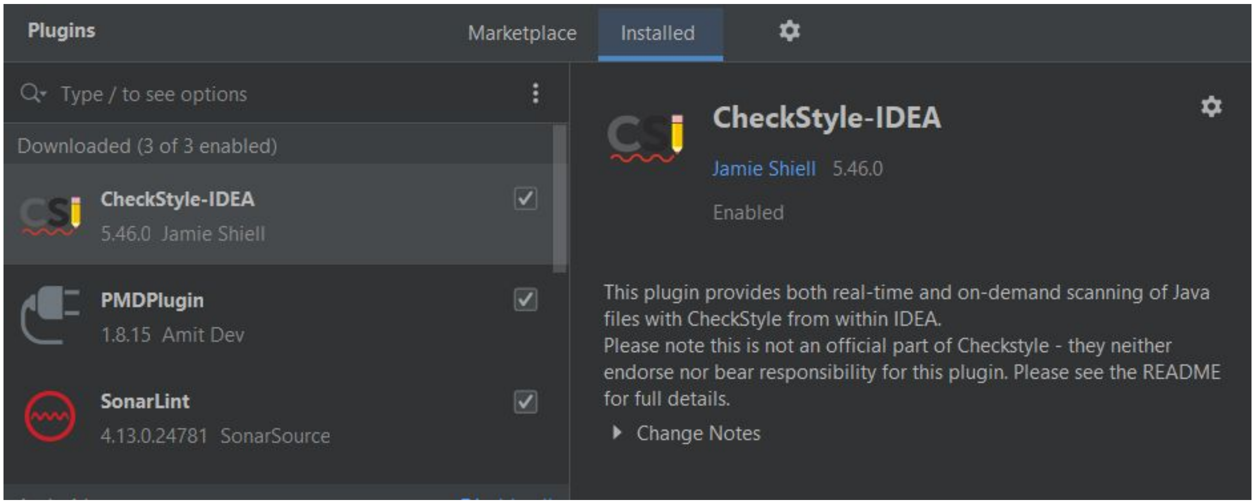
Java Code Quality Assignment

Maithreyan K

A) Please do install following code analyzers in your IDE and document the installation process along with a screenshot of a report of code analysis for each plugin

1) Sonarlint (https://www.sonarlint.org/)
2) PMD (we haven't discussed about it but it's a similar tool) (https://pmd.github.io/)
3) Checkstyle (https://maven.apache.org/plugins/maven-checkstyle-plugin/usage.html)

Plugins Installed



Downloaded (3 of 3 enabled)

- CheckStyle-IDEA 5.46.0 Jamie Shiell ☑
- PMDPlugin 1.8.15 Amit Dev ☑
- SonarLint 4.13.0.24781 SonarSource ☑

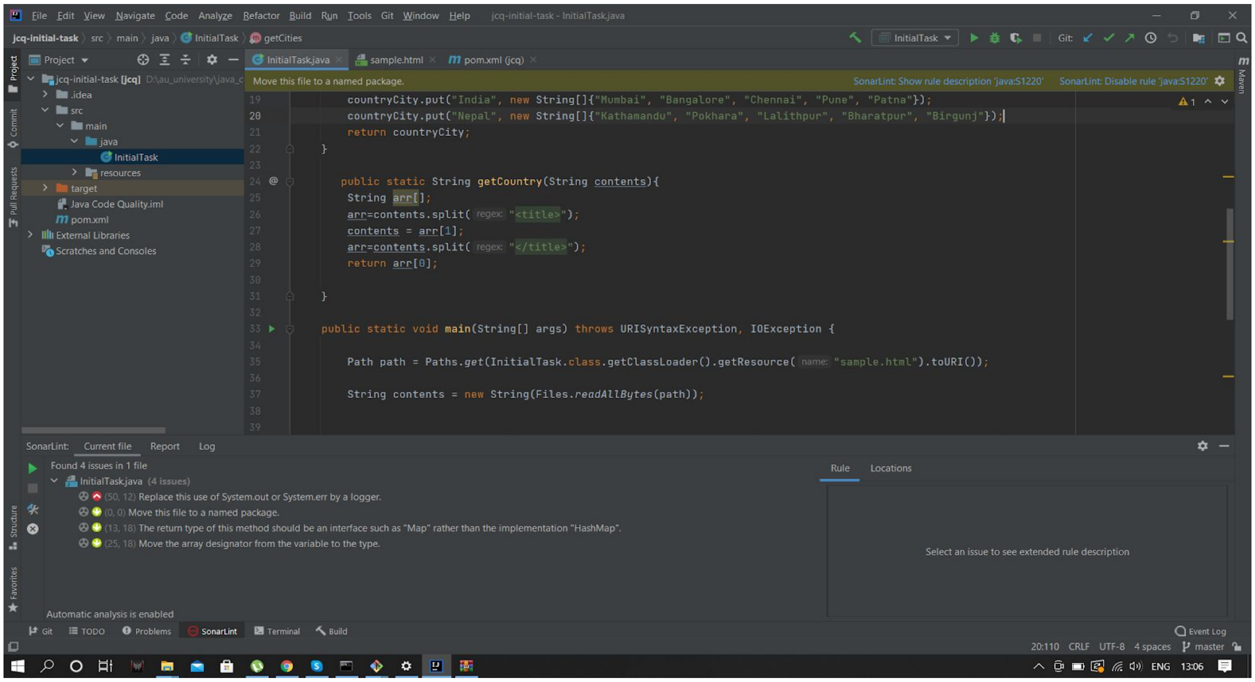
CheckStyle-IDEA

Jamie Shiell 5.46.0

Enabled

This plugin provides both real-time and on-demand scanning of Java files with CheckStyle from within IDEA.
Please note this is not an official part of Checkstyle - they neither endorse nor bear responsibility for this plugin. Please see the README for full details.

1)Sonarlint


File Edit View Navigate Code Analyze Refactor Build Run Tools Git Window Help
jcq-initial-task - InitialTask.java
jcq-initial-task › src › main › java › InitialTask › getCities
InitialTask
Git:
Project
InitialTask.java
sample.html
pom.xml (jcq)
jcq-initial-task [jcq] D:\au_university\java_c
.idea
src
main
java
InitialTask
resources
target
Java Code Quality.iml
pom.xml
External Libraries
Scratches and Consoles
Git
TODO
Problems
SonarLint
Terminal
Build
Event Log
20:110 CRLF UTF-8 4 spaces master
ENG 13:06

Move this file to a named package.

