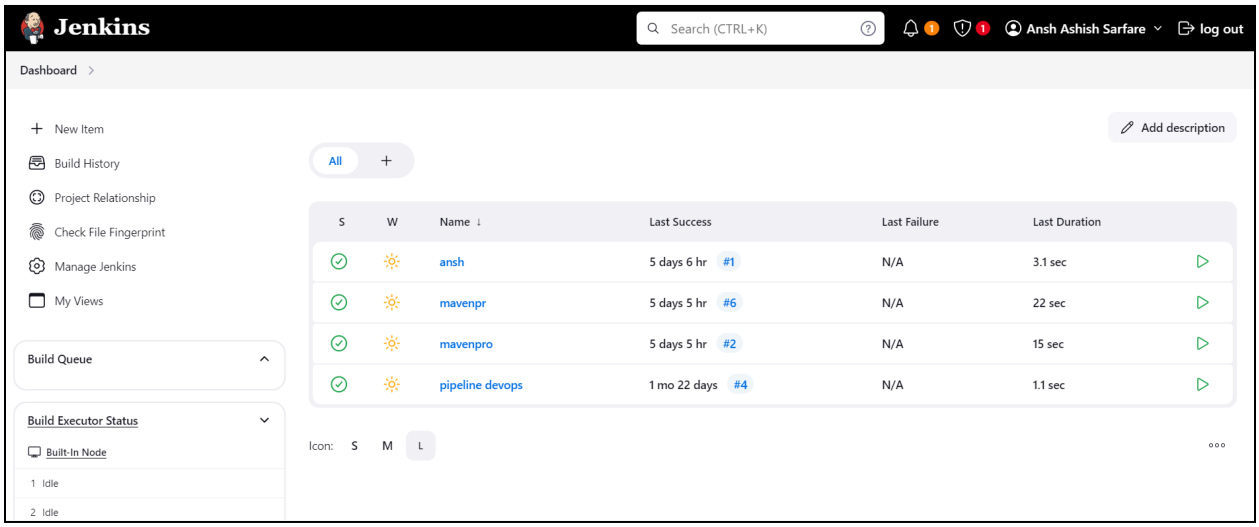
ADVANCE DEVOPS EXP-7

ANSH SARFARE **D15A/50**

Aim: To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.

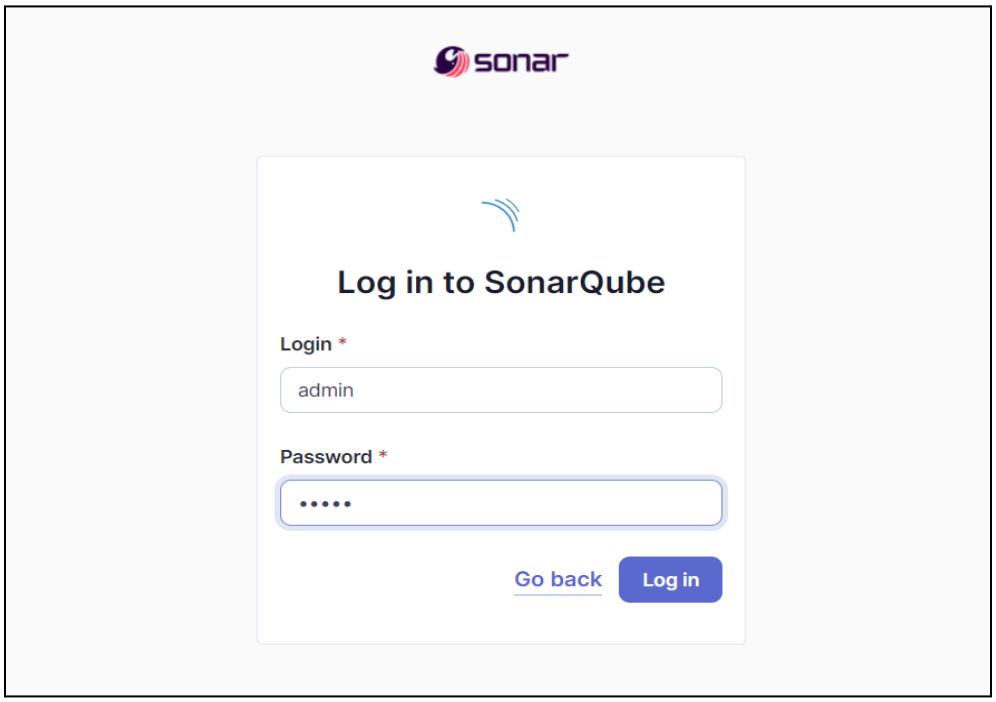
Step-1: Open up Jenkins Dashboard on localhost, port 8080 or whichever port it is at for you.



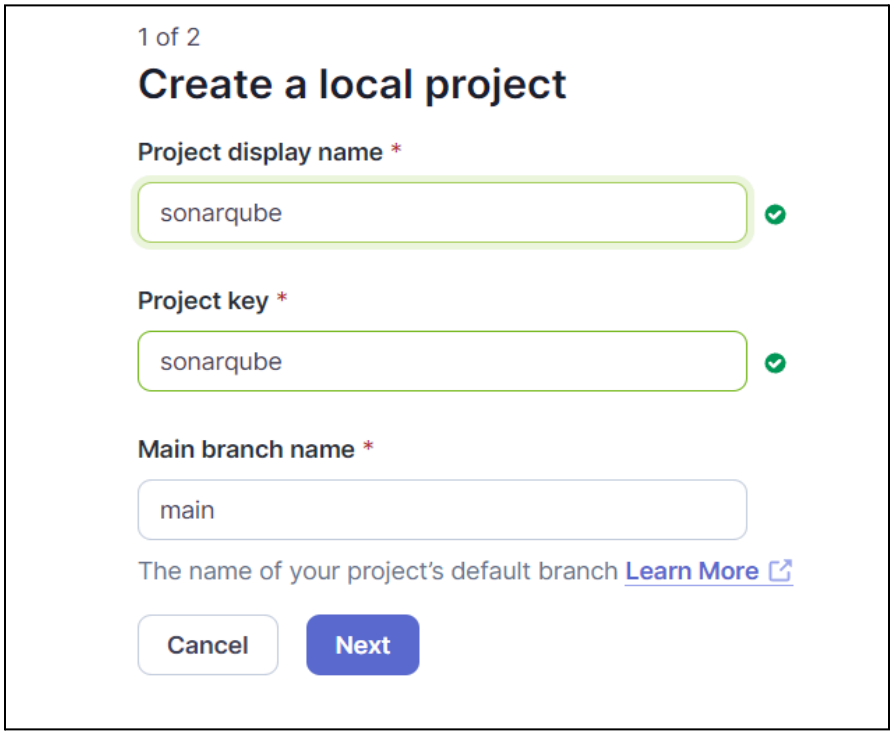
Step-2: Run SonarQube in a Docker container using this command :- a]docker -v
b] docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest

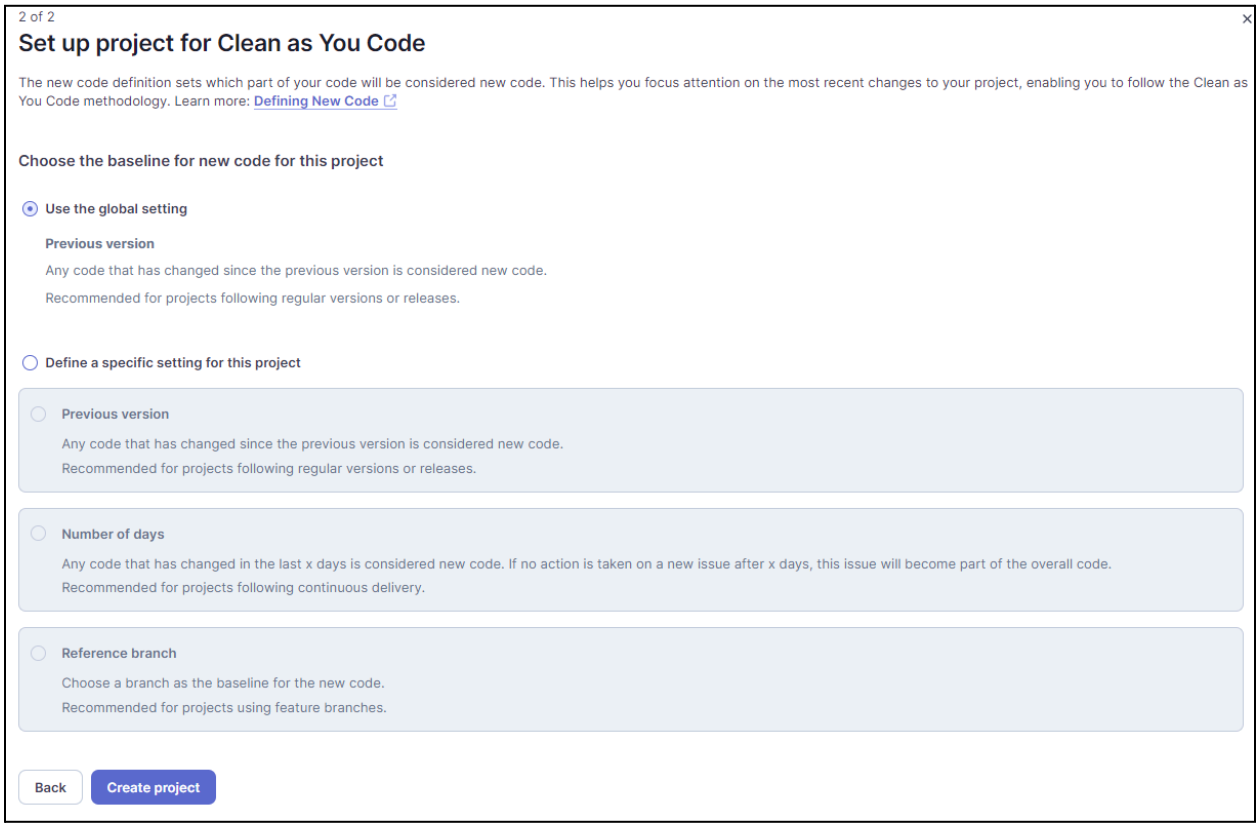
```
PS C:\Users\Ansh> docker -v
Docker version 27.0.3, build 7d4bcd8
PS C:\Users\Ansh> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube

7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
e4a886abe0db4f8a8c19e8f125ce97244d50eea97f9e98f2d829b724bc95c973
PS C:\Users\Ansh>
```

Step-3: Once the container is up and running, you can check the status of SonarQube at localhost port 9000. The login id is “admin” and the password is also “admin”.

