ADVANCE DEVOPS EXP 7

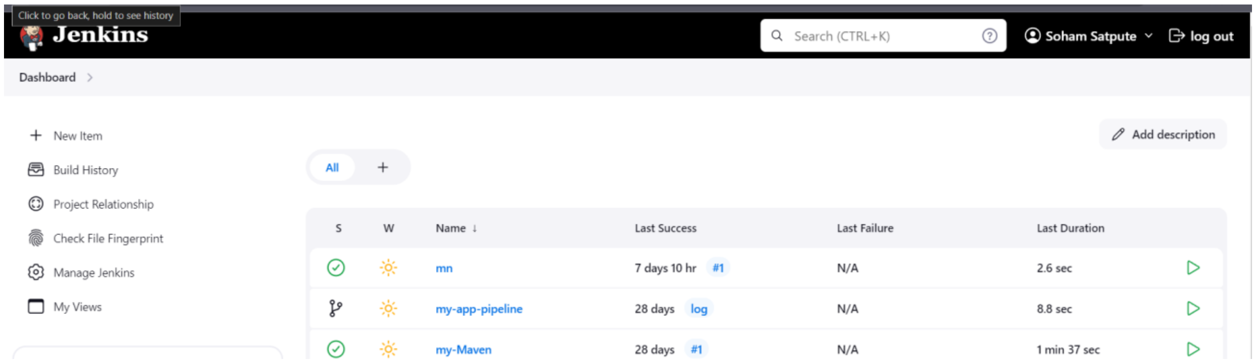
Name: Soham Satpute
Class:D15A
Roll No:52

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

Jenkins integration with SonarQube:

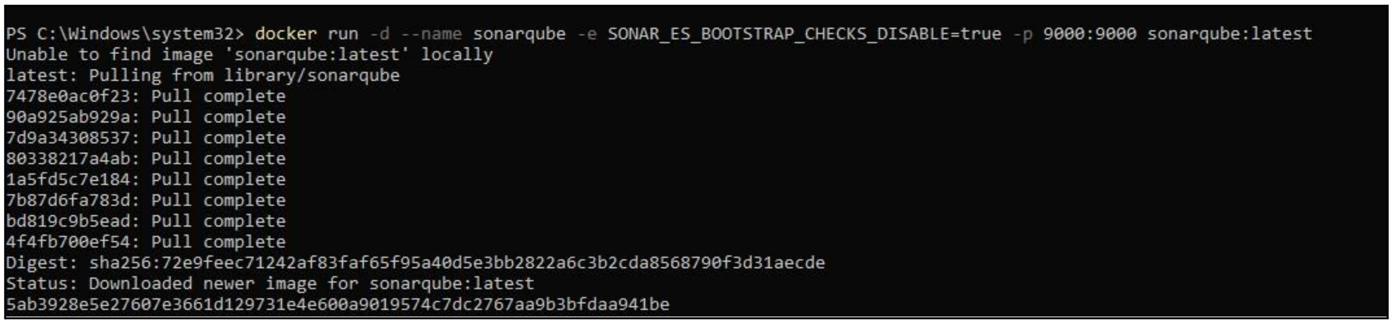
Steps:

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



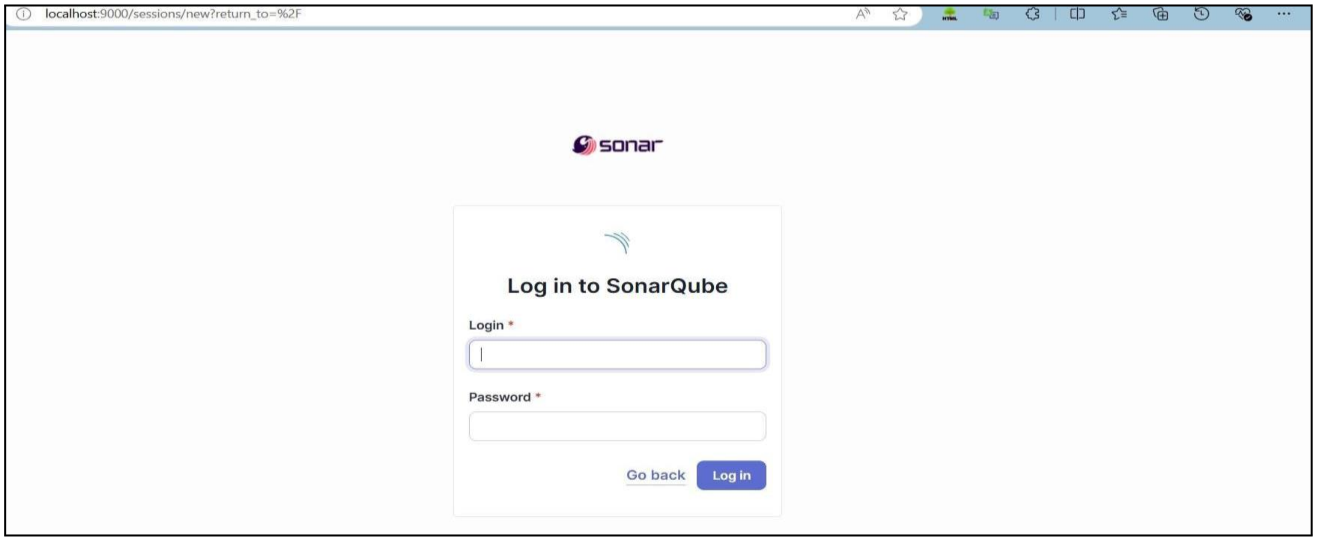
S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☀	mn	7 days 10 hr #1	N/A	2.6 sec
	☀	my-app-pipeline	28 days log	N/A	8.8 sec
✓	☀	my-Maven	28 days #1	N/A	1 min 37 sec

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

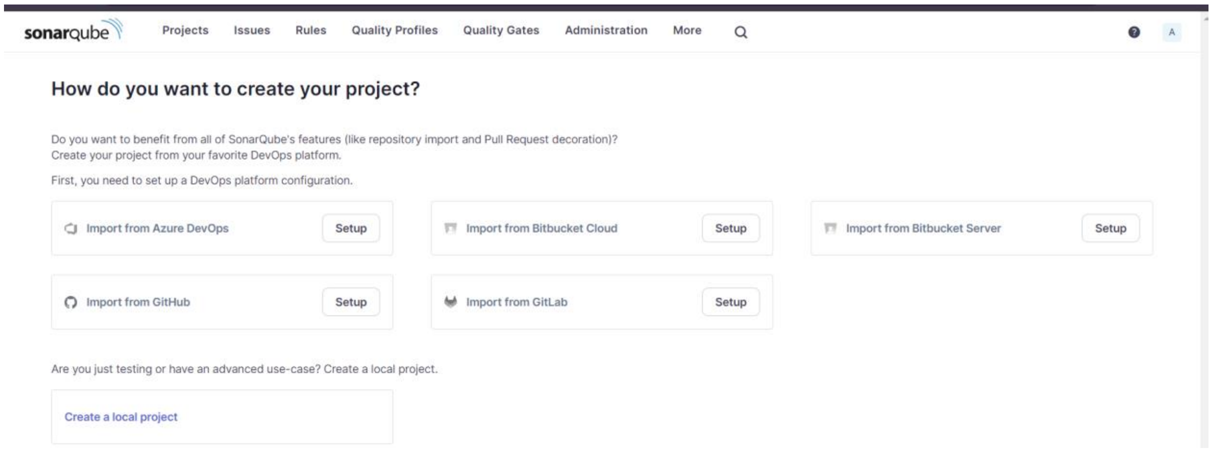


```
PS C:\Windows\system32> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
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
5ab3928e5e27607e3661d129731e4e600a9019574c7dc2767aa9b3bfdaa941be
```

3. Once the container is up and running, you can check the status of SonarQube at localhost port 9000.



4.Login to SonarQube using username admin and password admin.



