ADITYA COLLEGE OF ENGINEERING & TECHNOLOGY

Exp-5

Static Code Analyzer

By
B Manikyala Rao M.Tech(Ph.d)
Assistant Professor
Dept of Computer Science & Engineering
Aditya College of Engineering & Technology
Surampalem

Sonarqube

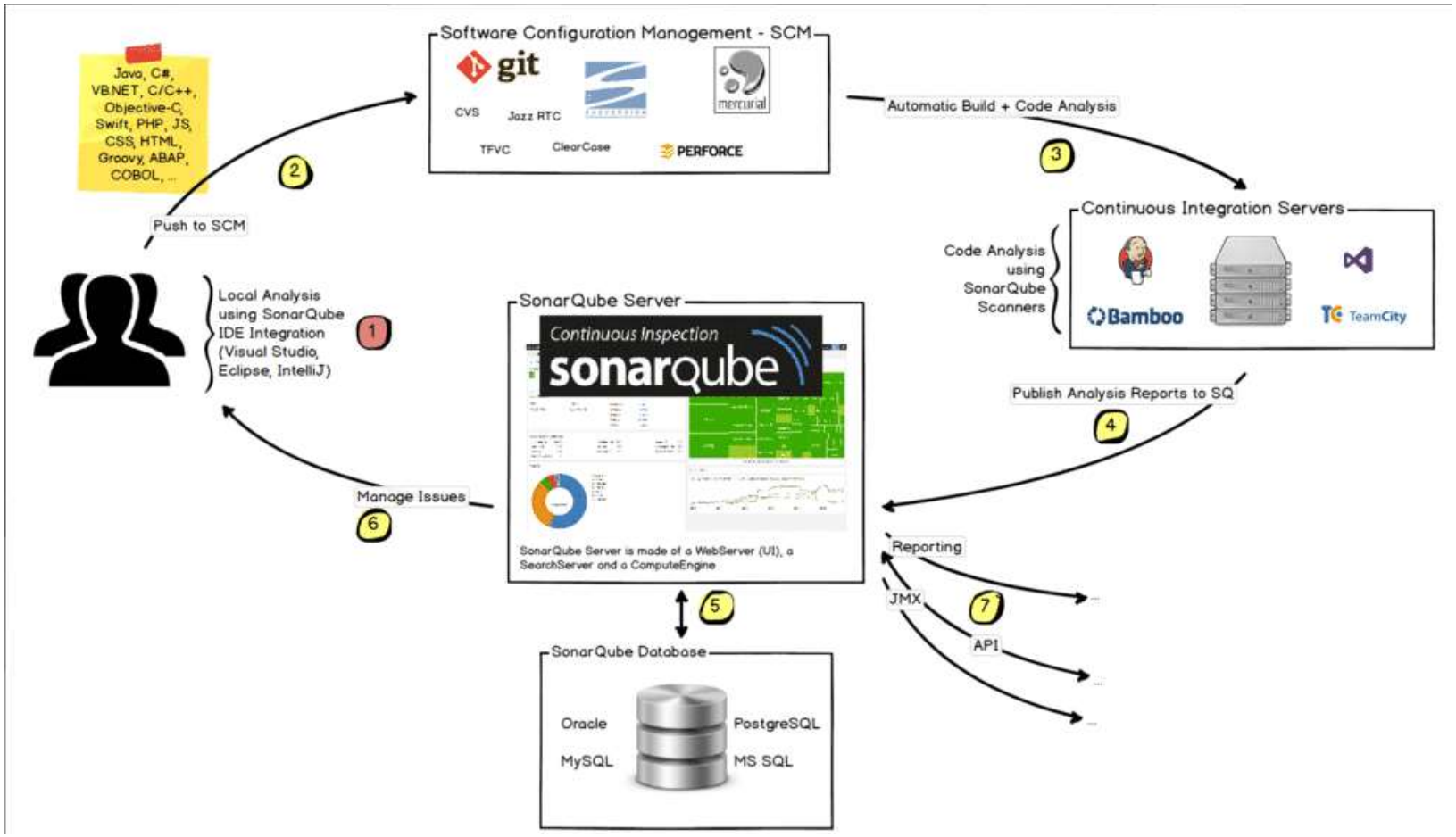
What is Static Code Analysis?

Computer code that is performed **without** actually **executing** programs. Source code will be checked for compliance with a predefined set of rules or best practices set by the organization.

What is SonarQube?

- Sonar is an **open-source software quality platform**. SonarQube saves the calculated measures in a database and showcases them in a rich web-based dashboard. Provides trends and leading indicators.

SonarQube CI



SonarQube Features

- **Supports languages:** Java, C/C++, Objective-C, C#, PHP, Flex, Groovy, JavaScript, Python, PL/SQL, COBOL, etc. (note that some of them are commercial)
- Can also be used in Android development.
- Offers reports on duplicated code, coding standards, unit tests, code coverage, code complexity, potential bugs, comments, design, and architecture.
- Records metrics history and provides evolution graphs (“time machine”) and differential views.
- Provides fully automated analyses: integrates with Maven, Ant, Gradle, and continuous integration tools (Atlassian Bamboo, Jenkins, Hudson, etc.).
- Integrates with the Eclipse development environment
- Integrates with external tools: JIRA, Mantis, LDAP, Fortify, etc.
- Is expandable with the use of plugins.

Sonarqube

Technical debt is caused by the 7 deadly sins of the developer:

- **Duplications:** SonarQube has a **copy/paste** detection engine to find duplications
- **Bad distribution of complexity**: ***Cyclomatic complexity***
- **Spaghetti Design:Bad naming, Lack of patterns, Over abstraction**
- **Lack of unit tests**
- **No coding standards**
- **Potential bugs**
- **Not enough or too many comments or incorrect comments**

SonarQube Installation on Docker

1.The first thing is to pull a docker image from using SonarQube's community edition docker image. Pull the docker image in your local machine by running this command:

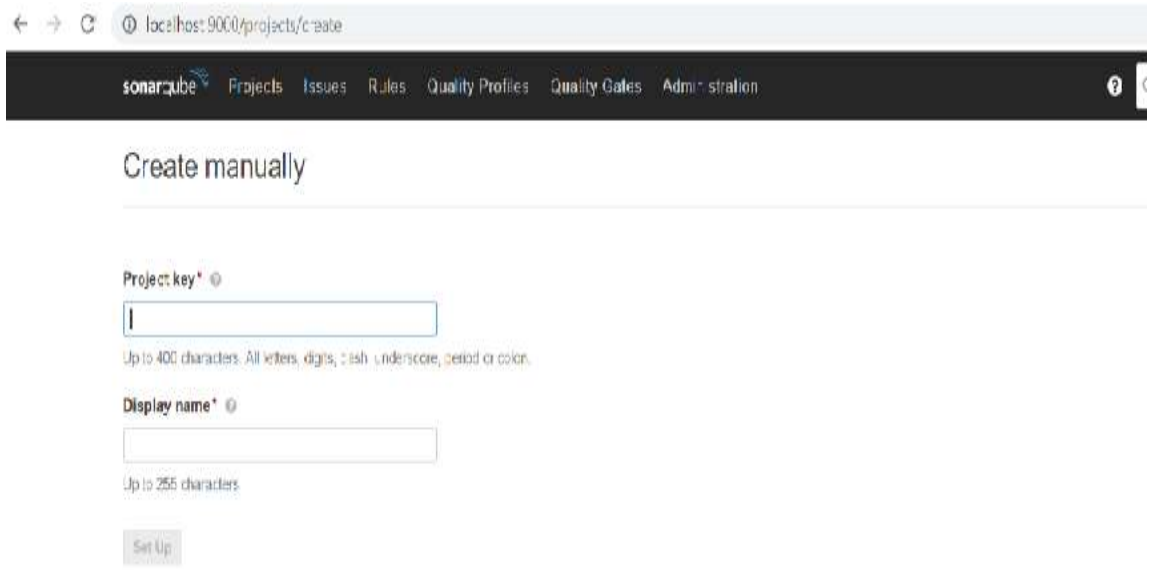
docker pull sonarqube:8.2-community

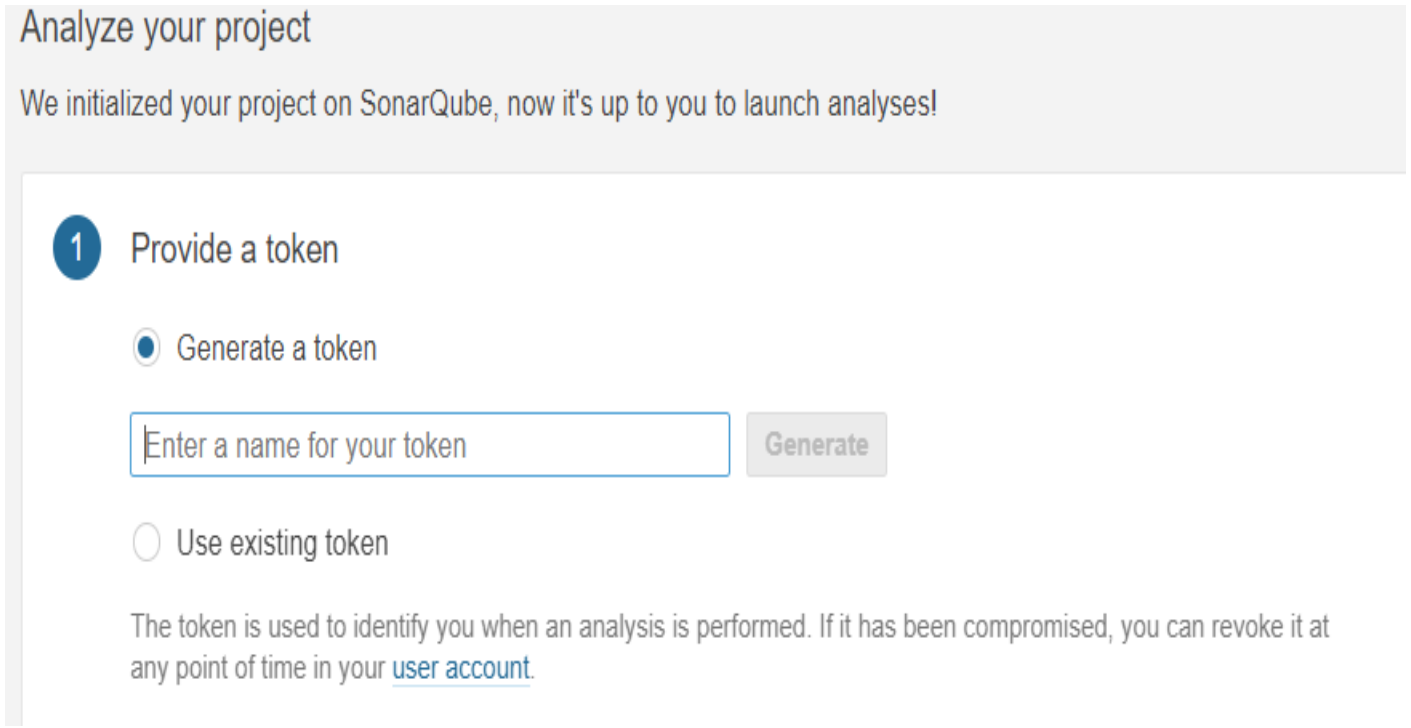
2. Once you have this image in your local machine, run the following command to run the sonar-server inside a docker container.

docker container run -d -p 9000:9000 --name sonarserver SonarQube:8.2-community

3. This will start your sonar server on port 9000. After a few minutes, open the URL localhost:9000. There you will be asked to log in, and the default username and password is admin.

4. Once we're logged in to create a new project and analyze the source code, click on the + icon on the top right corner of the window and Enter your project key and display name, now you will need to generate a token for your project.




Analyze your project
We initialized your project on SonarQube, now it's up to you to launch analyses!
1
Provide a token
Generate a token
Enter a name for your token
Generate
Use existing token
The token is used to identify you when an analysis is performed. If it has been compromised, you can revoke it at any point of time in your user account.

2 Run analysis on your project

What is your project's main language?

Java | C# or VB.NET | **Other (JS, TS, Go, Python, PHP, ...)**

What is your OS?