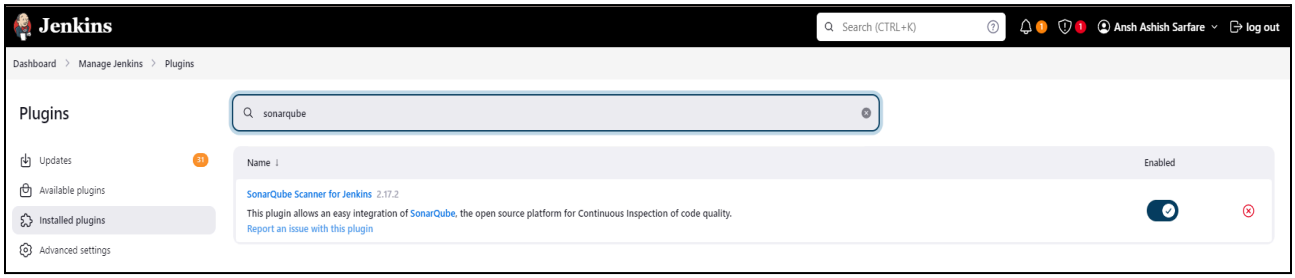


Step-4: Create a local project in SonarQube with the name sonarqube

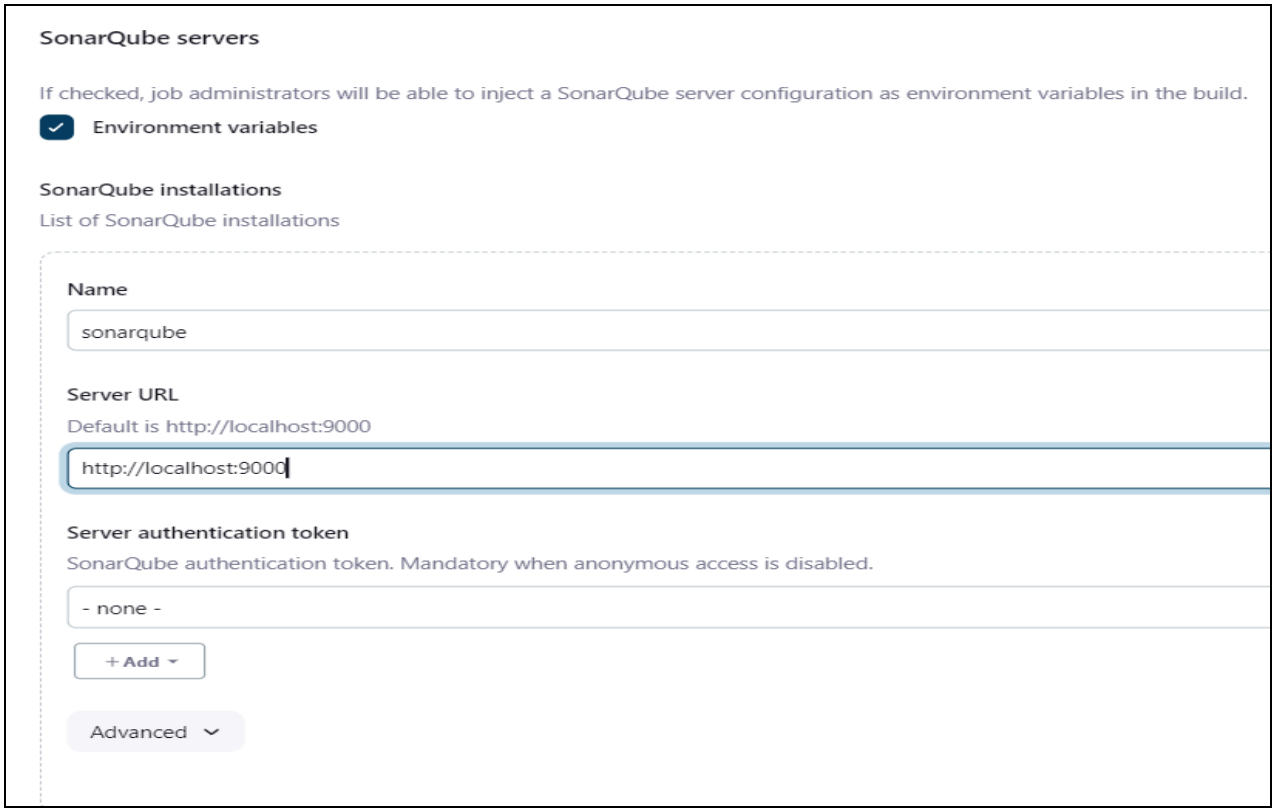




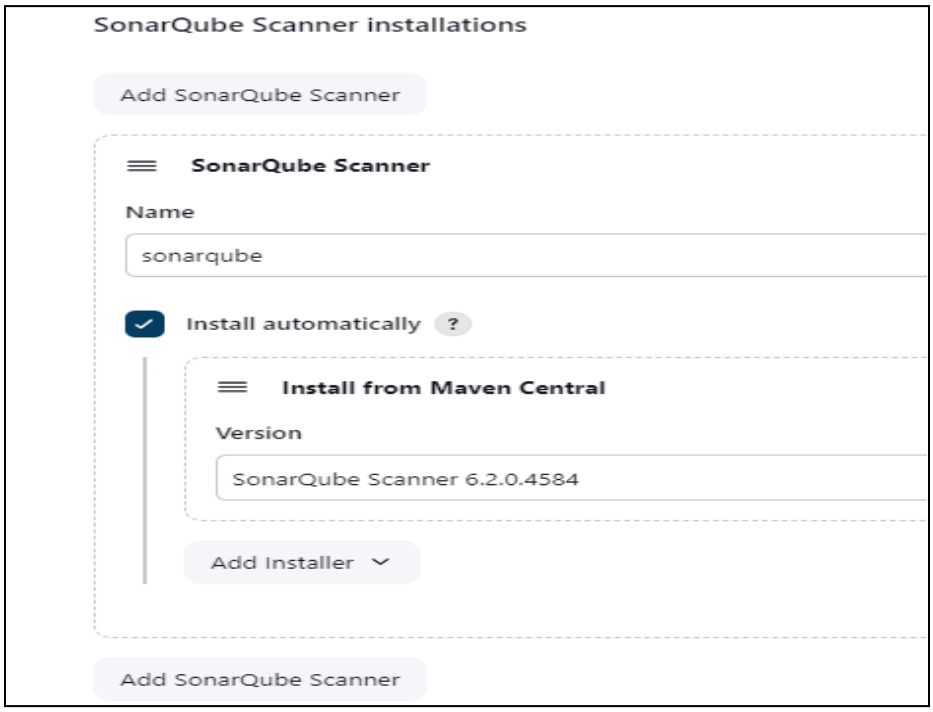
Step-5: Setup the project and come back to Jenkins Dashboard. Go to Manage Jenkins → Plugins and search for SonarQube Scanner in Available Plugins and install it.



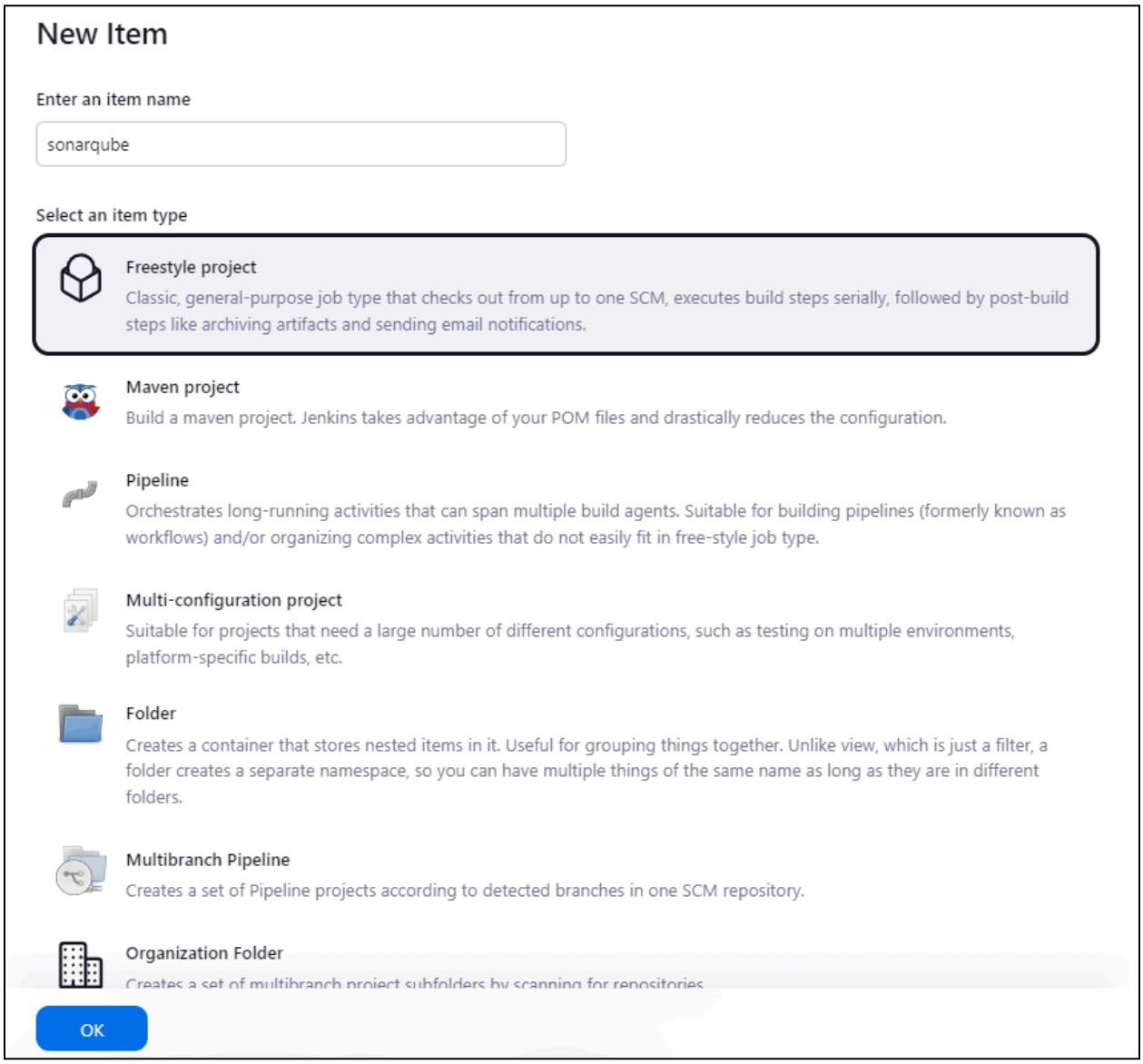
Step-6: Under 'Manage Jenkins → System', look for SonarQube Servers and enter these details. Name : sonarqube, Server URL : http://localhost:9000



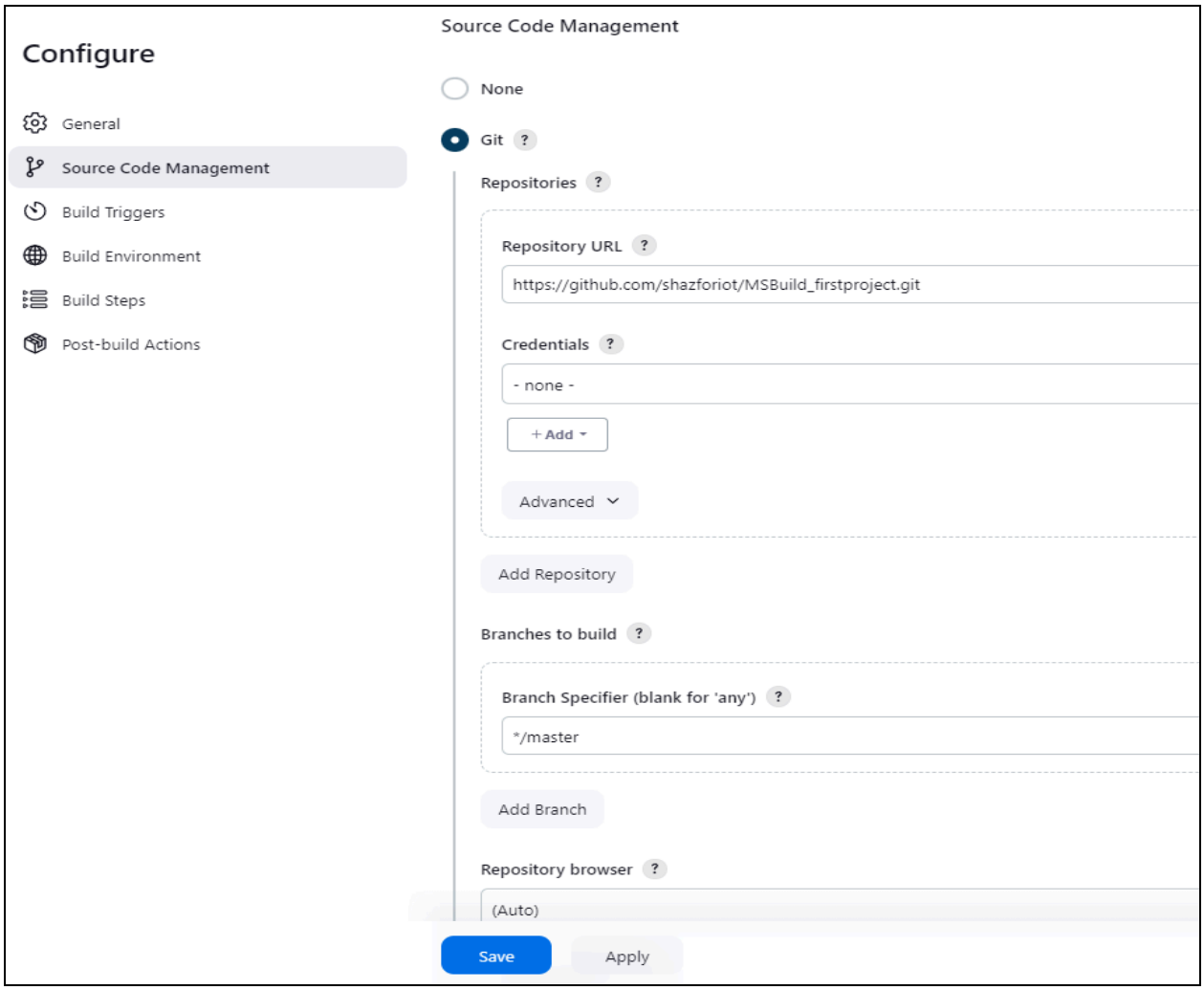
Step-7: Search for SonarQube Scanner under Global Tool Configuration. Choose the latest configuration and choose Install automatically. Manage Jeknins → Tools → SonarQube Scanner Installation.



Step-8: After the configuration, create a New Item in Jenkins, choose a freestyle project named sonarqube.



Step-9: Choose this GitHub repository in Source Code Management. https://github.com/shazforiot/MSBuild_firstproject.git . It is a sample hello-world project with no vulnerabilities and issues, just to test the integration.



Step-10: Under Build-> Execute SonarQube Scanner, enter these Analysis Properties. Mention the SonarQube Project Key, Login, Password, Source path and Host URL.

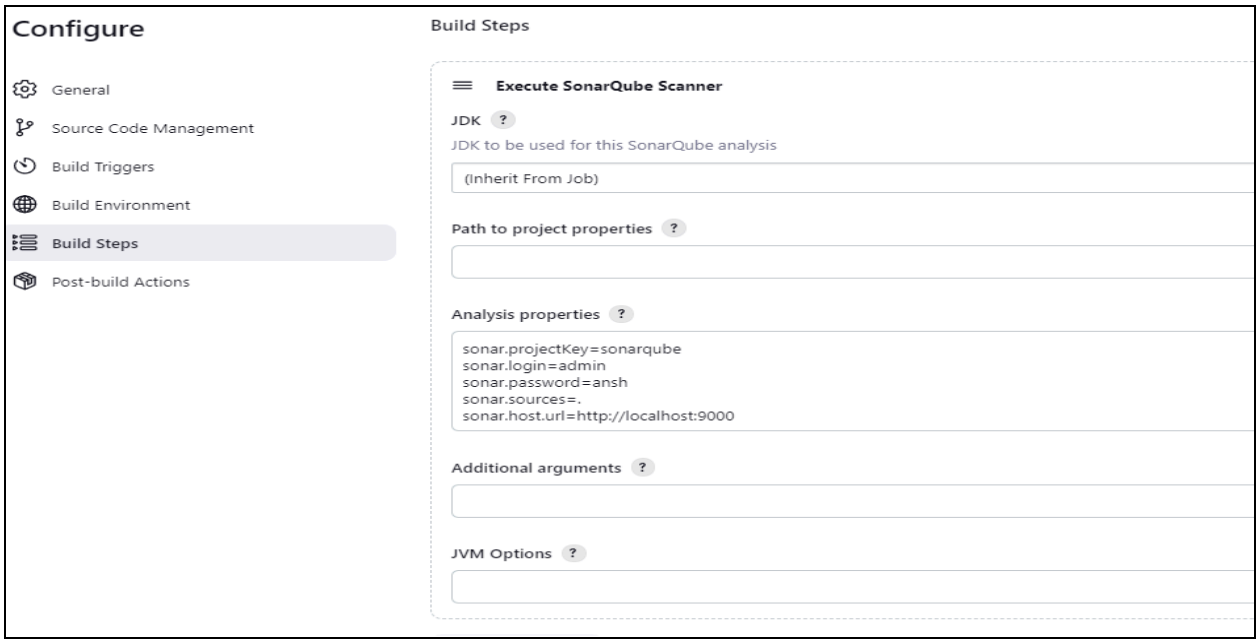
sonar.projectKey=sonarqube

sonar.login=admin

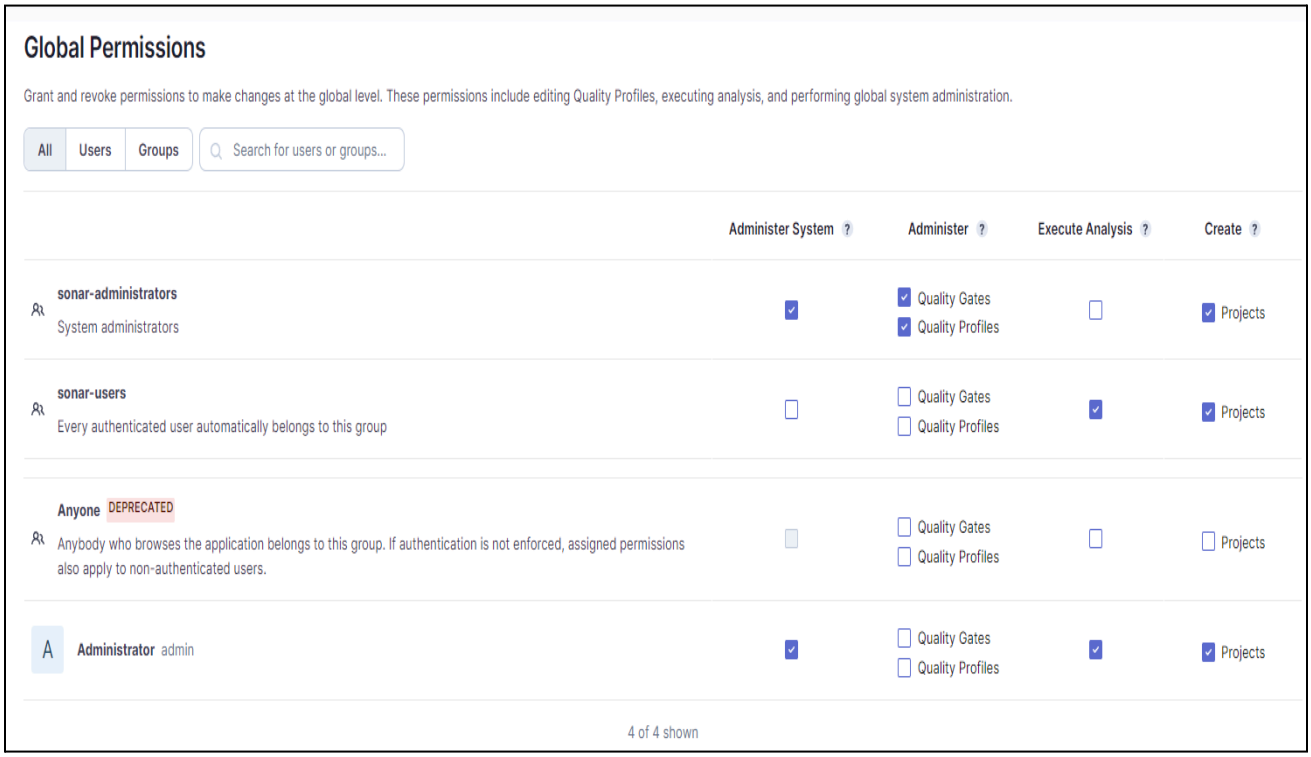
sonar.password=ansh

sonar.sources=.

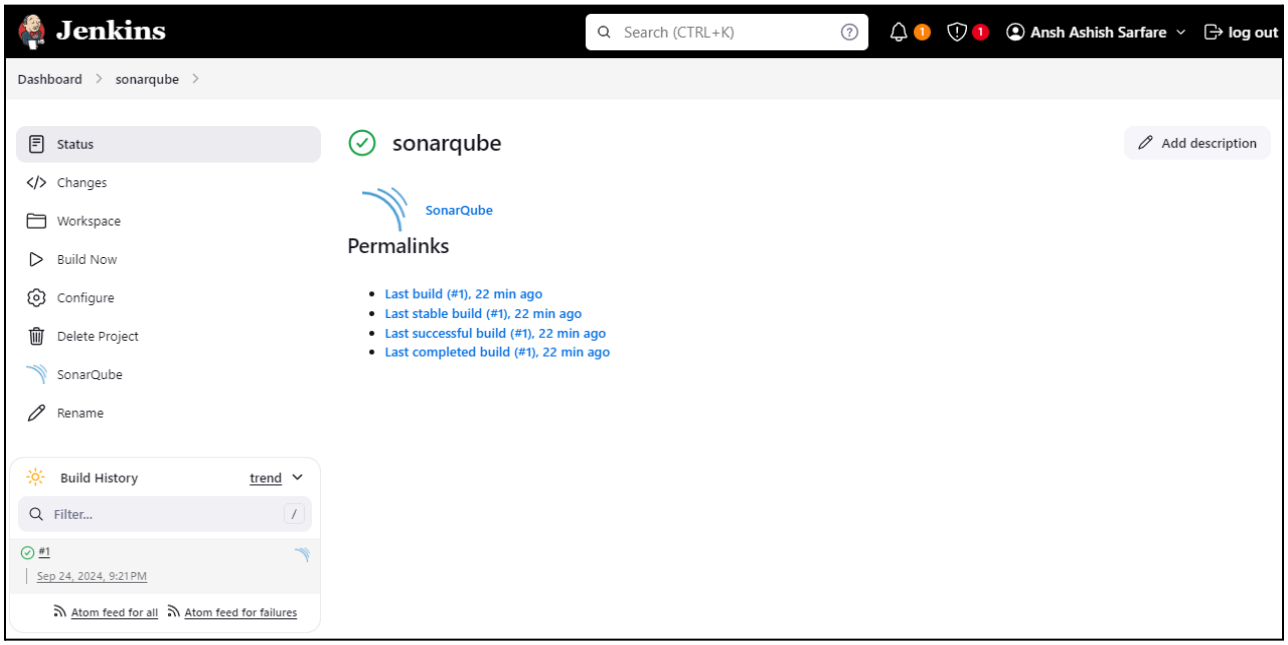
sonar.host.url=http://localhost:9000

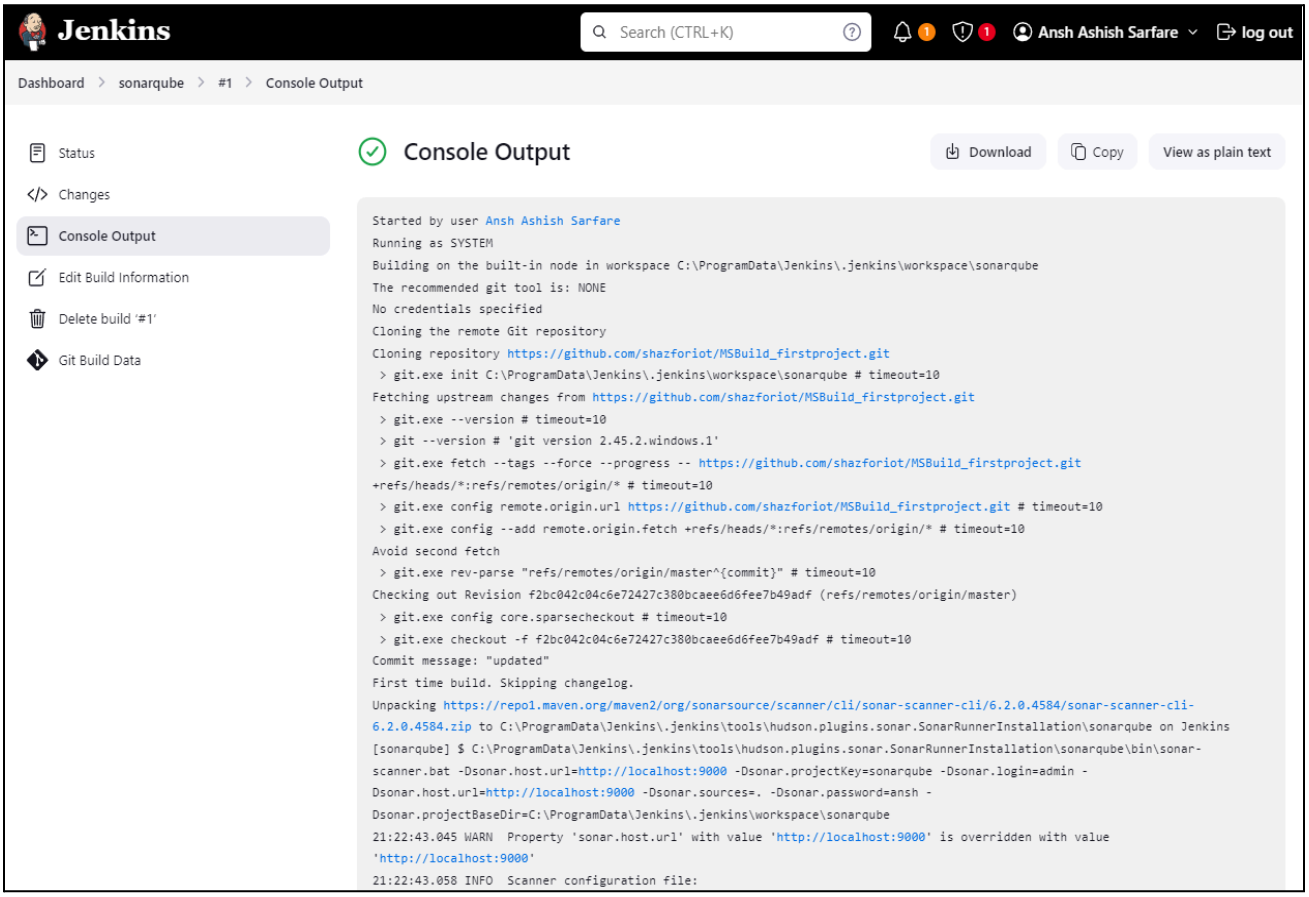


Step-11: Go to http://localhost:9000/admin/permissions and allow Execute Permissions to the Admin user.



Step-12: Run The Build and check the console output.