SonarLint: Show rule description 'java:S1220'   SonarLint: Disable rule 'java:S1220'

```
        countryCity.put("India", new String[]{"Mumbai", "Bangalore", "Chennai", "Pune", "Patna"});
        countryCity.put("Nepal", new String[]{"Kathamandu", "Pokhara", "Lalithpur", "Bharatpur", "Birgunj"});
        return countryCity;
    }

      public static String getCountry(String contents){
        String arr[];
        arr=contents.split( regex: "<title>");
        contents = arr[1];
        arr=contents.split( regex: "</title>");
        return arr[0];

    }

    public static void main(String[] args) throws URISyntaxException, IOException {

        Path path = Paths.get(InitialTask.class.getClassLoader().getResource( name: "sample.html").toURI());

        String contents = new String(Files.readAllBytes(path));
```

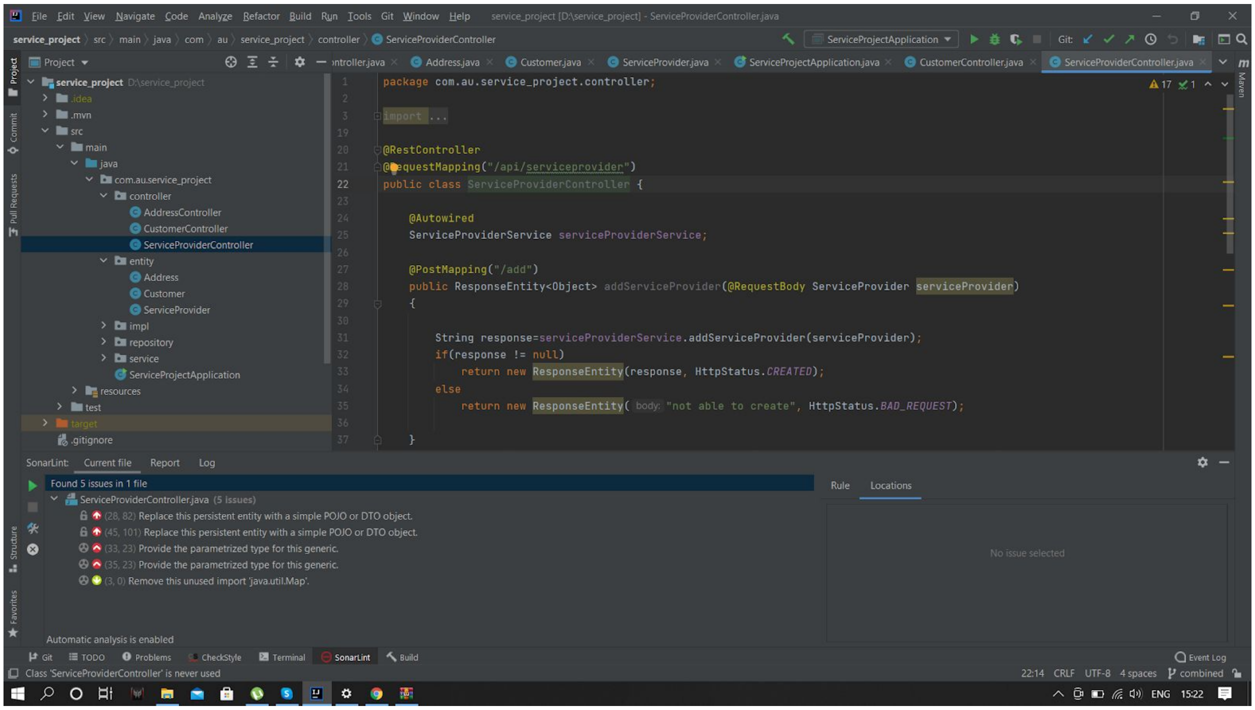
SonarLint: Current file Report Log

```
Found 4 issues in 1 file
InitialTask.java (4 issues)
    (50, 12) Replace this use of System.out or System.err by a logger.
    (0, 0) Move this file to a named package.
    (13, 18) The return type of this method should be an interface such as "Map" rather than the implementation "HashMap".
    (25, 18) Move the array designator from the variable to the type.
```

Rule Locations

Select an issue to see extended rule description

Automatic analysis is enabled


File Edit View Navigate Code Analyze Refactor Build Run Tools Git Window Help
service_project [D:\service_project] - ServiceProviderController.java
service_project › src › main › java › com › au › service_project › controller › ServiceProviderController
ServiceProjectApplication
Git:
Project
ntroller.java
Address.java
Customer.java
ServiceProvider.java
ServiceProjectApplication.java
CustomerController.java
ServiceProviderController.java
service_project D:\service_project
.idea
.mvn
src
main
java
com.au.service_project
controller
AddressController
CustomerController
ServiceProviderController
entity
Address
Customer
ServiceProvider
impl
repository
service
ServiceProjectApplication
resources
test
target
.gitignore
Git
TODO
Problems
CheckStyle
Terminal
SonarLint
Build
Event Log
22:14 CRLF UTF-8 4 spaces combined
ENG 15:22

```
package com.au.service_project.controller;

import ...

@RestController
@RequestMapping("/api/serviceprovider")
public class ServiceProviderController {

    @Autowired
    ServiceProviderService serviceProviderService;

    @PostMapping("/add")
    public ResponseEntity<Object> addServiceProvider(@RequestBody ServiceProvider serviceProvider)
    {

        String response=serviceProviderService.addServiceProvider(serviceProvider);
        if(response != null)
            return new ResponseEntity(response, HttpStatus.CREATED);
        else
            return new ResponseEntity( body: "not able to create", HttpStatus.BAD_REQUEST);

    }
```

SonarLint: Current file Report Log

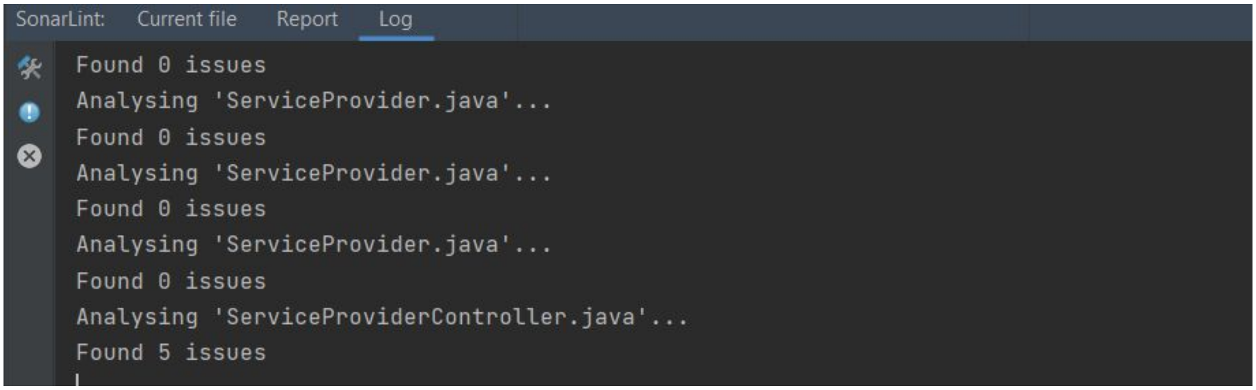
```
Found 5 issues in 1 file
ServiceProviderController.java (5 issues)
    (28, 82) Replace this persistent entity with a simple POJO or DTO object.
    (45, 101) Replace this persistent entity with a simple POJO or DTO object.
    (33, 23) Provide the parametrized type for this generic.
    (35, 23) Provide the parametrized type for this generic.
    (3, 0) Remove this unused import 'java.util.Map'.
```

