors on module main
[INFO] Load metrics repository
[INFO] Load metrics repository (done) | time=24ms
```

```
C:\Windows\System32\cmd.exe
[INFO] 0 source files to be analyzed
[INFO] Java Generated Files AST scan (done) | time=5ms
[INFO] 0/0 source files have been analyzed
[INFO] Sensor JavaSquidSensor [java] (done) | time=8154ms
[INFO] Sensor CSS Rules [cssfamily]
[INFO] No CSS, PHP, HTML or VueJS files are found in the project. CSS analysis is skipped.
[INFO] Sensor CSS Rules [cssfamily] (done) | time=8ms
[INFO] Sensor JaCoCo XML Report Importer [jacoco]
[INFO] 'sonar.coverage.jacoco.xmlReportPaths' is not defined. Using default locations: target/site/jacoco/jacoco.xml,target/site/jacoco-it/jacoco.xml,build/reports/jacoco/test/jacocoTestReport.xml
[INFO] No report imported, no coverage information will be imported by JaCoCo XML Report Importer
[INFO] Sensor JaCoCo XML Report Importer [jacoco] (done) | time=28ms
[INFO] Sensor C# Properties [csharp]
[INFO] Sensor C# Properties [csharp] (done) | time=14ms
[INFO] Sensor SureFireSensor [java]
[INFO] parsing [E:\Vocolite AU\Day 11\afternoon\main\target\surefire-reports]
[INFO] Sensor SureFireSensor [java] (done) | time=19ms
[INFO] Sensor JavaXmlSensor [java]
[INFO] 1 source files to be analyzed
[INFO] Sensor JavaXmlSensor [java] (done) | time=495ms
[INFO] 1/1 source files have been analyzed
[INFO] Sensor HTML [web]
[INFO] Sensor HTML [web] (done) | time=13ms
[INFO] Sensor XML Sensor [xml]
[INFO] 1 source files to be analyzed
[INFO] Sensor XML Sensor [xml] (done) | time=265ms
[INFO] Sensor VB.NET Properties [vbnet]
[INFO] 1/1 source files have been analyzed
[INFO] Sensor VB.NET Properties [vbnet] (done) | time=2ms
[INFO] ----- Run sensors on project
[INFO] Sensor Zero Coverage Sensor
[INFO] Sensor Zero Coverage Sensor (done) | time=60ms
[INFO] Sensor Java CPD Block Indexer
[INFO] Sensor Java CPD Block Indexer (done) | time=100ms
[INFO] SCM Publisher No SCM system was detected. You can use the 'sonar.scm.provider' property to explicitly specify it.
[INFO] CPD Executor 7 files had no CPD blocks
[INFO] CPD Executor Calculating CPD for 6 files
[INFO] CPD Executor CPD calculation finished (done) | time=18ms
[INFO] Analysis report generated in 141ms, dir size=122 KB
[INFO] Analysis report compressed in 3900ms, zip size=38 KB
[INFO] Analysis report uploaded in 449ms
[INFO] ANALYSIS SUCCESSFUL, you can browse http://localhost:9000/dashboard?id=sarahah
[INFO] Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
[INFO] More about the report processing at http://localhost:9000/api/ce/task?id=AX0b5Nw1A1Mj8XcpUJ
[INFO] Analysis total time: 23.949 s
[INFO] -----
[INFO] BUILD SUCCESS
[INFO] -----
[INFO] Total time: 01:54 min
[INFO] Finished at: 2021-01-31T13:24:26+05:30
[INFO] -----
E:\Vocolite AU\Day 11\afternoon\main>
```

Result page:



Vulnerability:

The screenshot displays the SonarQube web interface with the 'Issues' tab selected. The left sidebar shows filters for 'Type' (VULNERABILITY) and 'Severity' (Critical: 2, Info: 0). The main panel lists two vulnerability issues:

- Issue 1:** Replace this persistent entity with a simple POJO or DTO object. Why is this an issue? (2 minutes ago, L35, 10min effort, Critical, Open, Not assigned). Code Smell: cwe, owasp-a5, spring.
- Issue 2:** Replace this persistent entity with a simple POJO or DTO object. Why is this an issue? (2 minutes ago, L47, 10min effort, Critical, Open, Not assigned). Code Smell: cwe, owasp-a5, spring.