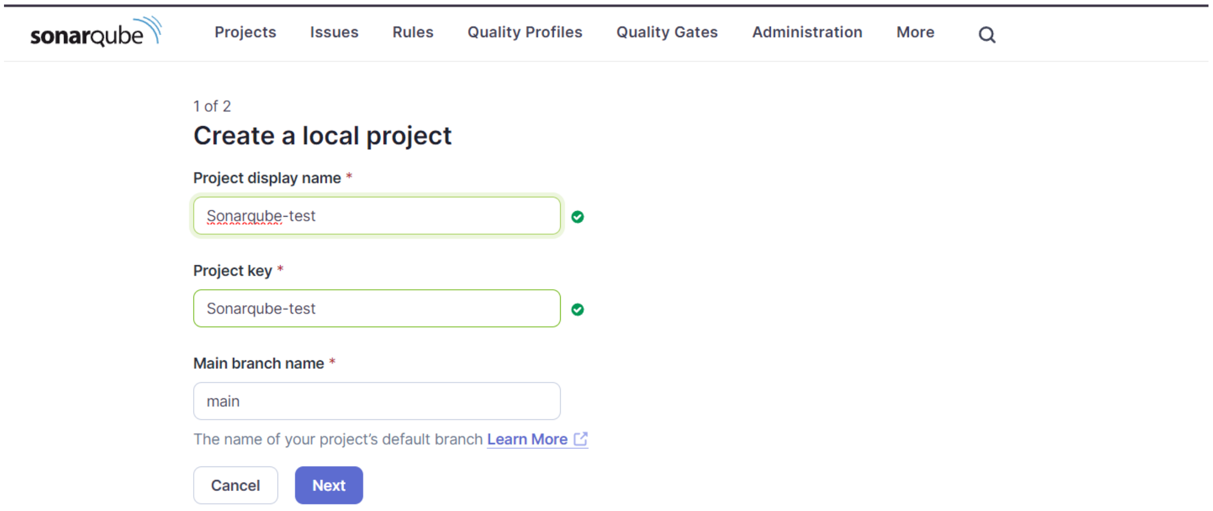
How do you want to create your project?

Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)?
Create your project from your favorite DevOps platform.

First, you need to set up a DevOps platform configuration.

Are you just testing or have an advanced use-case? Create a local project.

5.Create a manual project in SonarQube with the name sonarqube



1 of 2

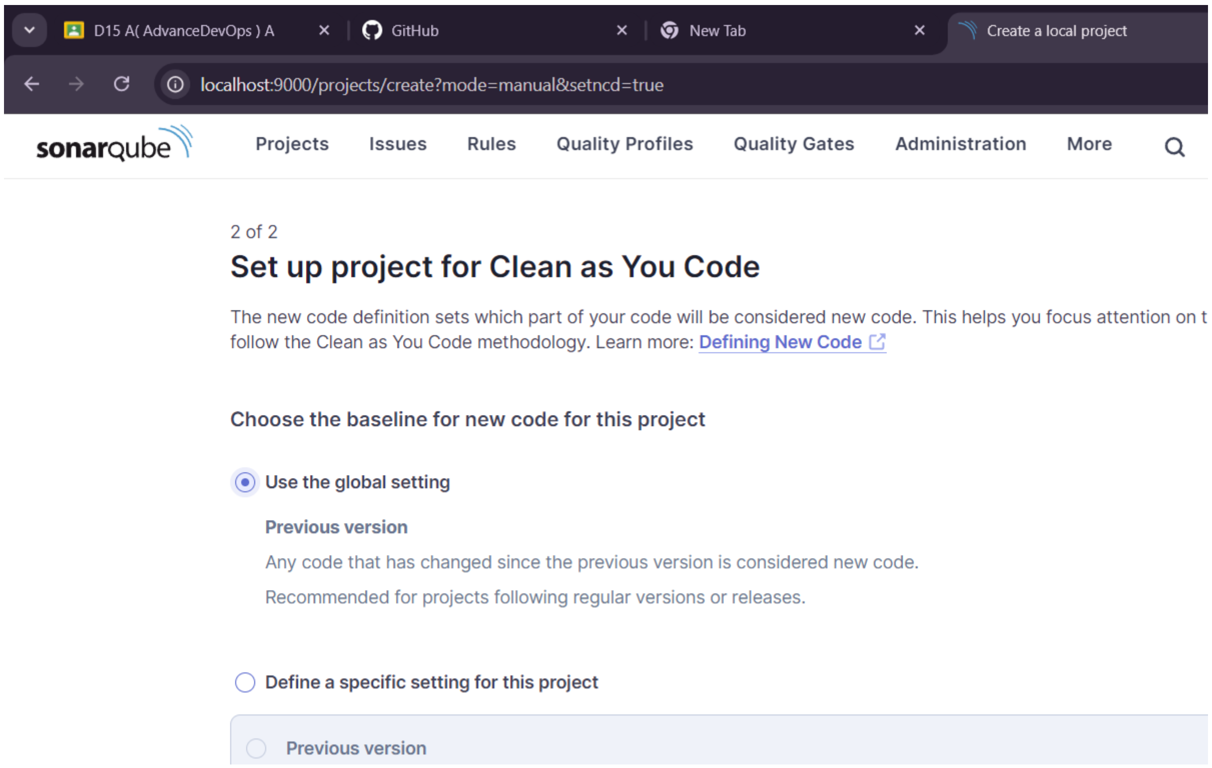
Create a local project

Project display name *: Sonarqube-test

Project key *: Sonarqube-test

Main branch name *: main

The name of your project's default branch Learn More



D15 A(AdvanceDevOps) A | GitHub | New Tab | Create a local project

localhost:9000/projects/create?mode=manual&setncd=true

sonarqube — Projects | Issues | Rules | Quality Profiles | Quality Gates | Administration | More

2 of 2

Set up project for Clean as You Code

The new code definition sets which part of your code will be considered new code. This helps you focus attention on t
follow the Clean as You Code methodology. Learn more: Defining New Code

Choose the baseline for new code for this project

● Use the global setting

Previous version

Any code that has changed since the previous version is considered new code.