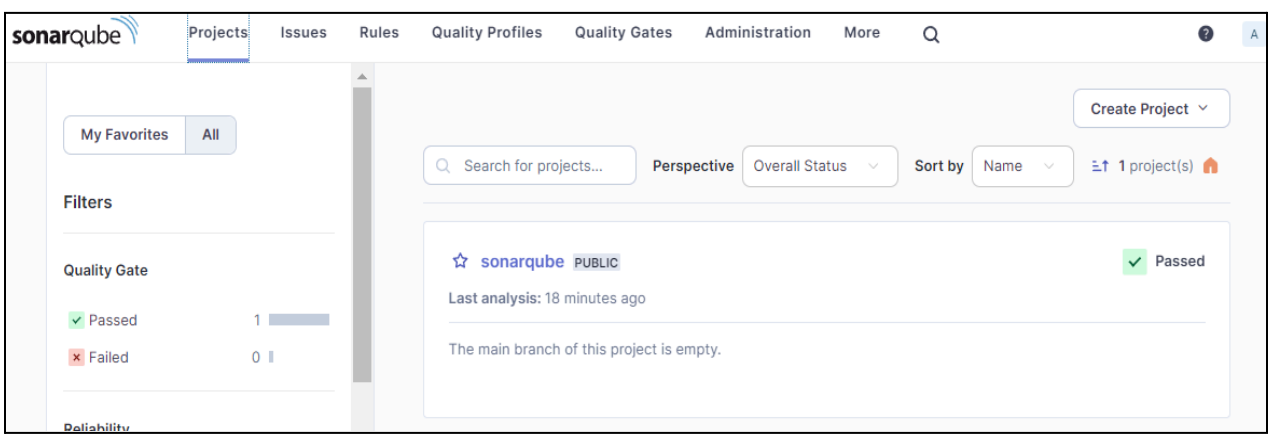


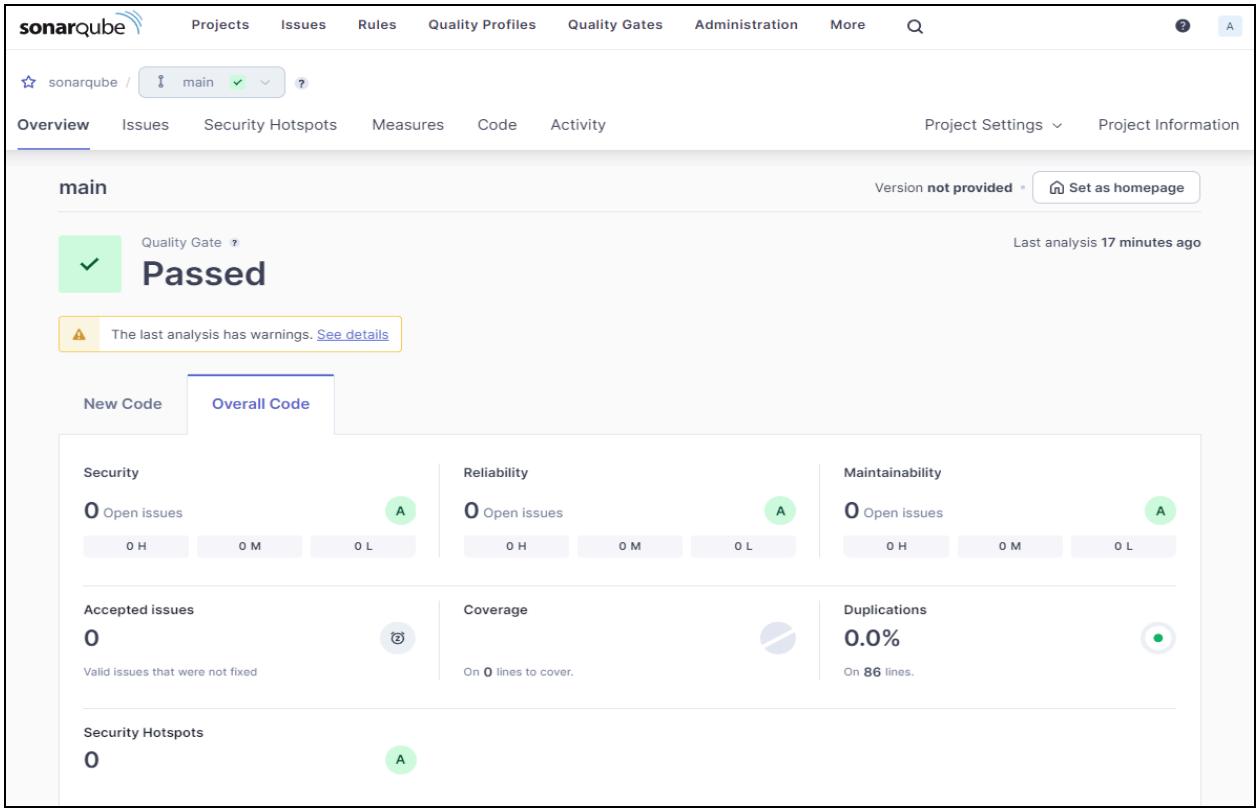


Dashboard > sonarqube > #1 > Console Output

```
21:23:05.658 INFO  14/14 source files have been analyzed
21:23:05.658 INFO  Sensor TextAndSecretsSensor [text] (done) | time=903ms
21:23:05.662 INFO  ------------- Run sensors on project
21:23:05.748 INFO  Sensor C# [csharp]
21:23:05.749 WARN  Your project contains C# files which cannot be analyzed with the scanner you are using. To analyze C# or
VB.NET, you must use the SonarScanner for .NET 5.x or higher, see https://redirect.sonarsource.com/doc/install-configure-
scanner-msbuild.html
21:23:05.749 INFO  Sensor C# [csharp] (done) | time=1ms
21:23:05.749 INFO  Sensor Analysis Warnings import [csharp]
21:23:05.751 INFO  Sensor Analysis Warnings import [csharp] (done) | time=2ms
21:23:05.752 INFO  Sensor C# File Caching Sensor [csharp]
21:23:05.752 WARN  Incremental PR analysis: Could not determine common base path, cache will not be computed. Consider setting
'sonar.projectBaseDir' property.
21:23:05.752 INFO  Sensor C# File Caching Sensor [csharp] (done) | time=1ms
21:23:05.752 INFO  Sensor Zero Coverage Sensor
21:23:05.762 INFO  Sensor Zero Coverage Sensor (done) | time=9ms
21:23:05.765 INFO  SCM Publisher SCM provider for this project is: git
21:23:05.767 INFO  SCM Publisher 4 source files to be analyzed
21:23:06.128 INFO  SCM Publisher 4/4 source files have been analyzed (done) | time=360ms
21:23:06.130 INFO  CPD Executor Calculating CPD for 0 files
21:23:06.131 INFO  CPD Executor CPD calculation finished (done) | time=0ms
21:23:06.134 INFO  SCM revision ID 'f2bc042c04c6e72427c380bcaee6d6fee7b49adf'
21:23:06.355 INFO  Analysis report generated in 92ms, dir size=201.0 kB
21:23:06.392 INFO  Analysis report compressed in 28ms, zip size=22.6 kB
21:23:06.533 INFO  Analysis report uploaded in 139ms
21:23:06.534 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube
21:23:06.534 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted
analysis report
21:23:06.535 INFO  More about the report processing at http://localhost:9000/api/ce/task?id=e4638b3c-d13e-449c-991b-
639bd23c8ef1
21:23:06.543 INFO  Analysis total time: 16.829 s
21:23:06.543 INFO  SonarScanner Engine completed successfully
21:23:06.578 INFO  EXECUTION SUCCESS
21:23:06.579 INFO  Total time: 23.525s
Finished: SUCCESS
```

Step-13: Once the build is complete, check the project in SonarQube.




sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
A
sonarqube /
main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
main
Version not provided
Set as homepage
Quality Gate
Passed
Last analysis 17 minutes ago
The last analysis has warnings. See details
New Code
Overall Code
Security
0 Open issues
A
0 H
0 M
0 L
Reliability
0 Open issues
A
0 H
0 M
0 L
Maintainability
0 Open issues
A
0 H
0 M
0 L
Accepted issues
0
Valid issues that were not fixed
Coverage
On 0 lines to cover.
Duplications
0.0%
On 86 lines.
Security Hotspots
0
A