At the bottom, a yellow warning banner states: "Embedded database should be used for evaluation purposes only. The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine."

Code smell:

The screenshot displays the SonarQube web interface with the 'Issues' tab selected. The left sidebar shows filters for 'Type' (CODE SMELL) and 'Severity' (Blocker: 1, Critical: 0, Major: 8, Minor: 13, Info: 0). The main panel lists several code smell issues:

- Issue 1:** This block of commented-out lines of code should be removed. Why is this an issue? (3 minutes ago, L17, 5min effort, Code Smell, Major, Open, Not assigned). Code Smell: unused.
- Issue 2:** Remove this unused import 'javax.websocket.server.PathParam'. Why is this an issue? (3 minutes ago, L3, 2min effort, Code Smell, Minor, Open, Not assigned). Code Smell: unused.
- Issue 3:** Remove this unused import 'java.util.Date'. Why is this an issue? (3 minutes ago, L5, 2min effort, Code Smell, Minor, Open, Not assigned). Code Smell: unused.
- Issue 4:** Replace the type specification in this constructor call with the diamond operator ("<>"). Why is this an issue? (3 minutes ago, L41, 1min effort, Code Smell, Minor, Open, Not assigned). Code Smell: clumsy.
- Issue 5:** Replace the type specification in this constructor call with the diamond operator ("<>"). Why is this an issue? (3 minutes ago, L57, 1min effort, Code Smell, Minor, Open, Not assigned). Code Smell: clumsy.
- Issue 6:** This block of commented-out lines of code should be removed. Why is this an issue? (3 minutes ago, L60, 5min effort, Code Smell, Major, Open, Not assigned). Code Smell: unused.
- Issue 7:** This block of commented-out lines of code should be removed. Why is this an issue? (3 minutes ago, L64, 5min effort, Code Smell, Major, Open, Not assigned). Code Smell: unused.
- Issue 8:** Replace the type specification in this constructor call with the diamond operator ("<>"). Why is this an issue? (3 minutes ago, L66, 1min effort, Code Smell, Minor, Open, Not assigned). Code Smell: clumsy.

Severity – Blocker

The screenshot shows the SonarQube web interface with the URL `localhost:9000/project/issues?id=sarahah&resolved=false&severities=BLOCKER&types=CODE_SMELL`. The left sidebar shows the 'Issues' tab selected, with filters for 'Type: CODE_SMELL' and 'Severity: BLOCKER'. The main panel displays a single issue titled 'Add at least one assertion to this test case. Why is this an issue?' located in `src/test/java/com/sharp/main/MainApplicationTests.java`. The issue is classified as a 'Blocker' with a '10min effort' and was created '3 minutes ago'. A yellow warning banner at the bottom states: 'Embedded database should be used for evaluation purposes only. The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.'

Major

The screenshot shows the SonarQube web interface with the URL `localhost:9000/project/issues?id=sarahah&resolved=false&severities=MAJOR&types=CODE_SMELL`. The left sidebar shows the 'Issues' tab selected, with filters for 'Type: CODE_SMELL' and 'Severity: MAJOR'. The main panel displays a list of eight 'Major' issues. The issues are:

- 'This block of commented-out lines of code should be removed. Why is this an issue?' (L17, 5min effort, unused)
- 'This block of commented-out lines of code should be removed. Why is this an issue?' (L60, 5min effort, unused)
- 'This block of commented-out lines of code should be removed. Why is this an issue?' (L64, 5min effort, unused)
- 'Replace this use of System.out or System.err by a logger. Why is this an issue?' (L28, 10min effort, bad-practice, cert)
- 'This block of commented-out lines of code should be removed. Why is this an issue?' (L23, 5min effort, unused)
- 'Return an empty collection instead of null. Why is this an issue?' (L42, 30min effort, cert)
- 'Replace this use of System.out or System.err by a logger. Why is this an issue?' (L66, 10min effort, bad-practice, cert)

The issues are located in various files including `src/_/java/com/sharp/main/controller/HomeController.java`, `src/_/java/com/sharp/main/controller/PrivateMessageController.java`, `src/_/java/com/sharp/main/controller/UserController.java`, and `src/_/com/sharp/main/service/impl/MessageServiceImpl.java`. A yellow warning banner at the bottom is also present, identical to the one in the previous screenshot.

Measures:

