agilelab

Code Quality and Analysis Tool

sonarqube

2023, March 31

Giovanni Brunetti

agilelab

sonarqube

What is SonarQube? What is it for?

- It is an open-source tool developed by SonarSource for continuous inspection of code quality, performing automatic detection of static analysis of code to detect bugs, code smells, and security vulnerabilities on 25+ programming languages.

- SonarQube offers reports on duplicated code, coding standards, unit tests, code coverage, code complexity, comments, bugs, and security vulnerabilities.

agilelab

sonarqube

How it works

SonarQube uses several code analysis techniques to identify potential problems in the source code, including:

- Analysis of code quality metrics and indicators, such as cyclomatic complexity, code duplication, and test coverage.
- Analysis of coding rules and best practices, such as error handling, proper use of libraries, security and code optimization.
- Code security analysis, looking for vulnerabilities and potential security issues.

agilelab

sonarqube

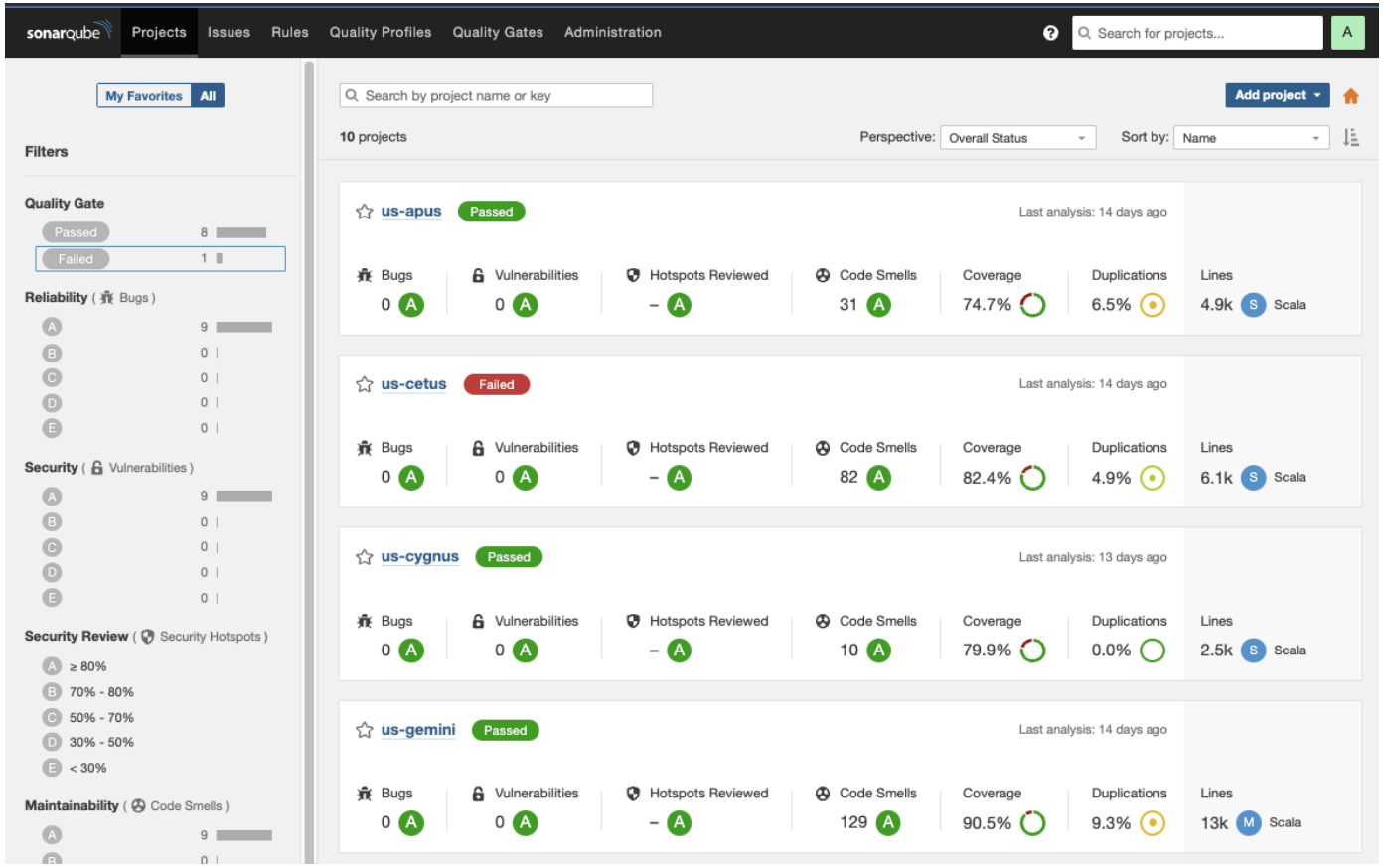
Metrics and Key Features

- **Code coverage**: indicates the percentage of code that is executed during testing. A 100% coverage indicates that all lines of code have been executed at least once during testing.
- **Cyclomatic complexity**: indicates the complexity of the program's control flow. High cyclomatic complexity values indicate that the code may be difficult to understand, test, and maintain.
- **Number of vulnerabilities**: indicates the number of potential code vulnerabilities identified during code security analysis.
- **Code duplication**: indicates the percentage of duplicated code in the project. The presence of duplicated code can make the code more difficult to maintain and can lead to consistency issues.
- **Technical debt**: indicates the cost of fixing the code over time. High technical debt indicates that the code will require more time and resources to fix in the future.
- **Number of code smells**: indicates the number of violations of coding best practices that could lead to maintainability and readability issues.
- **Quality Gate:** allows you to define acceptability rules and metrics for your code, If the code does not meet all defined criteria, the Quality Gate fails and the code analysis is considered unacceptable.
- And others…

agilelab

sonarqube

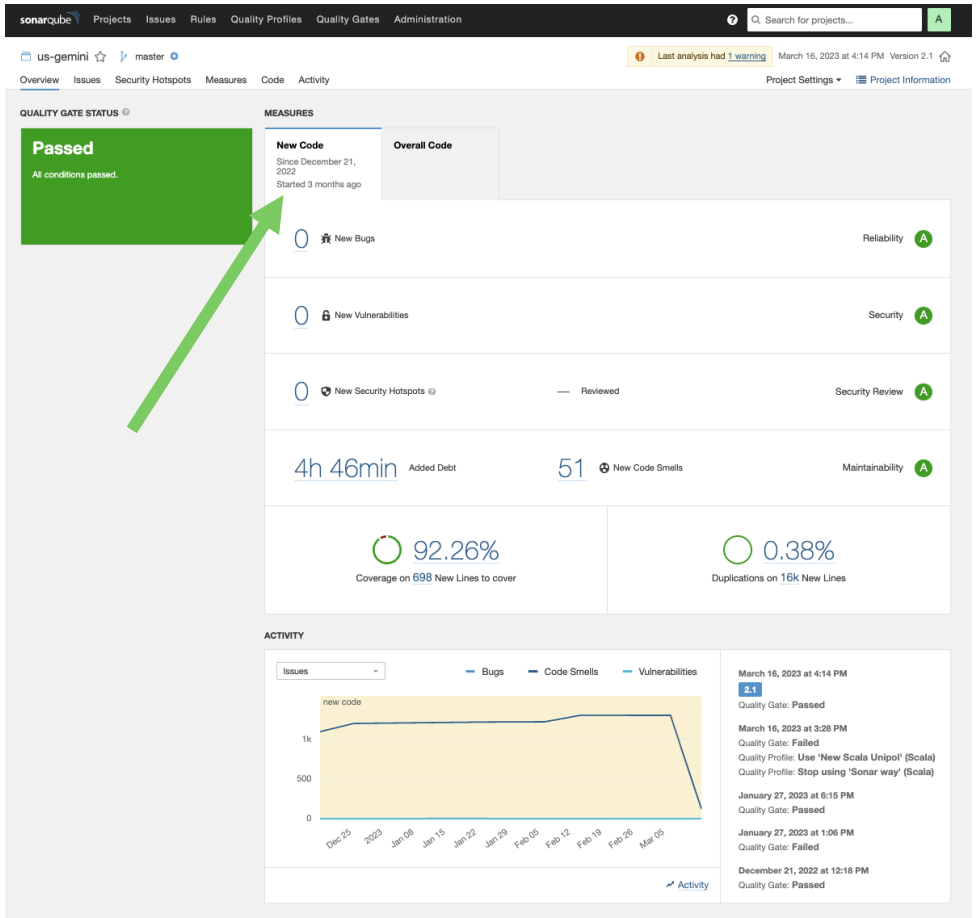
Sonar Dashboard - General

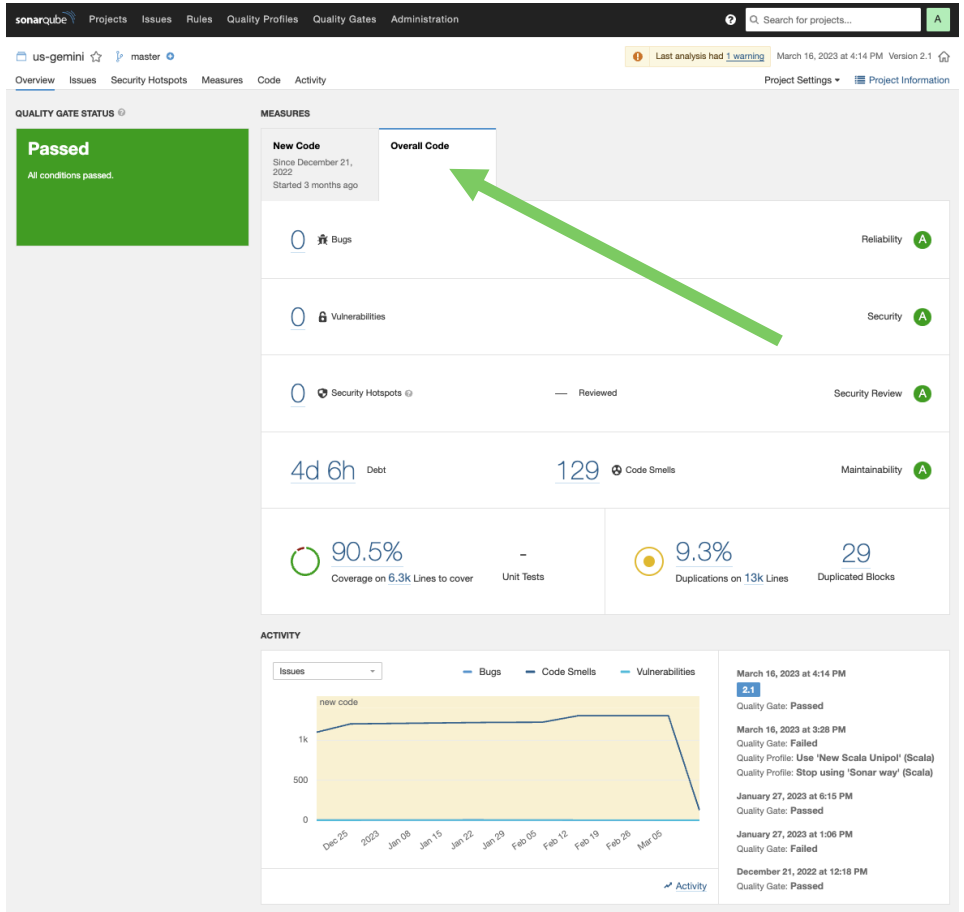


agilelab

sonarqube

Sonar Dashboard – Overview Project





agilelab

sonarqube

Sonar Dashboard – Overview Project

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

Search for projects...

us-gemini master

Last analysis had 1 warning March 16, 2023 at 4:14 PM Version 2.1

Overview Issues Security Hotspots Measures Code Activity

Project Settings Project Information

My Issues All

Bulk Change to select issues to navigate 1 / 129 issues 4d 6h effort

Filters

Type
- Bug 0
- Vulnerability 0
- Code Smell 129

Severity
- Blocker 0
- Critical 15
- Major 45
- Minor 8
- Info 61

Scope
Resolution
Status
Security Category
Creation Date
Language
Rule
Tag
Directory
File
Assignee
Author

src/.../unipolsai/gemini/application/MockJob.scala

Add a nested comment explaining why this function is empty or complete the implementation. Why is this an issue? 8 months ago L42
Code Smell Critical Open Not assigned 5min effort Comment suspicious

src/.../unipolsai/gemini/application/ReadIngestionJob.scala

Add a nested comment explaining why this function is empty or complete the implementation. Why is this an issue? 8 months ago L73
Code Smell Critical Open Not assigned 5min effort Comment suspicious

src/.../unipolsai/gemini/application/ReadRingFenceJob.scala

Add a nested comment explaining why this function is empty or complete the implementation. Why is this an issue? 8 months ago L95
Code Smell Critical Open Not assigned 5min effort Comment suspicious

src/.../unipolsai/gemini/application/SparkJob.scala

Complete the task associated to this TODO comment. Why is this an issue? 8 months ago L15
Code Smell Info Open Not assigned Comment cwe