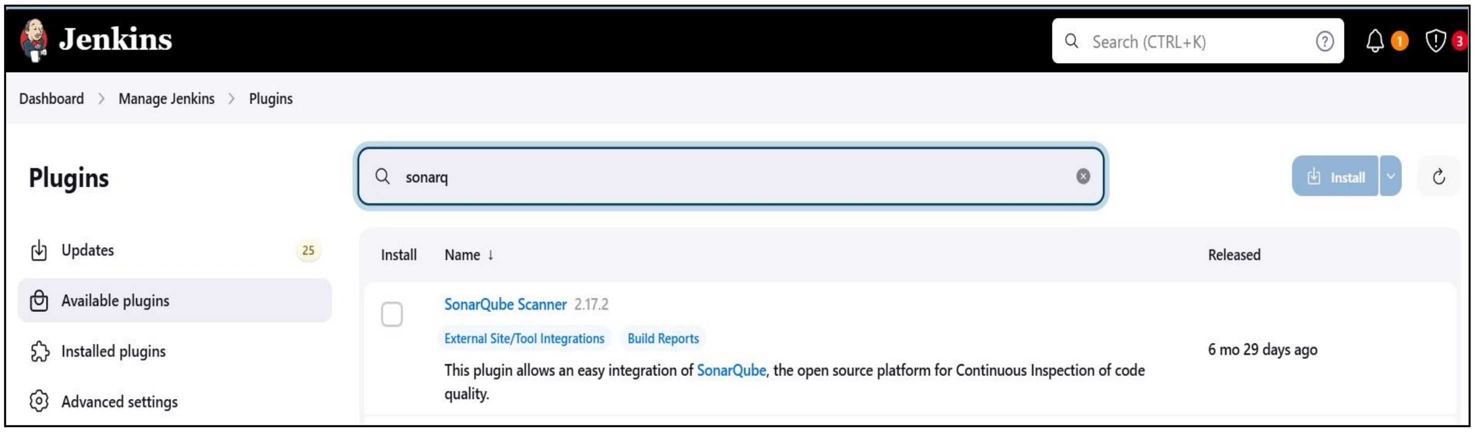
Recommended for projects following regular versions or releases.

○ Define a specific setting for this project

○ Previous version

Setup the project and come back to Jenkins Dashboard.

Go to Manage Jenkins and search for SonarQube Scanner for Jenkins and install it.



Jenkins — Search (CTRL+K)

Dashboard > Manage Jenkins > Plugins

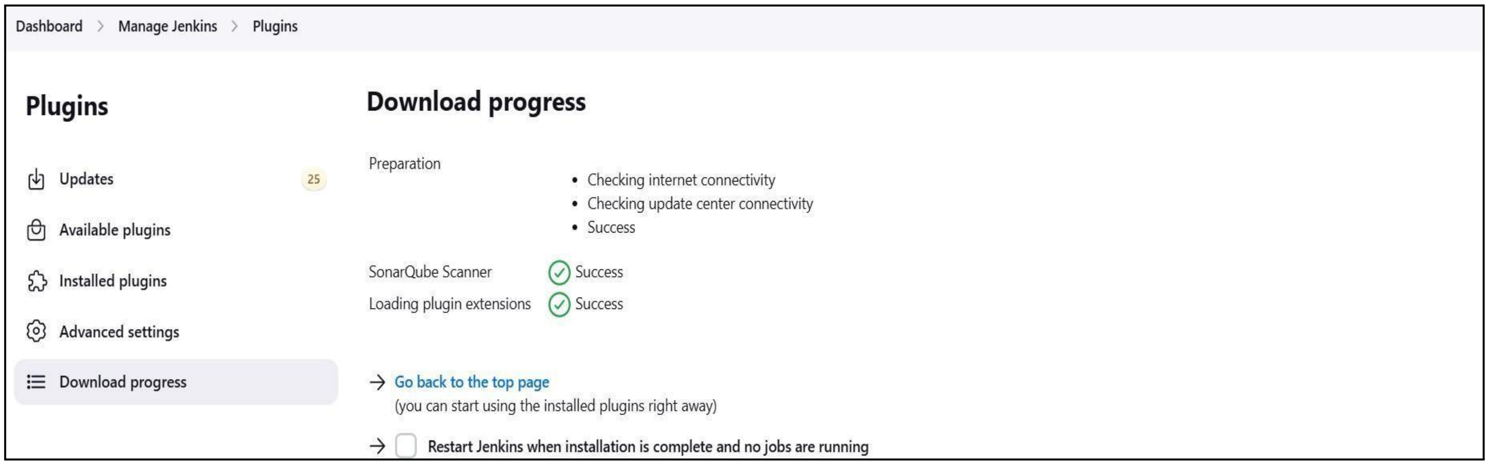
Plugins

- Updates 25
- Available plugins
- Installed plugins
- Advanced settings

sonarq

Install

Install	Name ↓	Released
☐	SonarQube Scanner 2.17.2 External Site/Tool Integrations Build Reports This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.	6 mo 29 days ago



Dashboard > Manage Jenkins > Plugins

Plugins

- Updates 25
- Available plugins
- Installed plugins
- Advanced settings
- Download progress

Download progress

Preparation
- Checking internet connectivity
- Checking update center connectivity
- Success