Rule Locations

No issue selected

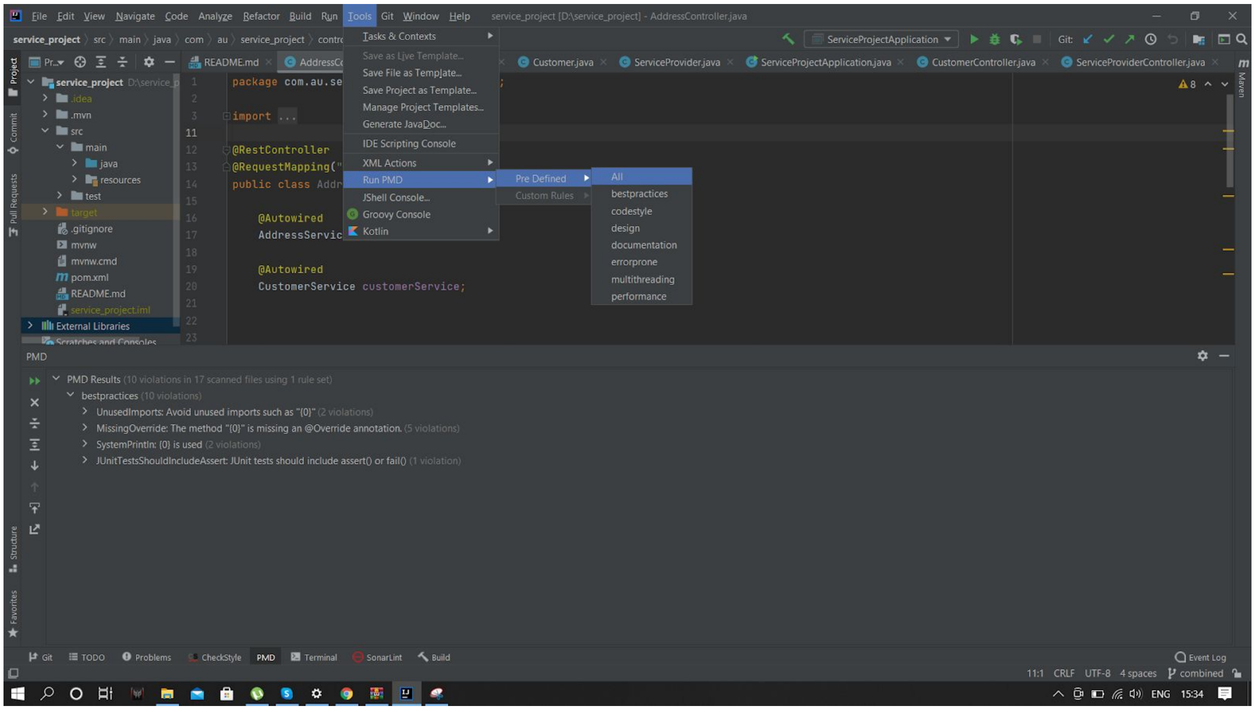
Automatic analysis is enabled

Class 'ServiceProviderController' is never used



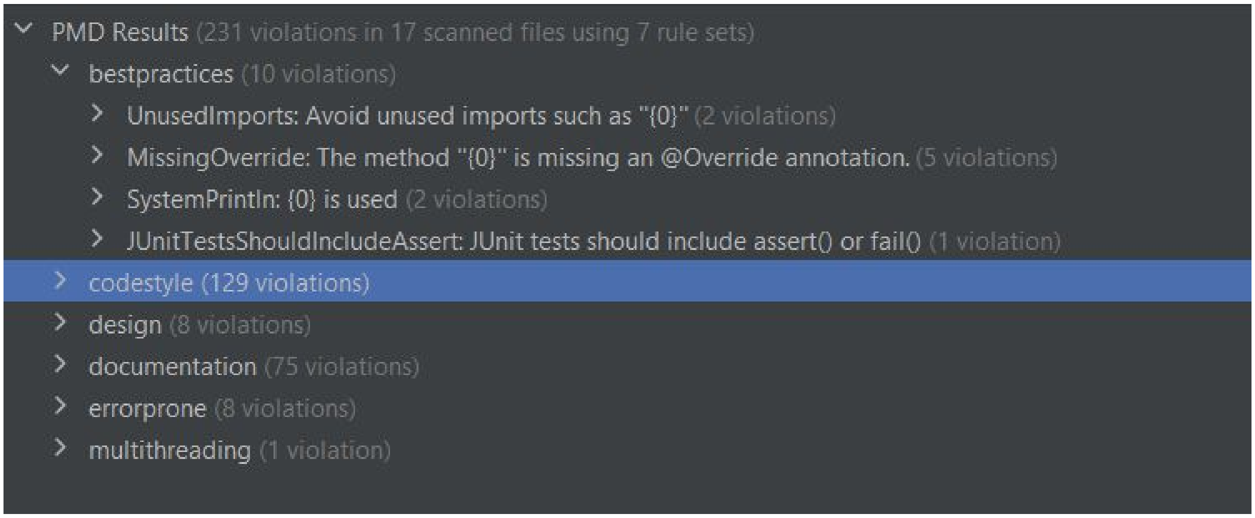
```
Found 0 issues
Analysing 'ServiceProvider.java'...
Found 0 issues
Analysing 'ServiceProvider.java'...
Found 0 issues
Analysing 'ServiceProvider.java'...
Found 0 issues
Analysing 'ServiceProviderController.java'...
Found 5 issues
```