Complete the task associated to this TODO comment. Why is this an issue? 8 months ago L57
Code Smell Info Open Not assigned Comment cwe

src/.../unipolsai/gemini/application/SparkReadJob.scala

Complete the task associated to this TODO comment. Why is this an issue? 4 months ago L16
Code Smell Info Open Not assigned Comment cwe

Complete the task associated to this TODO comment. Why is this an issue? 4 months ago L75
Code Smell Info Open Not assigned Comment cwe

Complete the task associated to this TODO comment. Why is this an issue? 4 months ago L76
Code Smell Info Open Not assigned Comment cwe

src/.../unipolsai/gemini/application/UsGeminiClientStatus.scala

Complete the task associated to this TODO comment. Why is this an issue? 21 days ago L115
Code Smell Info Open Not assigned Comment cwe

Define a constant instead of duplicating this literal "PIVA.partita_iva" 3 times. Why is this an issue? 14 days ago L124
Code Smell Critical Open Not assigned 6min effort Comment design

agilelab

sonarqube

Sonar Dashboard – Overview Project

Maintainability

Overview	
On new code	
Code Smells	51
Debt	4h 46min
Debt Ratio	0.4%
Rating	A
Overall	
Code Smells	129
Debt	4d 6h
Debt Ratio	0.6%
Rating	A
Effort to Reach A	0

Duplications

Overview	
On new code	
Density	0.4%
Duplicated Lines	61
Duplicated Blocks	3
Overall	
Density	9.3%
Duplicated Lines	1,636
Duplicated Blocks	29
Duplicated Files	19

Complexity

Cyclomatic Complexity	1,029
Cognitive Complexity	327

Coverage

Overview	
On new code	
Coverage	92.3%
Lines to Cover	698
Uncovered Lines	54
Line Coverage	92.3%
Conditions to Cover	0
Uncovered Conditions	0
Overall	
Coverage	90.5%
Lines to Cover	6,344
Uncovered Lines	605
Line Coverage	90.5%

Size

New Lines	16,088
Lines of Code	12,842
Lines	17,559
Statements	1,827
Functions	627
Classes	181
Files	267
Comment Lines	2,881
Comments (%)	18.3%

Issues

New Issues	51
Issues	129
Open Issues	129
Reopened Issues	0
Confirmed Issues	0
False Positive Issues	0
Won't Fix Issues	0

agilelab

sonarqube

How use it locally

To use SonarQube in a local environment you can use simply use docker.

Once Docker has been installed, you can download and launch a local version of Sonarquube through the command:

docker run –d –p 9000:9000 sonarqube

With this command the SonarQube image will be automatically downloaded and run. The web interface will be available at **localhost:9000** with default credentials **admin/admin**

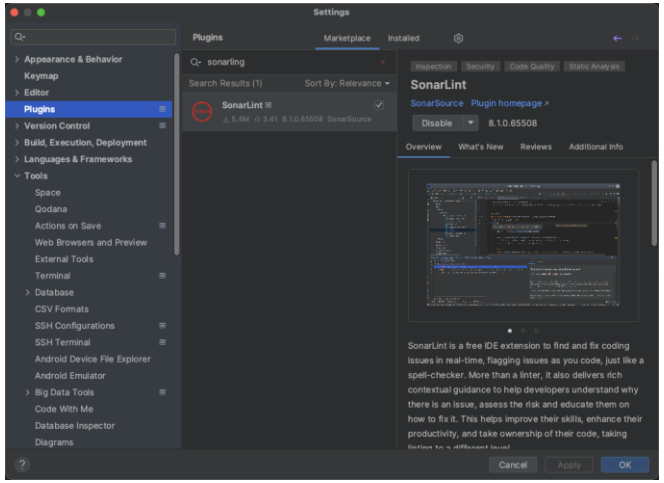
IMPORTANT: Actually official image of SonarQube is not supported by new silicon processor by Apple. You can run run this command instead of previous one:

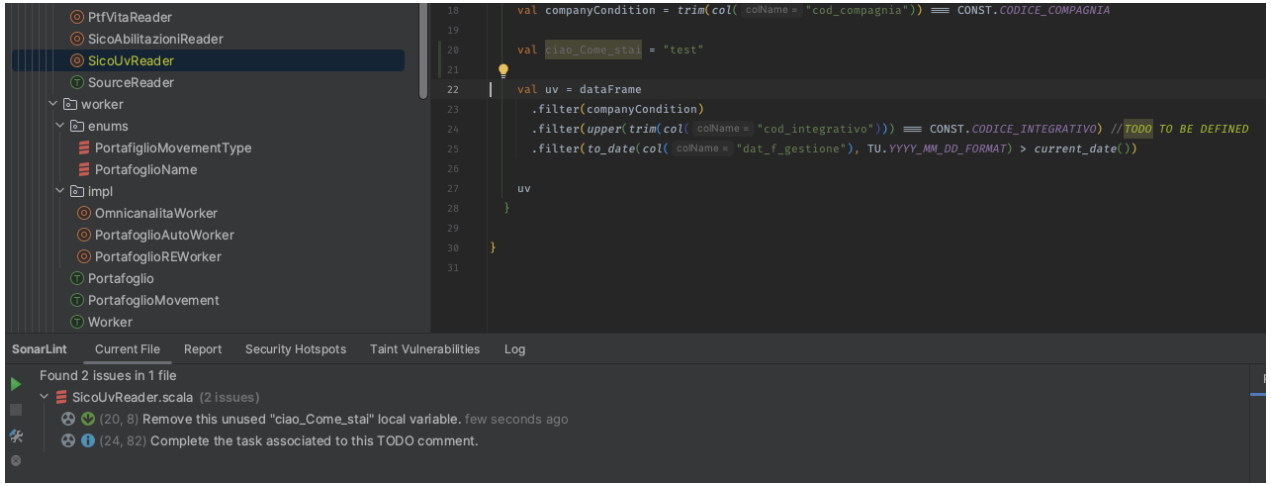
docker run –d –p 9000:9000 mwizner/sonarqube:8.7.1-community

How use it in IDE

To use Sonar in your project you can use the plugin SonarLint:

- SonarLint is a free IDE plugin which helps developer to fix known bugs and vulnerabilities, follow coding standards & best practices: Plugin Page.
- Provides clear guidance on fixing the code issues before you commit to the source code.
- Project is analysed using SonarQube server and retrieves the appropriate settings and quality profile for your projects.





How to use in Maven Project (Scala)

To use Sonar in maven projects you need to:

- Add Scoverage plugin in your pom:

```
<plugin>
    <groupId>org.scoverage</groupId>
    <artifactId>scoverage-maven-plugin</artifactId>
    <version>${scoverage.plugin.version}</version>
</plugin>
```

- Create an xml report:

```
mvn clean scoverage:report -f pom.xml
```

- Launch sonar analysis:

```
mvn sonar:sonar \
  -Dsonar.projectKey=$project \
  -Dsonar.sources=src/main/scala \
  -Dsonar.tests=src/test/scala \
  -Dsonar.host.url=http://localhost:$port \
  -Dsonar.login=$key \
  -Dsonar.scala.coverage.reportPaths="target/scoverage.xml"
```

- A complete script to execute Sonar analysis is available here: SonarQube Script

agilelab

sonarqube

How to use in Jenkins (Scala)

To use Sonar in Jenkins pipeline you need to:

- Install sonar plugin
- Install scoverage plugin
- Install cobertura plugin

agilelab

sonarqube

To Know…

- Quality Profile Setup
- Quality Gate Setup
- Fail SonarQube Projects with Quality Gate Rules criteria.
- User and Groups
- Token creation, password change, email notifications
- Integration with Jenkins

agilelab

sonarqube

Conclusion

- SonarQube performs static analysis of the code to evaluate the quality of it in terms of maintenance, reliability, efficiency and safety. The analysis of the quality code instead is performed in real time and it provides detailed feedback on the code, suggestions to improve it and report on the progress of the project.

- SonarQube is an excellent resource for development teams, as it helps to improve the software development process, identify code problems and to provide useful feedback to improve the quality of the code.