SonarQube Scanner ✓ Success

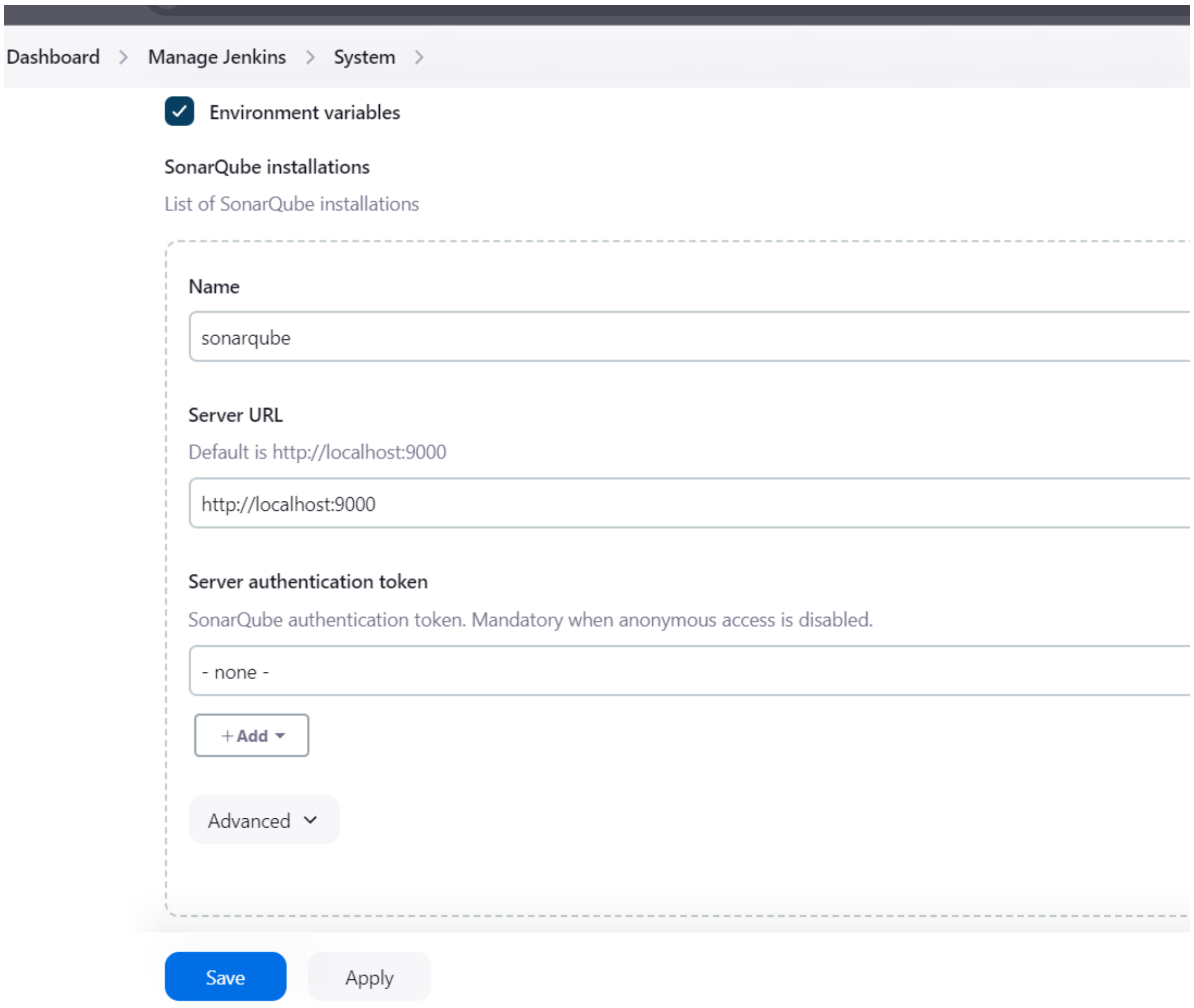
Loading plugin extensions ✓ Success

→ Go back to the top page
(you can start using the installed plugins right away)

→ ☐ Restart Jenkins when installation is complete and no jobs are running

6.Under Jenkins ‘Manage Jenkins’ then go to ‘system’, scroll and look for **SonarQube Servers** and enter
the details.
Enter the Server Authentication token if needed.

In SonarQube installations: Under **Name** add <project name of sonarqube>,here we have named it as **adv_devops_7_sonarqube** In **Server URL** Default is **http://localhost:9000**


Dashboard > Manage Jenkins > System >

✓ Environment variables

SonarQube installations

List of SonarQube installations

Name

sonarqube

Server URL

Default is http://localhost:9000

http://localhost:9000

Server authentication token

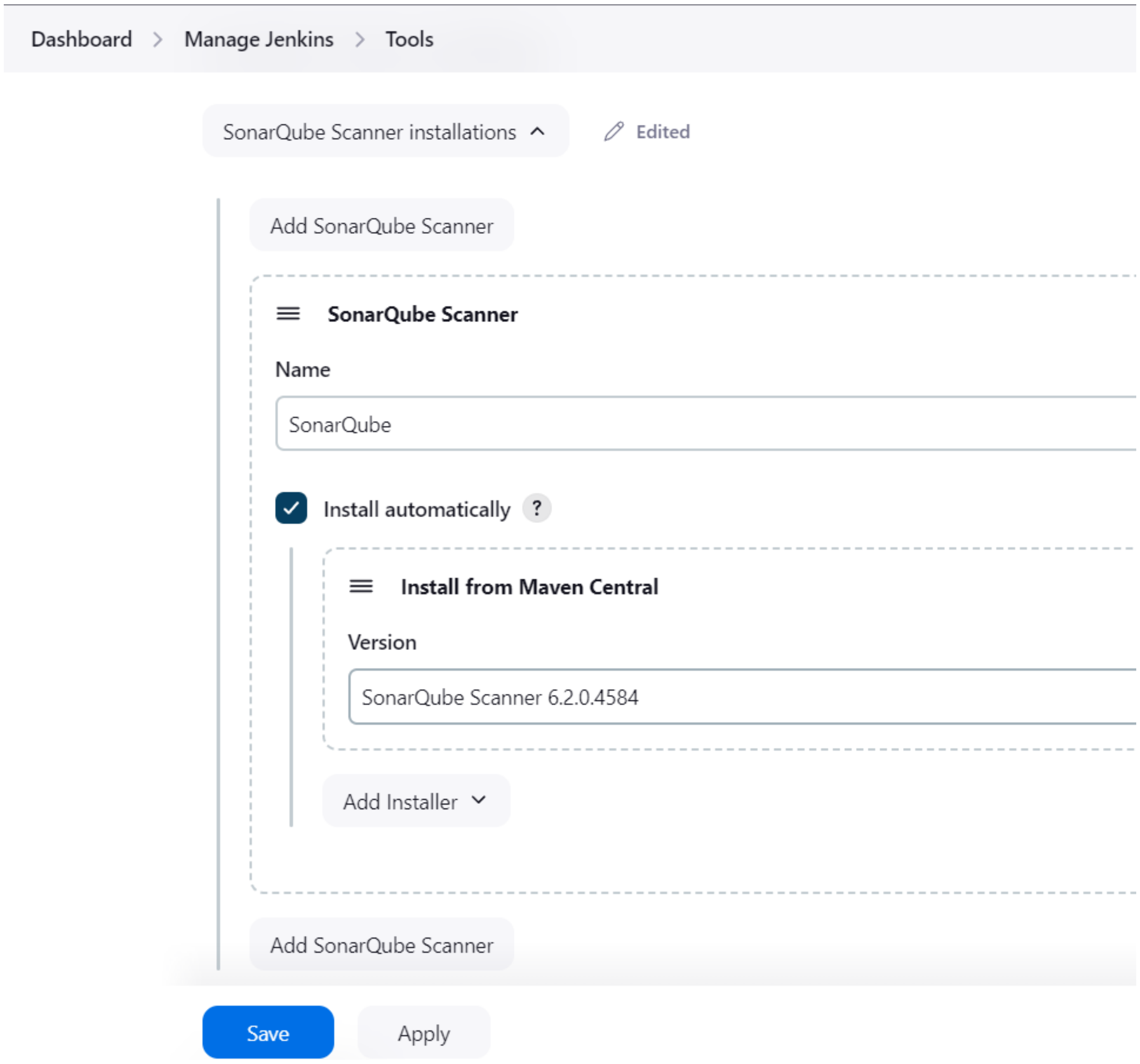
SonarQube authentication token. Mandatory when anonymous access is disabled.

- none -

7. Search for SonarQube Scanner under Global Tool Configuration.

Choose the latest configuration and choose Install automatically.

Dashboard > Manage Jenkins > Tools



Dashboard > Manage Jenkins > Tools

SonarQube Scanner installations

Edited

Add SonarQube Scanner

SonarQube Scanner

Name

SonarQube

✓ Install automatically ?