2)PMD



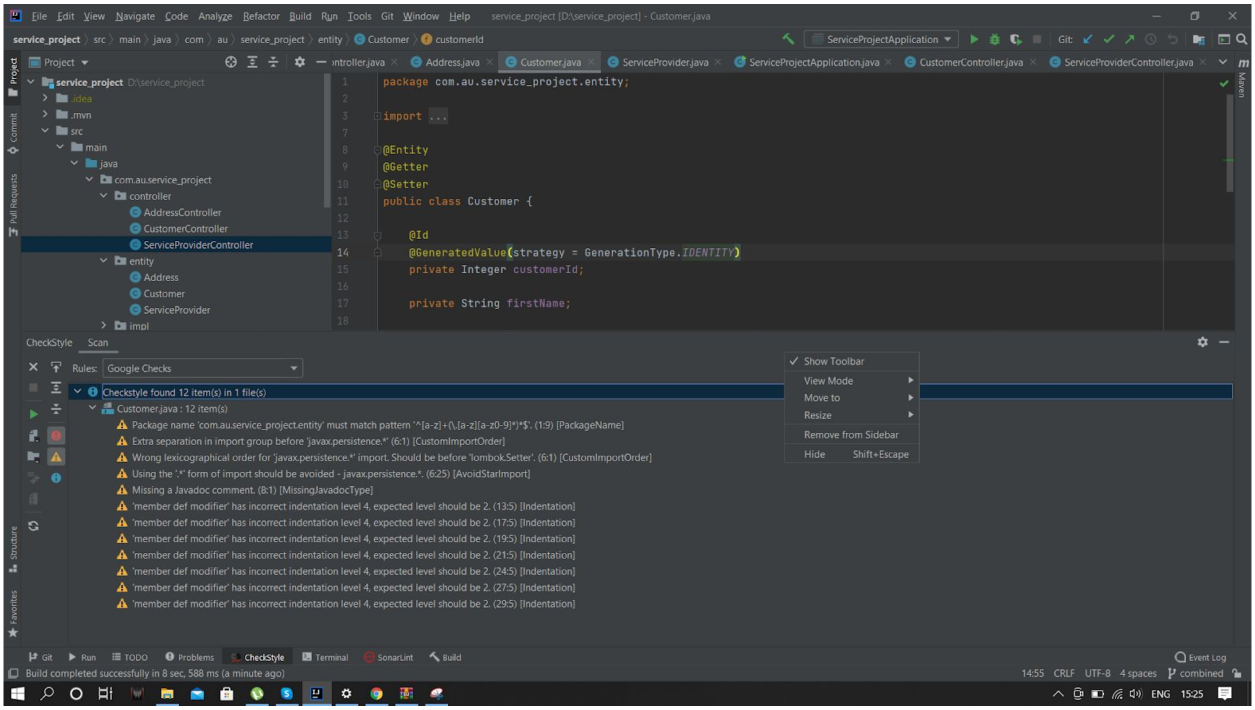
```
package com.au.se

import ...

@RestController
@RequestMapping("
public class Addr

    @Autowired
    AddressServic

    @Autowired
    CustomerService customerService;
```

PMD Results (10 violations in 17 scanned files using 1 rule set)
- bestpractices (10 violations)
  - UnusedImports: Avoid unused imports such as "{0}" (2 violations)
  - MissingOverride: The method "{0}" is missing an @Override annotation. (5 violations)
  - SystemPrintln: {0} is used (2 violations)
  - JUnitTestsShouldIncludeAssert: JUnit tests should include assert() or fail() (1 violation)



```
PMD Results (231 violations in 17 scanned files using 7 rule sets)
  bestpractices (10 violations)
    UnusedImports: Avoid unused imports such as "{0}" (2 violations)
    MissingOverride: The method "{0}" is missing an @Override annotation. (5 violations)
    SystemPrintln: {0} is used (2 violations)
    JUnitTestsShouldIncludeAssert: JUnit tests should include assert() or fail() (1 violation)
  codestyle (129 violations)
  design (8 violations)
  documentation (75 violations)
  errorprone (8 violations)
  multithreading (1 violation)
```

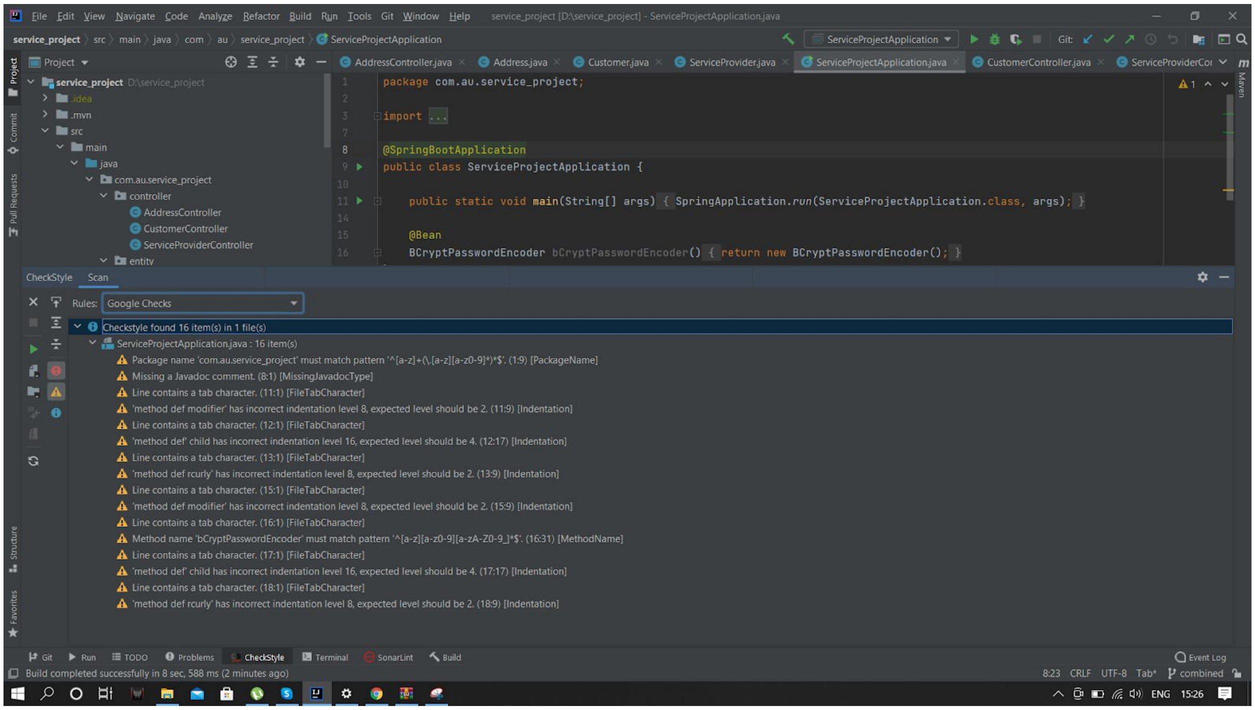
3)CheckStyle



```java
package com.au.service_project.entity;

import ...

@Entity
@Getter
@Setter
public class Customer {

    @Id
    @GeneratedValue(strategy = GenerationType.IDENTITY)
    private Integer customerId;

    private String firstName;

```

```
Checkstyle found 12 item(s) in 1 file(s)
  Customer.java : 12 item(s)
    Package name 'com.au.service_project.entity' must match pattern '^[a-z]+(\.[a-z][a-z0-9]*)*$'. (1:9) [PackageName]
    Extra separation in import group before 'javax.persistence.*' (6:1) [CustomImportOrder]
    Wrong lexicographical order for 'javax.persistence.*' import. Should be before 'lombok.Setter'. (6:1) [CustomImportOrder]
    Using the '.*' form of import should be avoided - javax.persistence.*. (6:25) [AvoidStarImport]
    Missing a Javadoc comment. (8:1) [MissingJavadocType]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (13:5) [Indentation]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (17:5) [Indentation]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (19:5) [Indentation]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (21:5) [Indentation]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (24:5) [Indentation]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (27:5) [Indentation]
    'member def modifier' has incorrect indentation level 4, expected level should be 2. (29:5) [Indentation]
```

```
Build completed successfully in 8 sec, 588 ms (a minute ago)
```



```java
package com.au.service_project;

import ...

@SpringBootApplication
public class ServiceProjectApplication {

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

    @Bean
    BCryptPasswordEncoder bCryptPasswordEncoder() { return new BCryptPasswordEncoder(); }
```