Linux | **Windows** | macOS

Download and unzip the Scanner for Windows

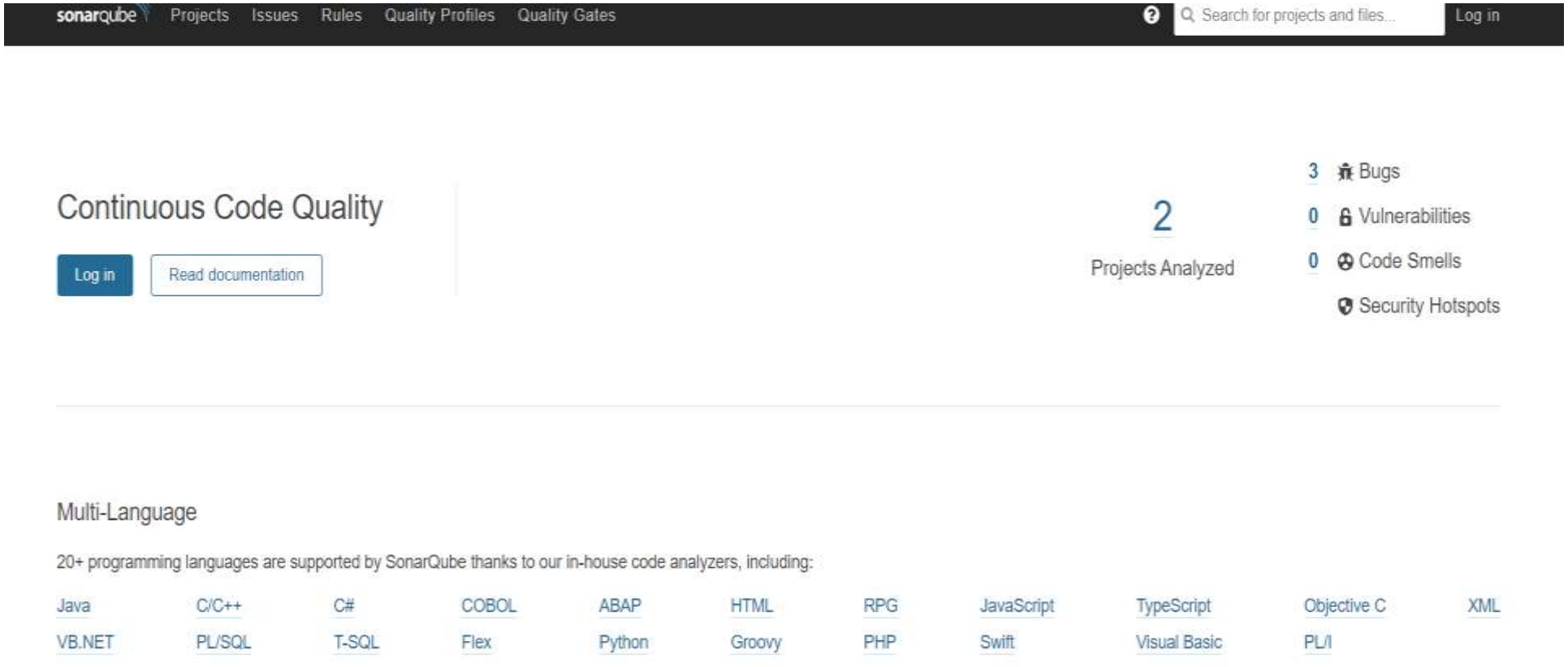
And add the `bin` directory to the `%PATH%` environment variable