Install from Maven Central

Version

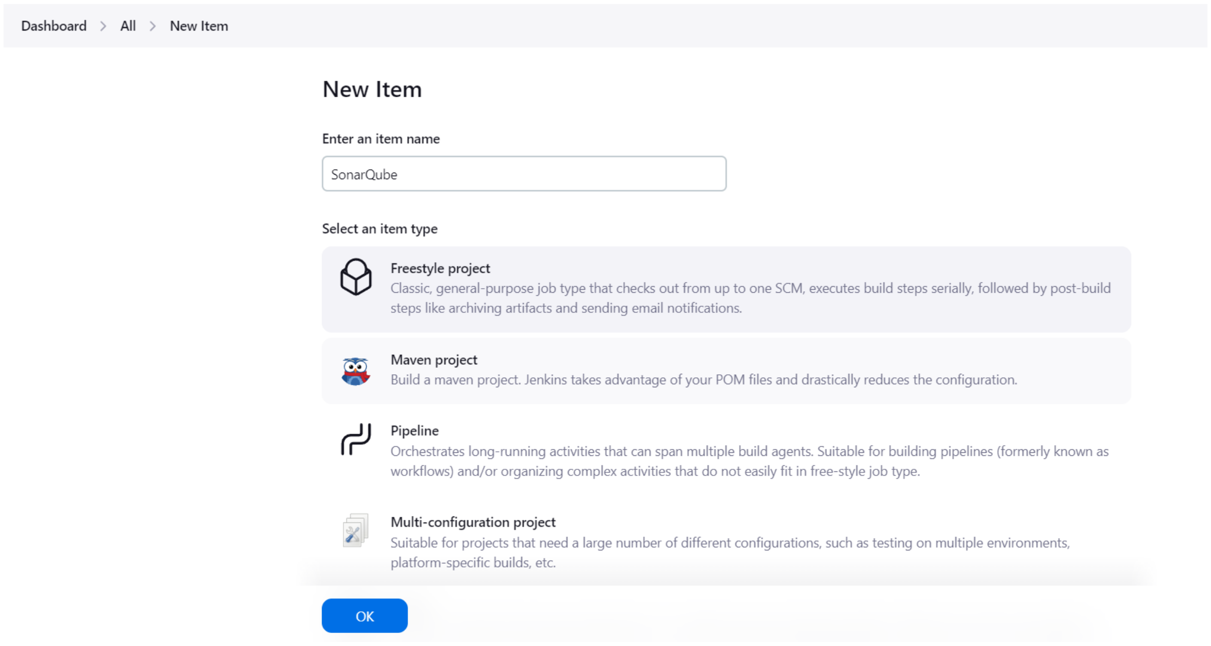
SonarQube Scanner 6.2.0.4584

Add Installer

Add SonarQube Scanner

Save Apply

8.After the configuration, create a New Item in Jenkins, choose a freestyle project.


Dashboard > All > New Item

New Item

Enter an item name

SonarQube

Select an item type

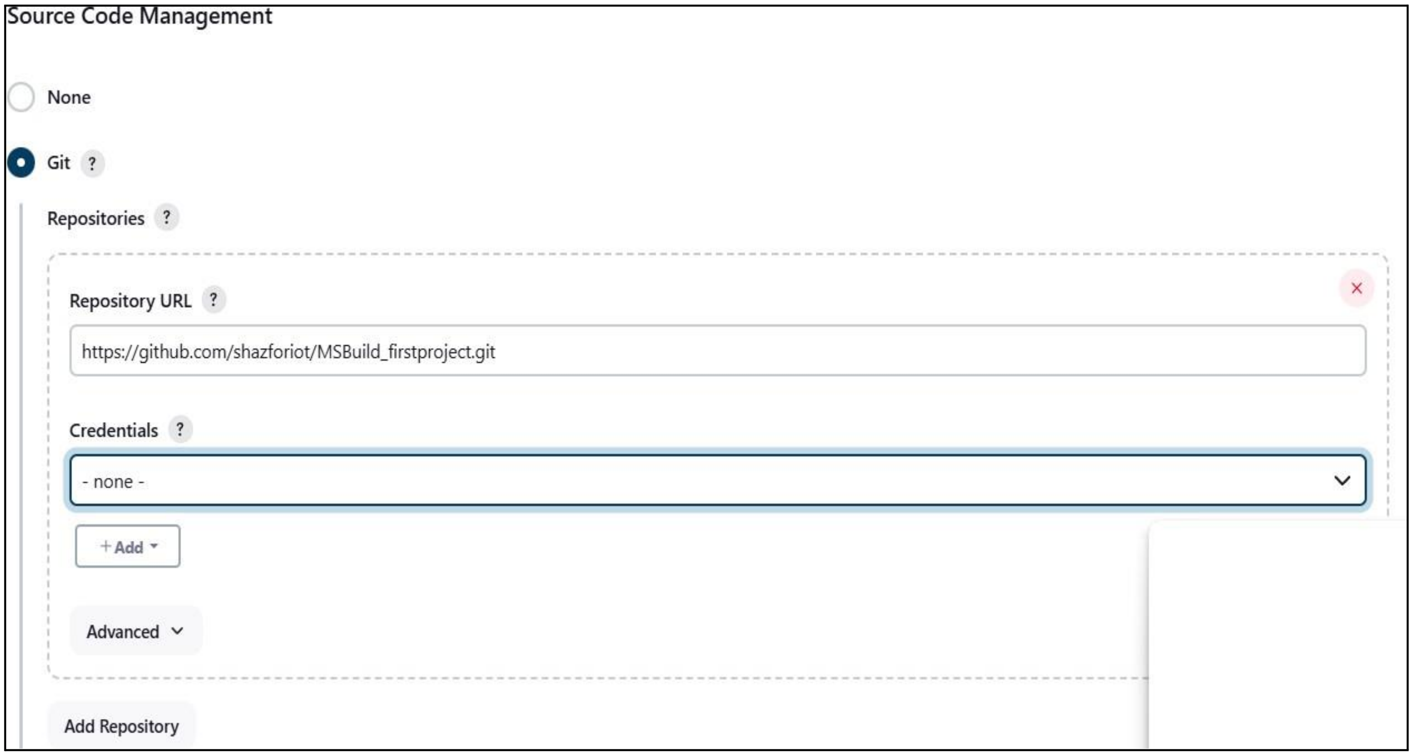
Freestyle project
Classic, general-purpose job type that checks out from up to one SCM, executes build steps serially, followed by post-build steps like archiving artifacts and sending email notifications.

Maven project
Build a maven project. Jenkins takes advantage of your POM files and drastically reduces the configuration.

Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

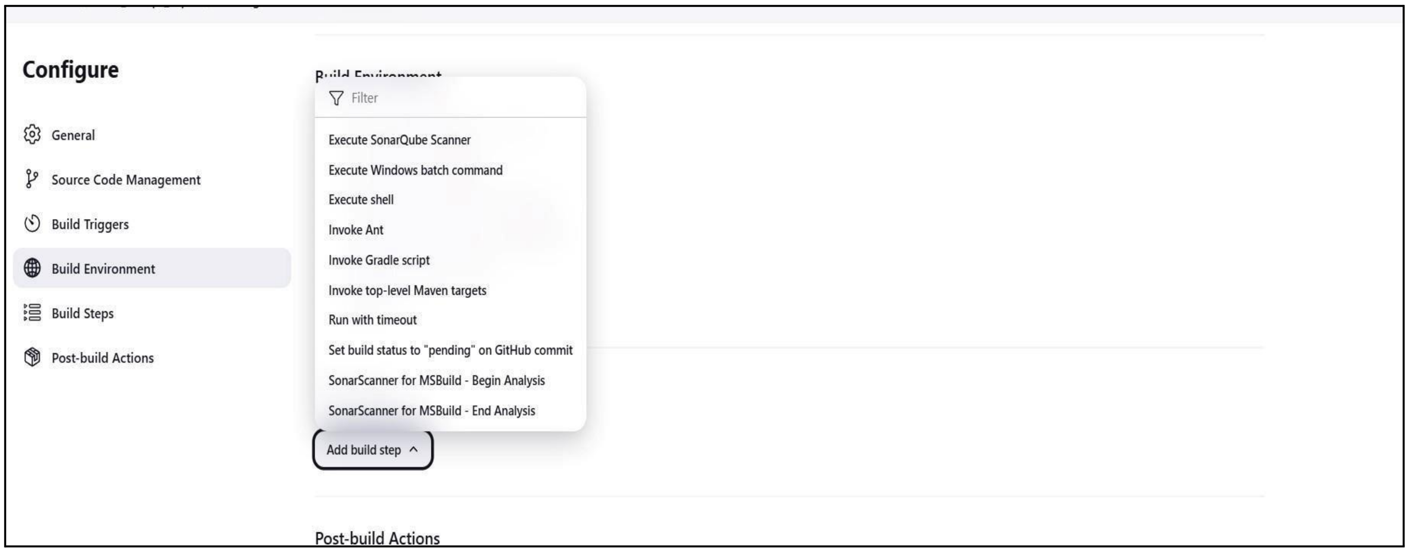
Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