Rules: Google Checks

```
Checkstyle found 16 item(s) in 1 file(s)
  ServiceProjectApplication.java : 16 item(s)
    Package name 'com.au.service_project' must match pattern '^[a-z]+(\.[a-z][a-z0-9]*)*$'. (1:9) [PackageName]
    Missing a Javadoc comment. (8:1) [MissingJavadocType]
    Line contains a tab character. (11:1) [FileTabCharacter]
    'method def modifier' has incorrect indentation level 8, expected level should be 2. (11:9) [Indentation]
    Line contains a tab character. (12:1) [FileTabCharacter]
    'method def' child has incorrect indentation level 16, expected level should be 4. (12:17) [Indentation]
    Line contains a tab character. (13:1) [FileTabCharacter]
    'method def rcurly' has incorrect indentation level 8, expected level should be 2. (13:9) [Indentation]
    Line contains a tab character. (15:1) [FileTabCharacter]
    'method def modifier' has incorrect indentation level 8, expected level should be 2. (15:9) [Indentation]
    Line contains a tab character. (16:1) [FileTabCharacter]
    Method name 'bCryptPasswordEncoder' must match pattern '^[a-z][a-z0-9][a-zA-Z0-9_]*$'. (16:31) [MethodName]
    Line contains a tab character. (17:1) [FileTabCharacter]
    'method def' child has incorrect indentation level 16, expected level should be 4. (17:17) [Indentation]
    Line contains a tab character. (18:1) [FileTabCharacter]
    'method def rcurly' has incorrect indentation level 8, expected level should be 2. (18:9) [Indentation]
```

Build completed successfully in 8 sec, 588 ms (2 minutes ago)

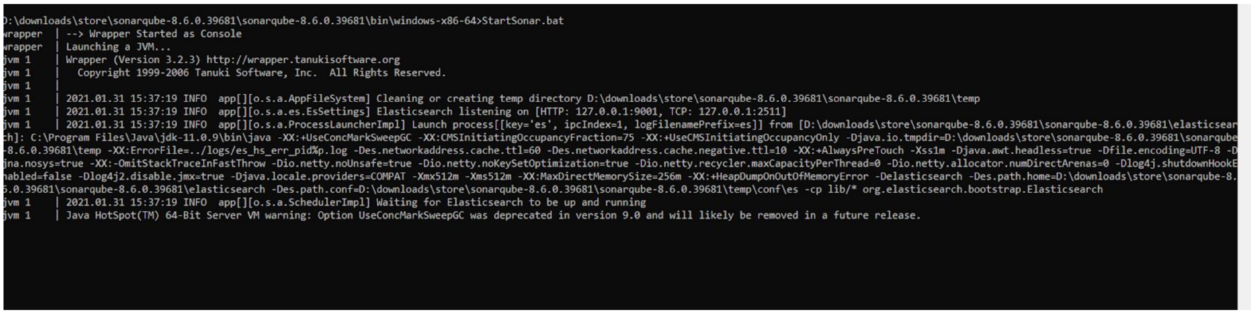
File Edit View Navigate Code Analyze Refactor Build Run Tools Git Window Help
service_project [D:\service_project] - ServiceProjectApplication.java
service_project > src > main > java > com > au > service_project > ServiceProjectApplication
ServiceProjectApplication
Git:
Project
service_project D:\service_project
.idea
.mvn
src
main
java
com.au.service_project
controller
AddressController
CustomerController
ServiceProviderController
entity
AddressController.java
Address.java
Customer.java
ServiceProvider.java
ServiceProjectApplication.java
CustomerController.java
ServiceProviderCo
CheckStyle
Scan
Git
Run
TODO
Problems
CheckStyle
Terminal
SonarLint
Build
Event Log
8:23 CRLF UTF-8 Tab* combined
ENG 15:26

B) Install the sonarqube server in your local machine and run sonarqube analysis against one of your projects.
Choose any project of your choice which has at least 4 different classes.

Document the process and add screenshot of sonarqube report.