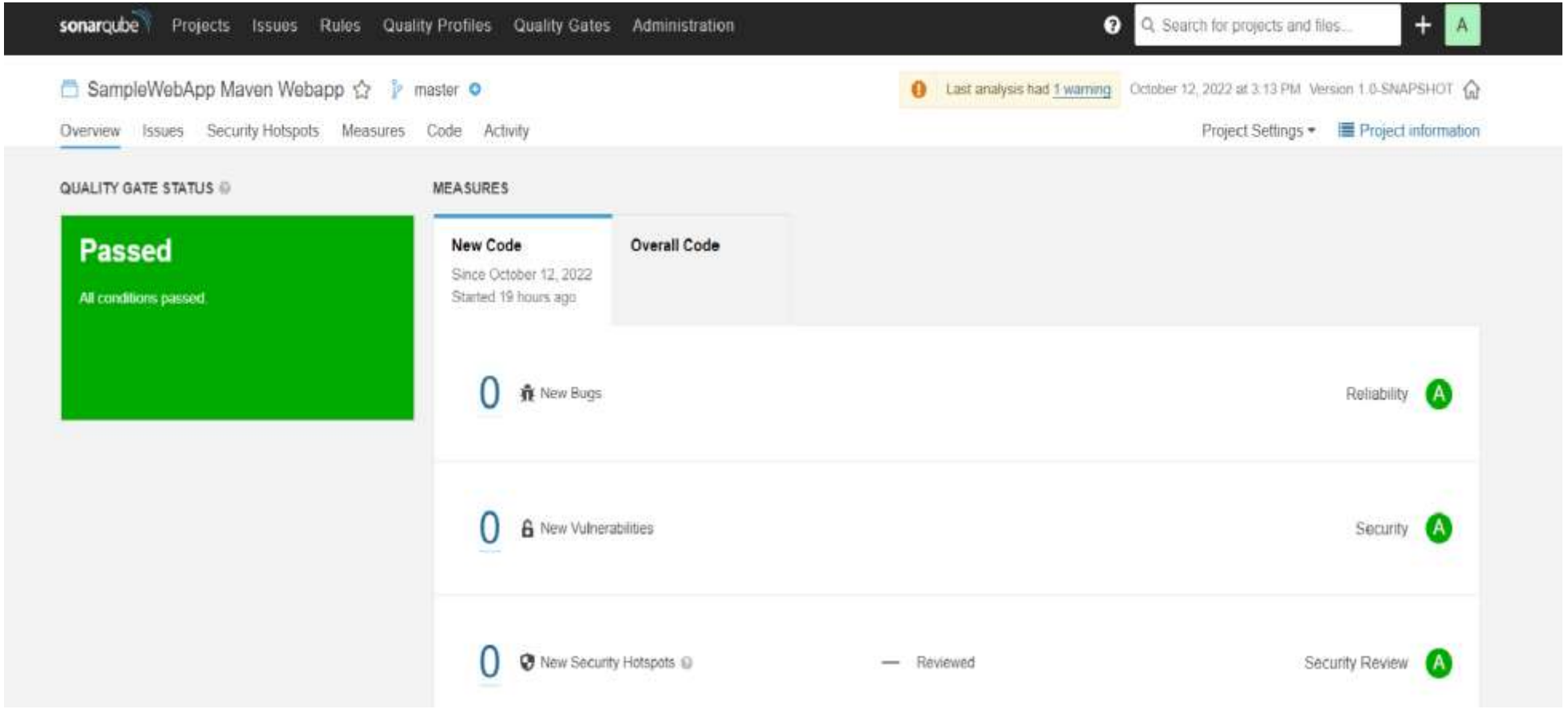
Download

Execute the Scanner for Maven from your computer

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

```
mvn sonar:sonar \ -Dsonar.projectKey=sam \ -
  Dsonar.host.url=http://localhost:9000 \ -
  Dsonar.login=6cf5a7debd7ca819b7e6130f0b324ea2ce3612bd
```


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Search for projects and files...
Log in
Continuous Code Quality
Log in
Read documentation
2
Projects Analyzed
3 Bugs
0 Vulnerabilities
0 Code Smells
Security Hotspots
Multi-Language
20+ programming languages are supported by SonarQube thanks to our in-house code analyzers, including:
Java
C/C++
C#
COBOL
ABAP
HTML
RPG
JavaScript
TypeScript
Objective C
XML
VB.NET
PL/SQL
T-SQL
Flex
Python
Groovy
PHP
Swift
Visual Basic
PL/I


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
Search for projects and files...
A
SampleWebApp Maven Webapp
master
Last analysis had 1 warning
October 12, 2022 at 3:13 PM Version 1.0-SNAPSHOT
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project information
QUALITY GATE STATUS
Passed
All conditions passed
MEASURES
New Code
Since October 12, 2022
Started 19 hours ago
Overall Code
0
New Bugs
Reliability
A
0
New Vulnerabilities
Security
A
0
New Security Hotspots
Reviewed
Security Review
A

ANY QUERIES