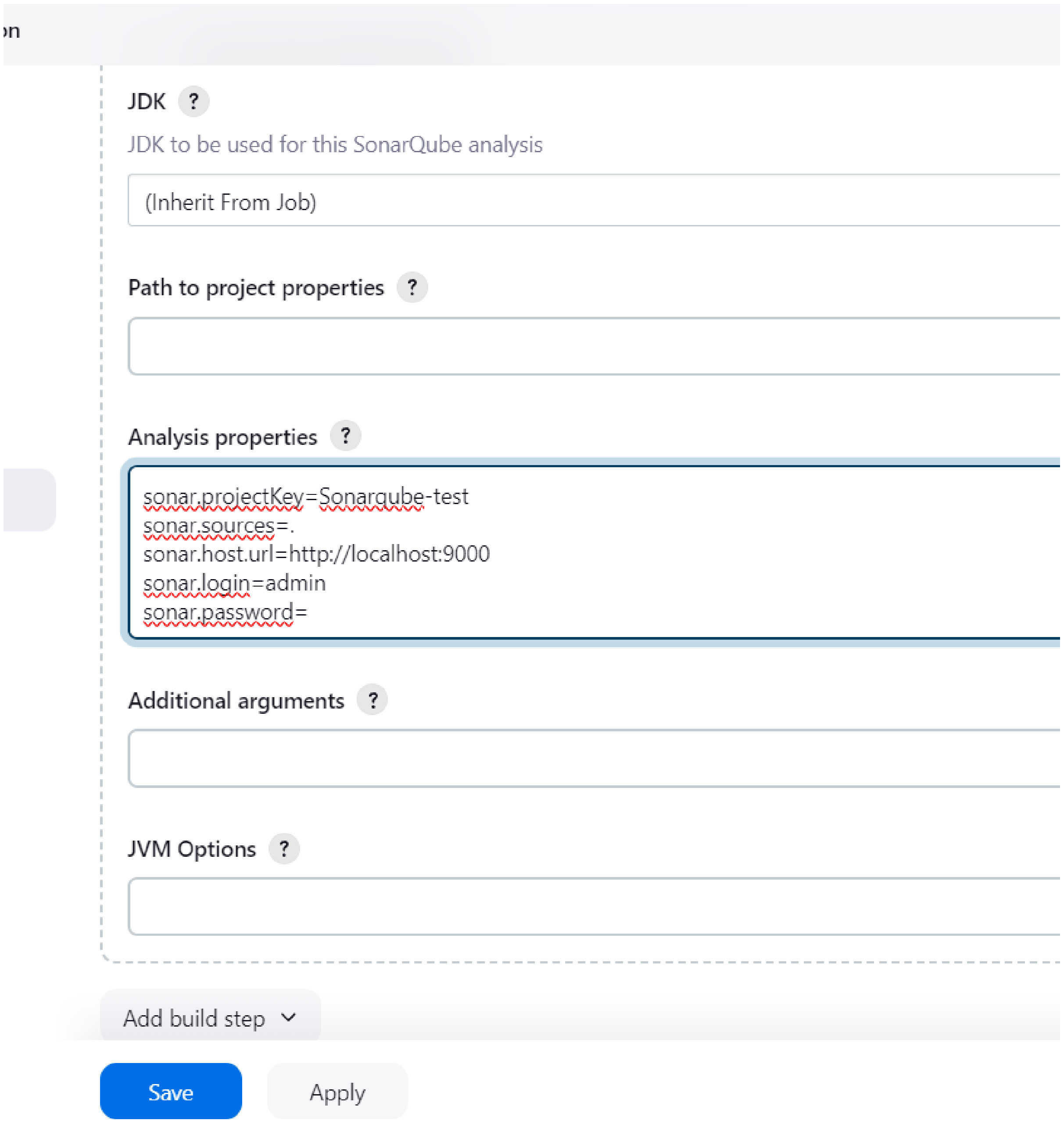
9. Choose this GitHub repository in Source Code Management.
https://github.com/shazforiot/MSBuild_firstproject.git
It is a sample hello-world project with no vulnerabilities and issues, just to test the integration.



Repository URL: https://github.com/shazforiot/MSBuild_firstproject.git
Credentials: - none -

10. Under **Select project → Configuration → Build steps → Execute SonarQube Scanner**, enter these Analysis properties. Mention the SonarQube Project Key, Login, Password, Source path and Host URL.





JDK ?

JDK to be used for this SonarQube analysis

(Inherit From Job)

Path to project properties ?

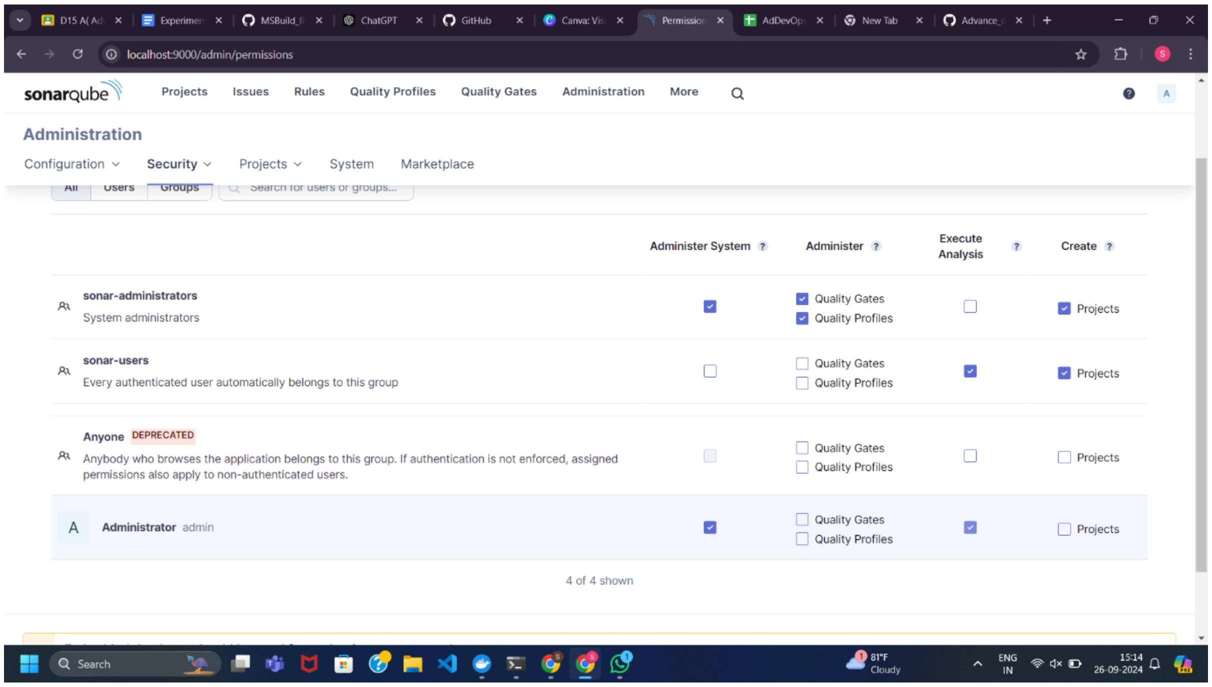
Analysis properties ?

```
sonar.projectKey=Sonarqube-test
sonar.sources=.
sonar.host.url=http://localhost:9000
sonar.login=admin
sonar.password=
```

Additional arguments ?