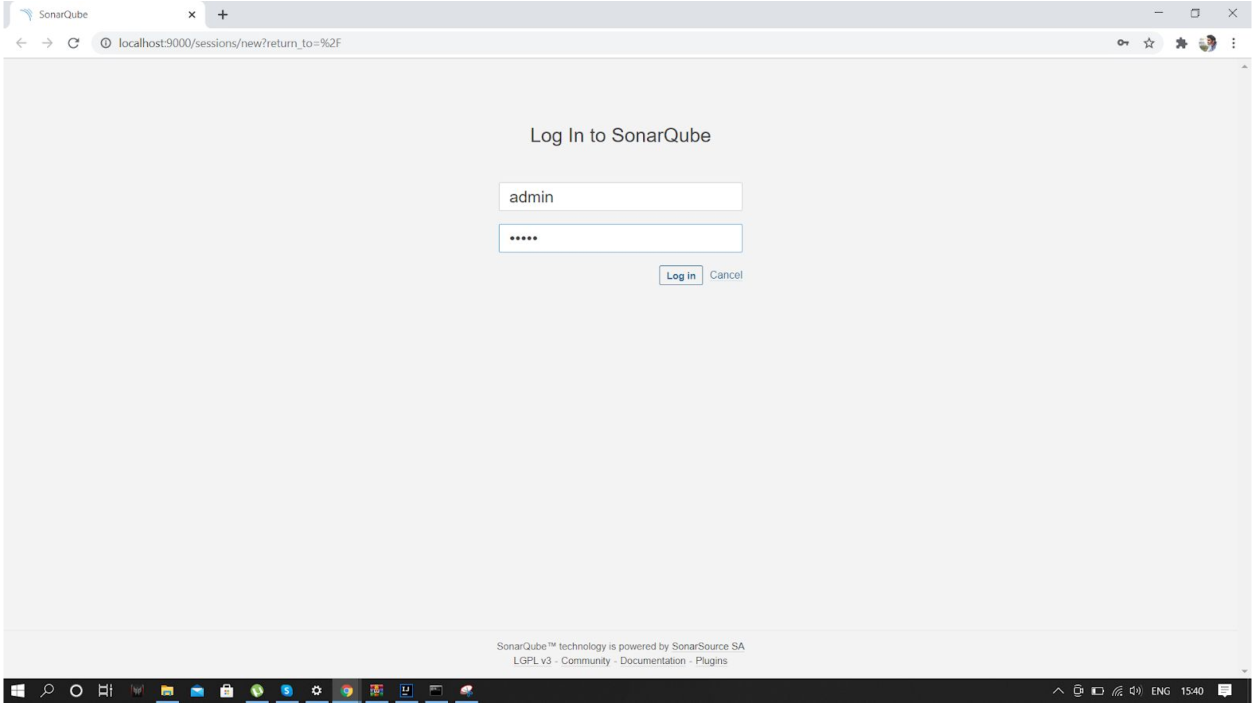
Sonarqube

Starting Sonarqube



```
D:\downloads\store\sonarqube-8.6.0.39681\sonarqube-8.6.0.39681\bin\windows-x86-64>StartSonar.bat
wrapper  | --> Wrapper Started as Console
wrapper  | Launching a JVM...
jvm 1    | Wrapper (Version 3.2.3) http://wrapper.tanukisoftware.org
jvm 1    |   Copyright 1999-2006 Tanuki Software, Inc.  All Rights Reserved.
jvm 1    |
jvm 1    | 2021.01.31 15:37:19 INFO  app[][o.s.a.AppFileSystem] Cleaning or creating temp directory D:\downloads\store\sonarqube-8.6.0.39681\sonarqube-8.6.0.39681\temp
jvm 1    | 2021.01.31 15:37:19 INFO  app[][o.s.a.es.EsSettings] Elasticsearch listening on [HTTP: 127.0.0.1:9001, TCP: 127.0.0.1:2511]
jvm 1    | 2021.01.31 15:37:19 INFO  app[][o.s.a.ProcessLauncherImpl] Launch process[[key='es', ipcIndex=1, logFilenamePrefix=es]] from [D:\downloads\store\sonarqube-8.6.0.39681\sonarqube-8.6.0.39681\elasticsear
ch]: C:\Program Files\Java\jdk-11.0.9\bin\java -XX:+UseConcMarkSweepGC -XX:CMSInitiatingOccupancyFraction=75 -XX:+UseCMSInitiatingOccupancyOnly -Djava.io.tmpdir=D:\downloads\store\sonarqube-8.6.0.39681\sonarqube
-8.6.0.39681\temp -XX:ErrorFile=../logs/es_hs_err_pid%p.log -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=true -Dfile.encoding=UTF-8 -D
jna.nosys=true -XX:-OmitStackTraceInFastThrow -Dio.netty.noUnsafe=true -Dio.netty.noKeySetOptimization=true -Dio.netty.recycler.maxCapacityPerThread=0 -Dio.netty.allocator.numDirectArenas=0 -Dlog4j.shutdownHookE
nabled=false -Dlog4j2.disable.jmx=true -Djava.locale.providers=COMPAT -Xmx512m -Xms512m -XX:MaxDirectMemorySize=256m -XX:+HeapDumpOnOutOfMemoryError -Delasticsearch -Des.path.home=D:\downloads\store\sonarqube-8.
6.0.39681\sonarqube-8.6.0.39681\elasticsearch -Des.path.conf=D:\downloads\store\sonarqube-8.6.0.39681\sonarqube-8.6.0.39681\temp\conf\es -cp lib/* org.elasticsearch.bootstrap.Elasticsearch
jvm 1    | 2021.01.31 15:37:19 INFO  app[][o.s.a.SchedulerImpl] Waiting for Elasticsearch to be up and running
jvm 1    | Java HotSpot(TM) 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in a future release.
```

Logging In



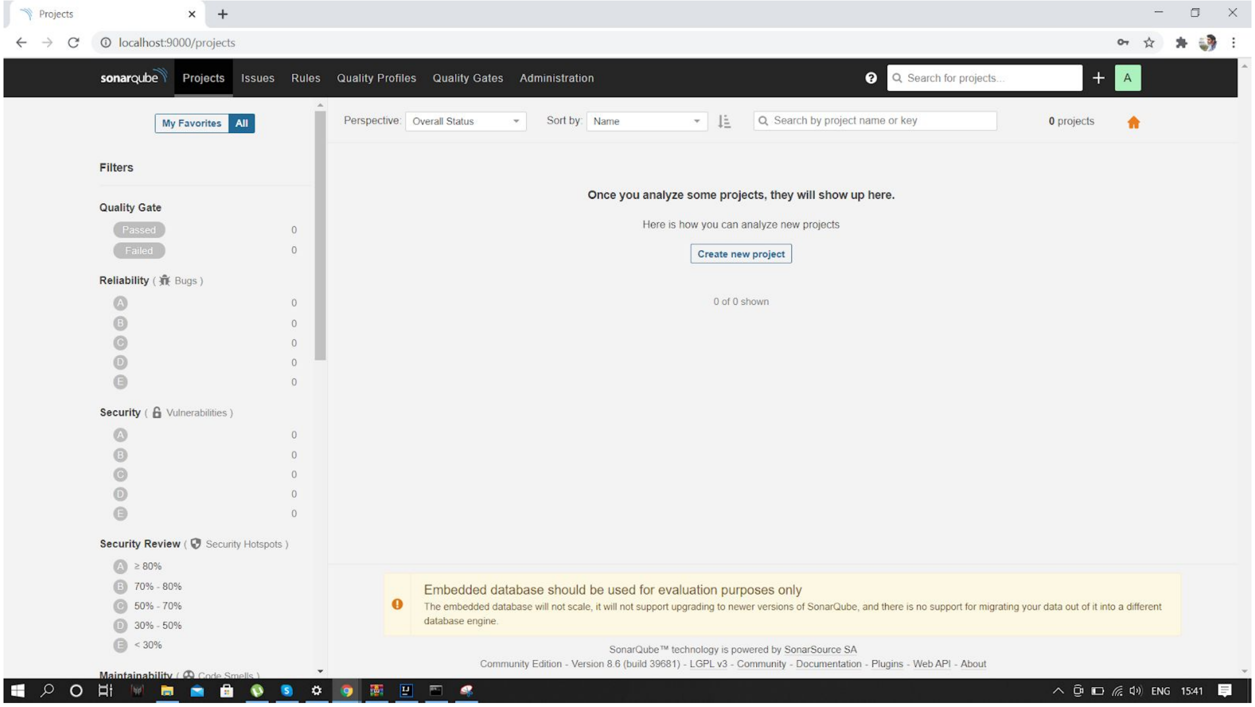
localhost:9000/sessions/new?return_to=%2F

Log In to SonarQube

admin

•••••

SonarQube™ technology is powered by SonarSource SA
LGPL v3 - Community - Documentation - Plugins



localhost:9000/projects

Perspective: Overall Status

Sort by: Name

0 projects

Once you analyze some projects, they will show up here.