JVM Options ?

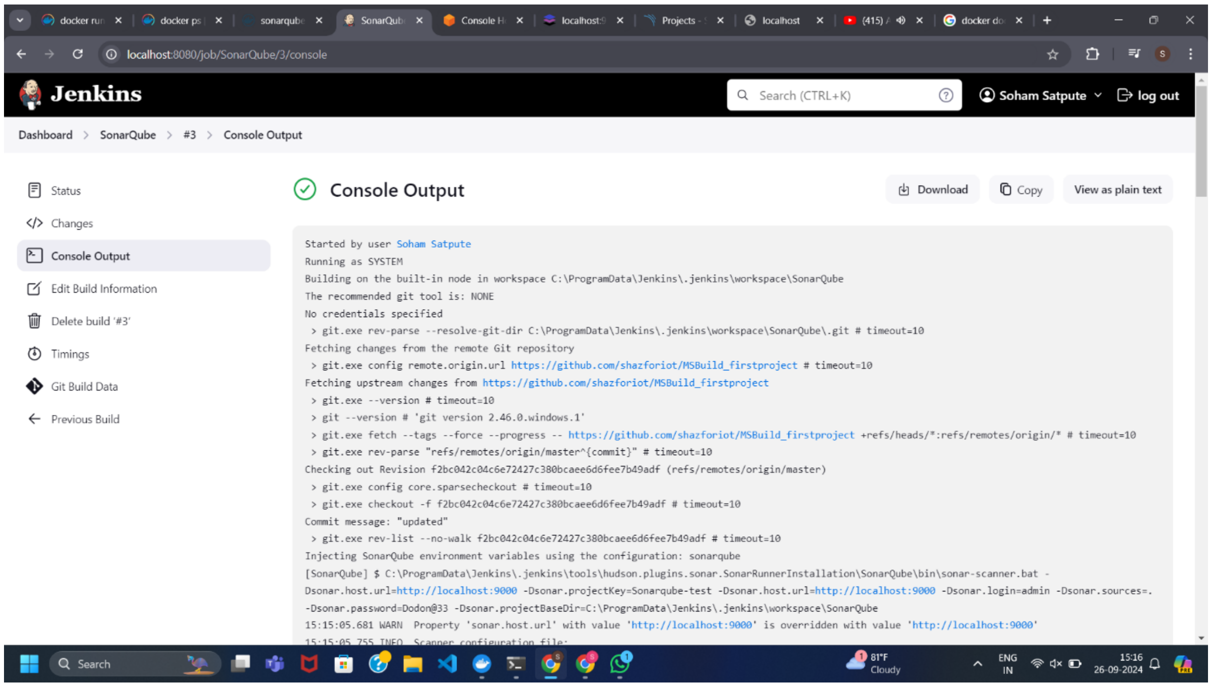
11. Go to http://localhost:9000/<user_name>/permissions and allow Execute Permissions to the Admin user



	Administer System	Administer	Execute Analysis	Create
sonar-administrators System administrators	✓	✓ Quality Gates ✓ Quality Profiles	☐	✓ Projects
sonar-users Every authenticated user automatically belongs to this group	☐	☐ Quality Gates ☐ Quality Profiles	✓	✓ Projects
Anyone DEPRECATED Anybody who browses the application belongs to this group. If authentication is not enforced, assigned permissions also apply to non-authenticated users.	☐	☐ Quality Gates ☐ Quality Profiles	☐	☐ Projects
Administrator admin	✓	☐ Quality Gates ☐ Quality Profiles	✓	☐ Projects