Here is how you can analyze new projects

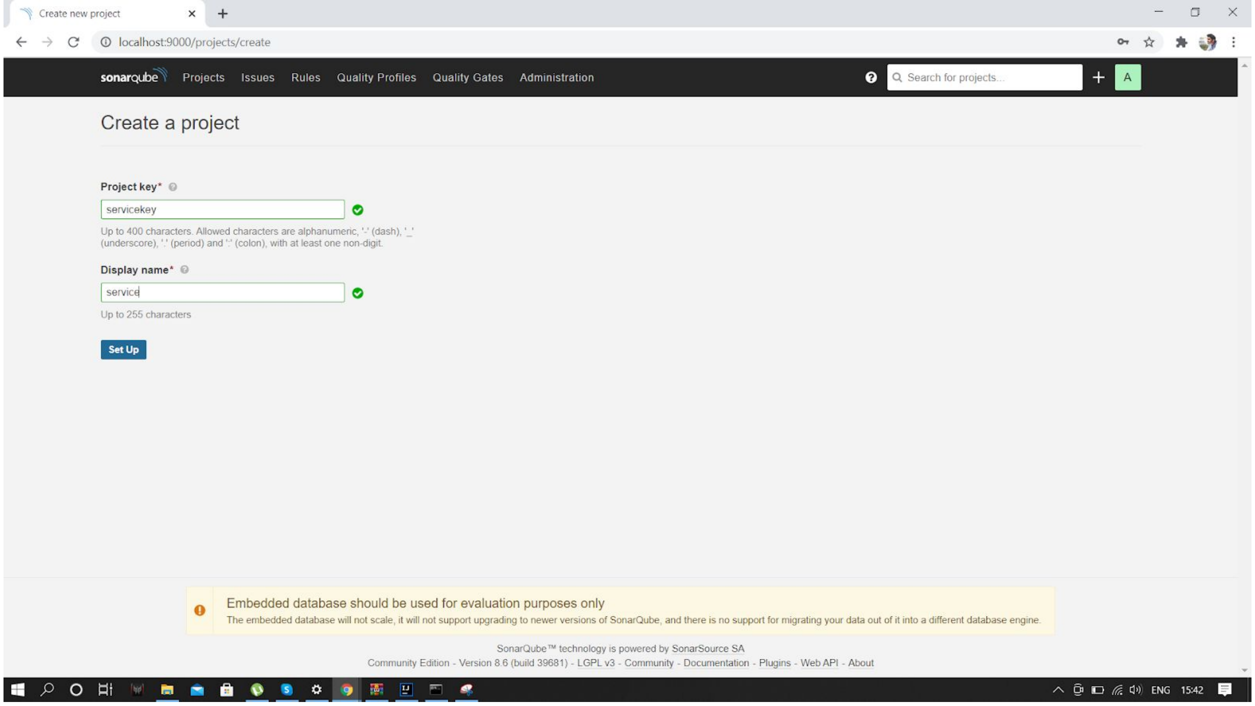
0 of 0 shown

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 (build 39681) - LGPL v3 - Community - Documentation - Plugins - Web API - About

Creating Project



Create a project

Project key*

servicekey

Up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '_' (underscore), '.' (period) and ':' (colon), with at least one non-digit.

Display name*

service

Up to 255 characters

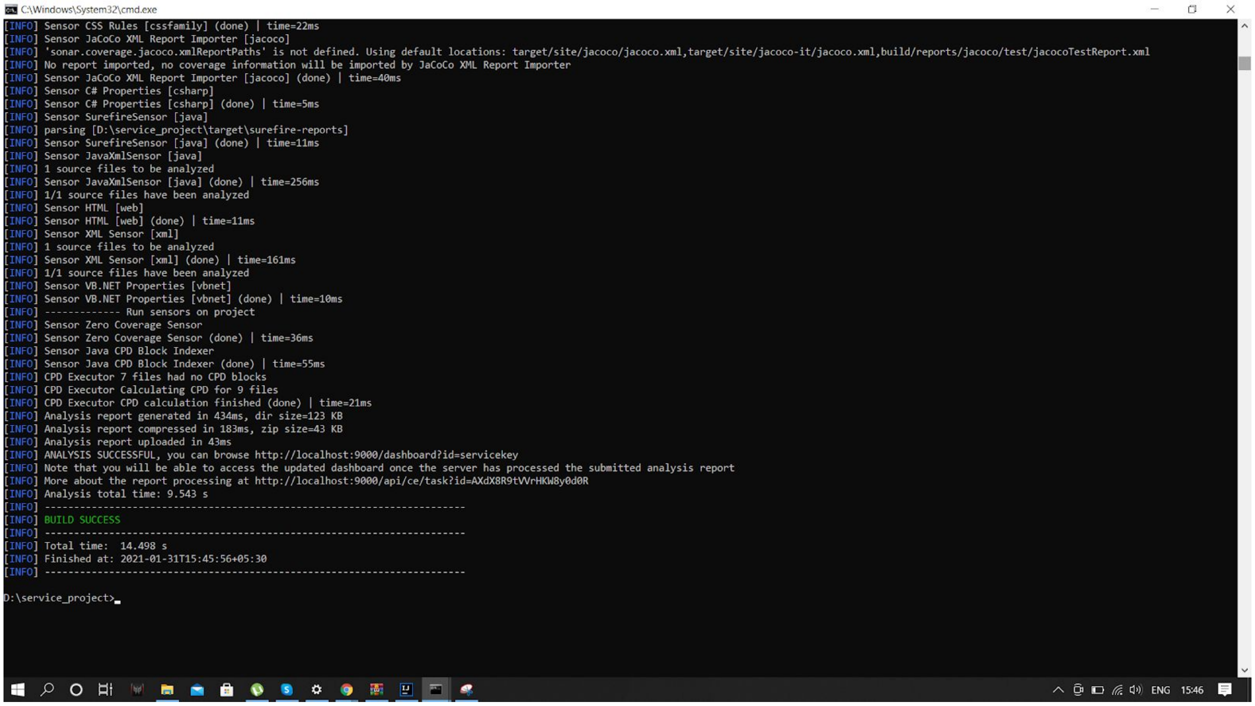
Embedded database should be used for evaluation purposes only