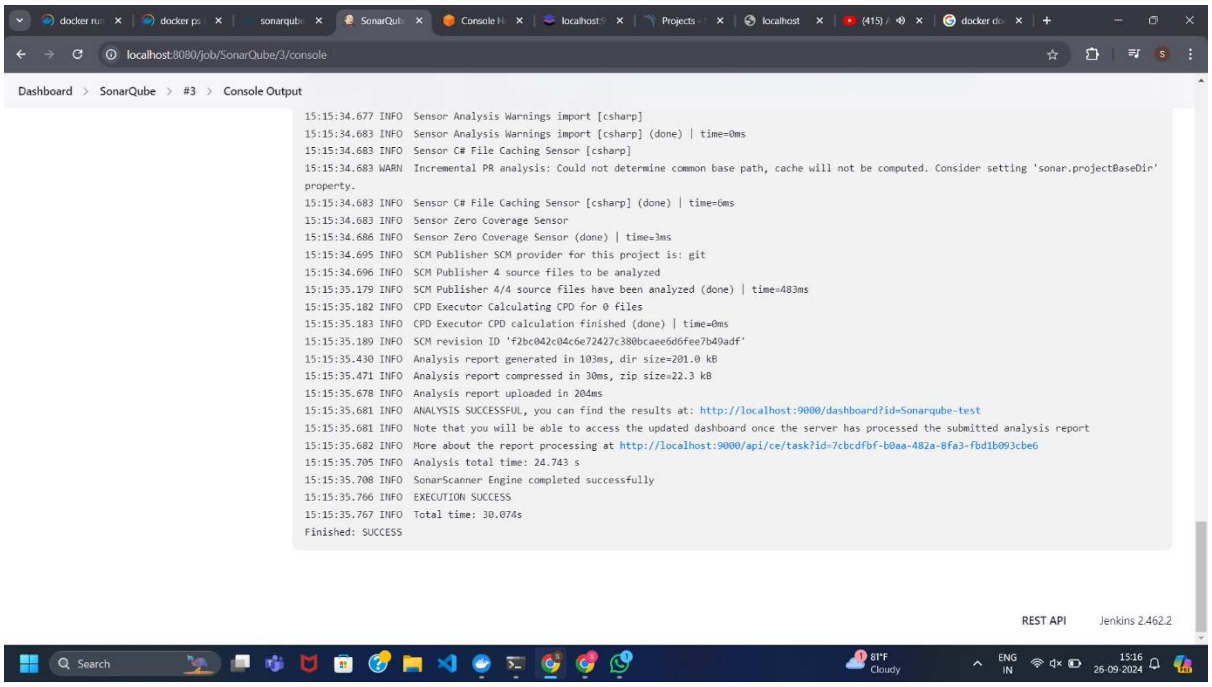
4 of 4 shown

12.Check the console Output



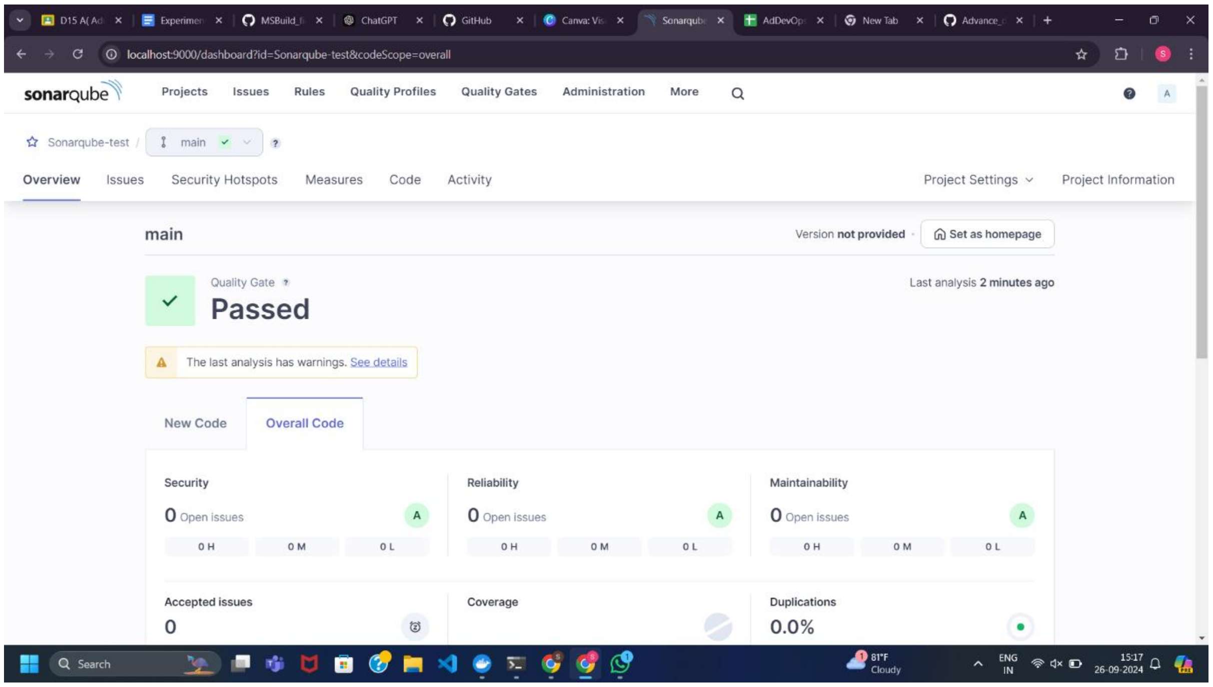
Console Output

```
Started by user Soham Satpute
Running as SYSTEM
Building on the built-in node in workspace C:\ProgramData\Jenkins\.jenkins\workspace\SonarQube
The recommended git tool is: NONE
No credentials specified
 > git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\.jenkins\workspace\SonarQube\.git # timeout=10
Fetching changes from the remote Git repository
 > git.exe config remote.origin.url https://github.com/shazforiot/MSBuild_firstproject # timeout=10
Fetching upstream changes from https://github.com/shazforiot/MSBuild_firstproject
 > git.exe --version # timeout=10
 > git --version # 'git version 2.46.0.windows.1'
 > git.exe fetch --tags --force --progress -- https://github.com/shazforiot/MSBuild_firstproject +refs/heads/*:refs/remotes/origin/* # timeout=10
 > git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision f2bc042c04c6e72427c380bcaee6d6fee7b49adf (refs/remotes/origin/master)
 > git.exe config core.sparsecheckout # timeout=10
 > git.exe checkout -f f2bc042c04c6e72427c380bcaee6d6fee7b49adf # timeout=10
Commit message: "updated"
 > git.exe rev-list --no-walk f2bc042c04c6e72427c380bcaee6d6fee7b49adf # timeout=10
Injecting SonarQube environment variables using the configuration: sonarqube
[SonarQube] $ C:\ProgramData\Jenkins\.jenkins\tools\hudson.plugins.sonar.SonarRunnerInstallation\SonarQube\bin\sonar-scanner.bat -
Dsonar.host.url=http://localhost:9000 -Dsonar.projectKey=Sonarqube-test -Dsonar.host.url=http://localhost:9000 -Dsonar.login=admin -Dsonar.sources=.
-Dsonar.password=Dodon@33 -Dsonar.projectBaseDir=C:\ProgramData\Jenkins\.jenkins\workspace\SonarQube
15:15:05.681 WARN  Property 'sonar.host.url' with value 'http://localhost:9000' is overridden with value 'http://localhost:9000'
15:15:05.755 INFO  Scanner configuration file:
```


localhost:8080/job/SonarQube/3/console
Dashboard > SonarQube > #3 > Console Output

```
15:15:34.677 INFO  Sensor Analysis Warnings import [csharp]
15:15:34.683 INFO  Sensor Analysis Warnings import [csharp] (done) | time=0ms
15:15:34.683 INFO  Sensor C# File Caching Sensor [csharp]
15:15:34.683 WARN  Incremental PR analysis: Could not determine common base path, cache will not be computed. Consider setting 'sonar.projectBaseDir'
property.
15:15:34.683 INFO  Sensor C# File Caching Sensor [csharp] (done) | time=6ms
15:15:34.683 INFO  Sensor Zero Coverage Sensor
15:15:34.686 INFO  Sensor Zero Coverage Sensor (done) | time=3ms
15:15:34.695 INFO  SCM Publisher SCM provider for this project is: git
15:15:34.696 INFO  SCM Publisher 4 source files to be analyzed
15:15:35.179 INFO  SCM Publisher 4/4 source files have been analyzed (done) | time=483ms
15:15:35.182 INFO  CPD Executor Calculating CPD for 0 files
15:15:35.183 INFO  CPD Executor CPD calculation finished (done) | time=0ms
15:15:35.189 INFO  SCM revision ID 'f2bc042c04c6e72427c380bcaee6d6fee7b49adf'
15:15:35.430 INFO  Analysis report generated in 103ms, dir size=201.0 kB
15:15:35.471 INFO  Analysis report compressed in 30ms, zip size=22.3 kB
15:15:35.678 INFO  Analysis report uploaded in 204ms
15:15:35.681 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=Sonarqube-test
15:15:35.681 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
15:15:35.682 INFO  More about the report processing at http://localhost:9000/api/ce/task?id=7cbcdfbf-b0aa-482a-8fa3-fbd1b093cbe6
15:15:35.705 INFO  Analysis total time: 24.743 s
15:15:35.708 INFO  SonarScanner Engine completed successfully
15:15:35.766 INFO  EXECUTION SUCCESS
15:15:35.767 INFO  Total time: 30.074s
Finished: SUCCESS
```

13.Once the build is complete, check project on SonarQube



main

Version not provided
Set as homepage

Quality Gate
Passed

Last analysis 2 minutes ago

The last analysis has warnings. See details

New Code | Overall Code

Security	Reliability	Maintainability
0 Open issues A	0 Open issues A	0 Open issues A
0 H 0 M 0 L	0 H 0 M 0 L	0 H 0 M 0 L
Accepted issues 0	Coverage	Duplications 0.0%

In this way, we have integrated Jenkins with SonarQube for SAST.