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

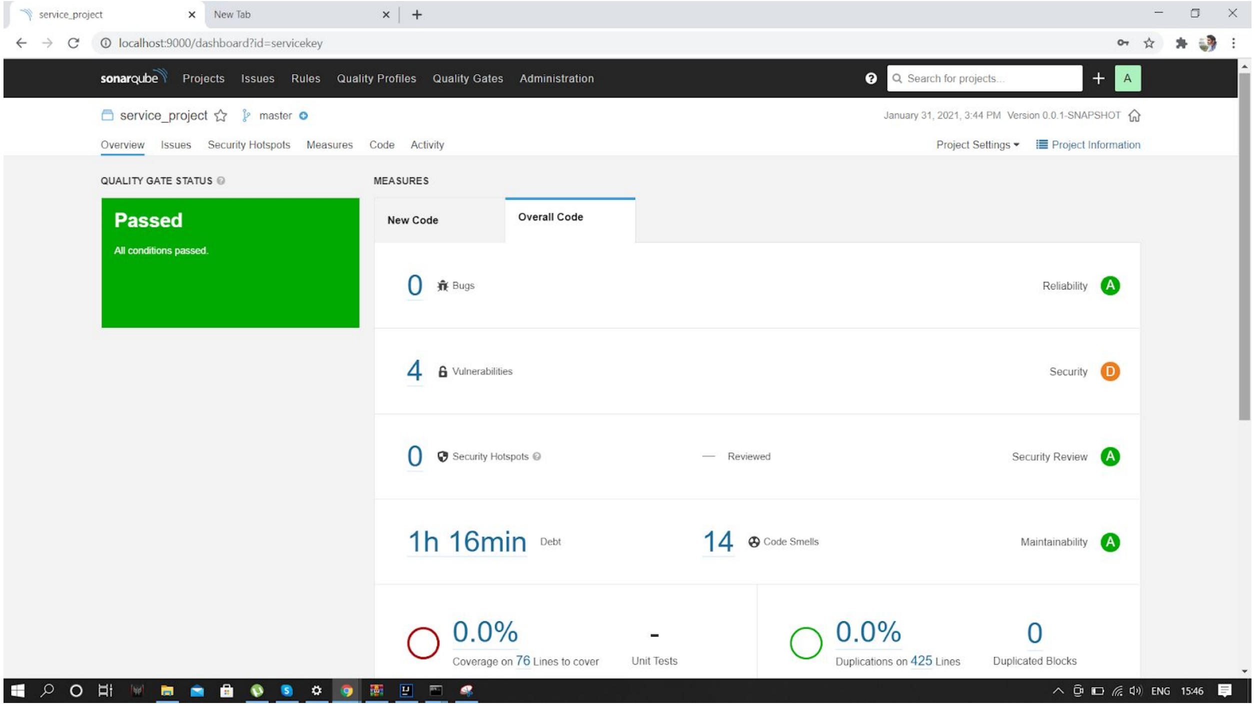
Community Edition - Version 8.6 (build 39681) - LGPL v3 - Community - Documentation - Plugins - Web API - About

Scanning the project



```
[INFO] Sensor CSS Rules [cssfamily] (done) | time=22ms
[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=40ms
[INFO] Sensor C# Properties [csharp]
[INFO] Sensor C# Properties [csharp] (done) | time=5ms
[INFO] Sensor SurefireSensor [java]
[INFO] parsing [D:\service_project\target\surefire-reports]
[INFO] Sensor SurefireSensor [java] (done) | time=11ms
[INFO] Sensor JavaXmlSensor [java]
[INFO] 1 source files to be analyzed
[INFO] Sensor JavaXmlSensor [java] (done) | time=256ms
[INFO] 1/1 source files have been analyzed
[INFO] Sensor HTML [web]
[INFO] Sensor HTML [web] (done) | time=11ms
[INFO] Sensor XML Sensor [xml]
[INFO] 1 source files to be analyzed
[INFO] Sensor XML Sensor [xml] (done) | time=161ms
[INFO] 1/1 source files have been analyzed
[INFO] Sensor VB.NET Properties [vbnet]
[INFO] Sensor VB.NET Properties [vbnet] (done) | time=10ms
[INFO] ------------- Run sensors on project
[INFO] Sensor Zero Coverage Sensor
[INFO] Sensor Zero Coverage Sensor (done) | time=36ms
[INFO] Sensor Java CPD Block Indexer
[INFO] Sensor Java CPD Block Indexer (done) | time=55ms
[INFO] CPD Executor 7 files had no CPD blocks
[INFO] CPD Executor Calculating CPD for 9 files
[INFO] CPD Executor CPD calculation finished (done) | time=21ms
[INFO] Analysis report generated in 434ms, dir size=123 KB
[INFO] Analysis report compressed in 183ms, zip size=43 KB
[INFO] Analysis report uploaded in 43ms
[INFO] ANALYSIS SUCCESSFUL, you can browse http://localhost:9000/dashboard?id=servicekey
[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=AXdX8R9tVVrHKW8y0d0R
[INFO] Analysis total time: 9.543 s
[INFO] ------------------------------------------------------------------------
[INFO] BUILD SUCCESS
[INFO] ------------------------------------------------------------------------
[INFO] Total time:  14.498 s
[INFO] Finished at: 2021-01-31T15:45:56+05:30
[INFO] ------------------------------------------------------------------------

D:\service_project>
```

Results



January 31, 2021, 3:44 PM Version 0.0.1-SNAPSHOT

QUALITY GATE STATUS

Passed

All conditions passed.

MEASURES

0 Bugs — Reliability A

4 Vulnerabilities — Security D

0 Security Hotspots — Reviewed — Security Review A

1h 16min Debt — 14 Code Smells — Maintainability A

0.0% Coverage on 76 Lines to cover — - Unit Tests

0.0% Duplications on 425 Lines — 0 Duplicated Blocks

CWE and SANS 25

Common Weakness Enumeration (CWE) is a community-developed list of common software and hardware weakness types that have security ramifications.
“Weaknesses” are flaws, faults, bugs, vulnerabilities, or other errors in software or hardware implementation, code, design, or architecture that if left unaddressed could result in systems, networks, or hardware being vulnerable to attack.
The CWE List and associated classification taxonomy serve as a language that can be used to identify and describe these weaknesses in terms of CWEs.

CWE helps developers and security practitioners to:

- Describe and discuss software and hardware weaknesses in a common language.
- Check for weaknesses in existing software and hardware products.
- Evaluate coverage of tools targeting these weaknesses.
- Leverage a common baseline standard for weakness identification, mitigation, and prevention efforts.
- Prevent software and hardware vulnerabilities prior to deployment.

There list 25 Most Dangerous Software Weaknesses (SANS 25)

Here are ten of them

[1]	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	46.82
[2]	CWE-787	Out-of-bounds Write	46.17
[3]	CWE-20	Improper Input Validation	33.47
[4]	CWE-125	Out-of-bounds Read	26.50
[5]	CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	23.73
[6]	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20.69

[7]	CWE-200	Exposure of Sensitive Information to an Unauthorized Actor	19.16
[8]	CWE-416	Use After Free	18.87
[9]	CWE-352	Cross-Site Request Forgery (CSRF)	17.29
[10]	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16.44

OWASP Top 10

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

- Injection.
- Broken authentication.
- Sensitive data exposure.
- XML external entities (XXE)
- Broken access control.
- Security misconfigurations.
- Cross-site scripting (XSS)
- Insecure deserialization.
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

CERT

CERT is a secure coding standard maintained by the Software Engineering Institute at Carnegie Mellon University. It supports commonly used programming languages such as C, C++, and Java.

CERT Risk Assessment For each guideline included in the secure coding standard, there is a risk assessment to help determine the possible consequences of violating that specific rule or recommendation. There are three sections to the risk assessment: Severity, Likelihood, and Remediation Cost. Each section is assigned a value between 1 and 3, and based upon the results of the assessment, you are able to determine the priority of the violation.

Severity — How serious are the consequences of the rule being ignored.

Likelihood — How likely is the coding flaw introduced by violating the rule can lead to an exploitable vulnerability?

Remediation Cost — How expensive will it be to comply with the rule.

Each of these three values— Severity, Likelihood, and Remediation Cost — are then multiplied together to determine priority, which is a measure of the risk, and therefore the level of the vulnerability. This can be used to prioritize the repair of violations.