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

Run docker -v command. Use this command to check if docker is installed and running on your system

```
C:\Users\Aditya>docker -v
Docker version 27.2.0, build 3ab4256
```

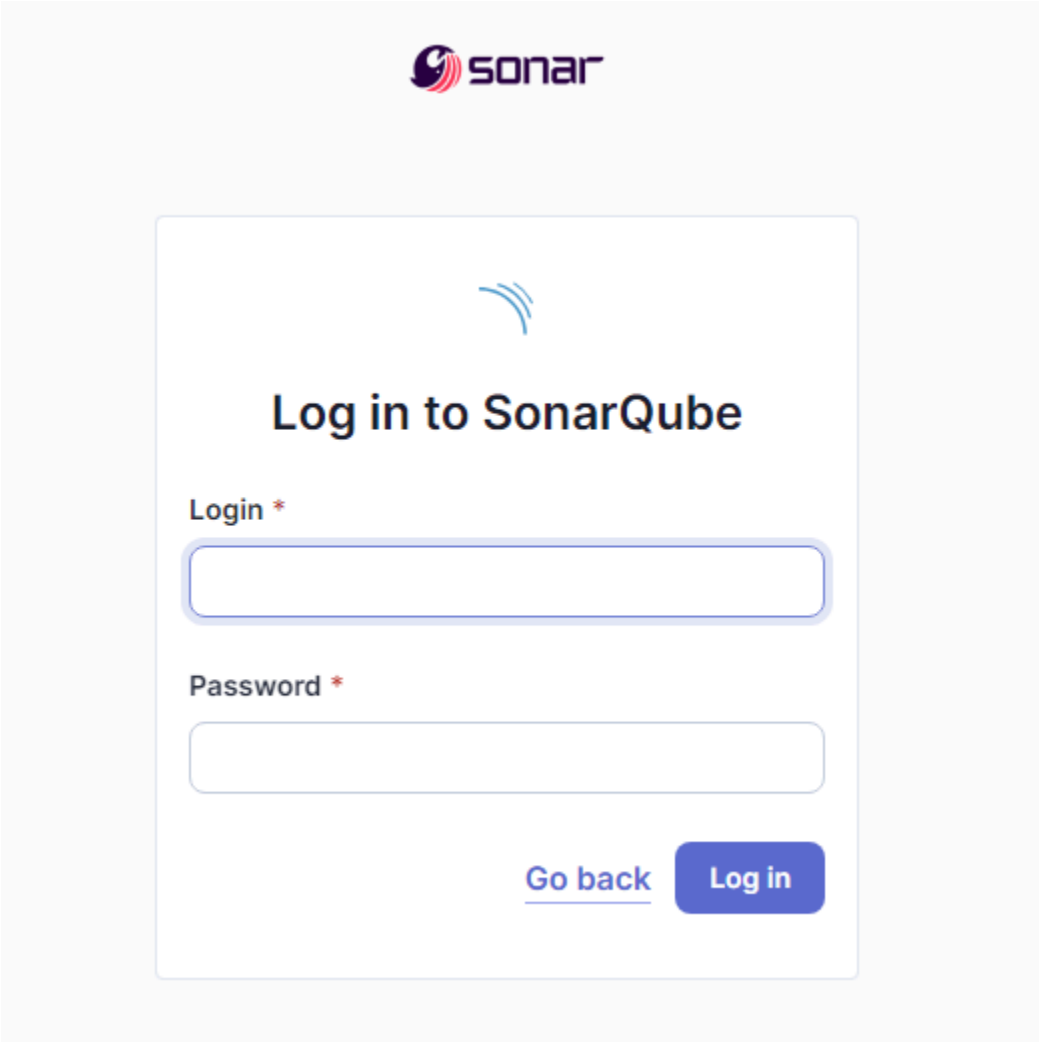
docker pull sonarqube This command helps you to install an image of SonarQube that can be used on the local system without actually installing the SonarQube installer.

```
:\Users\Aditya>docker pull sonarqube
Using default tag: latest
atest: Pulling from library/sonarqube
4f4fb700ef54: Download complete
d819c9b5ead: Download complete
30338217a4ab: Download complete
7478e0ac0f23: Download complete
90a925ab929a: Download complete
7b87d6fa783d: Download complete
1a5fd5c7e184: Download complete
7d9a34308537: Download complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
docker.io/library/sonarqube:latest
```

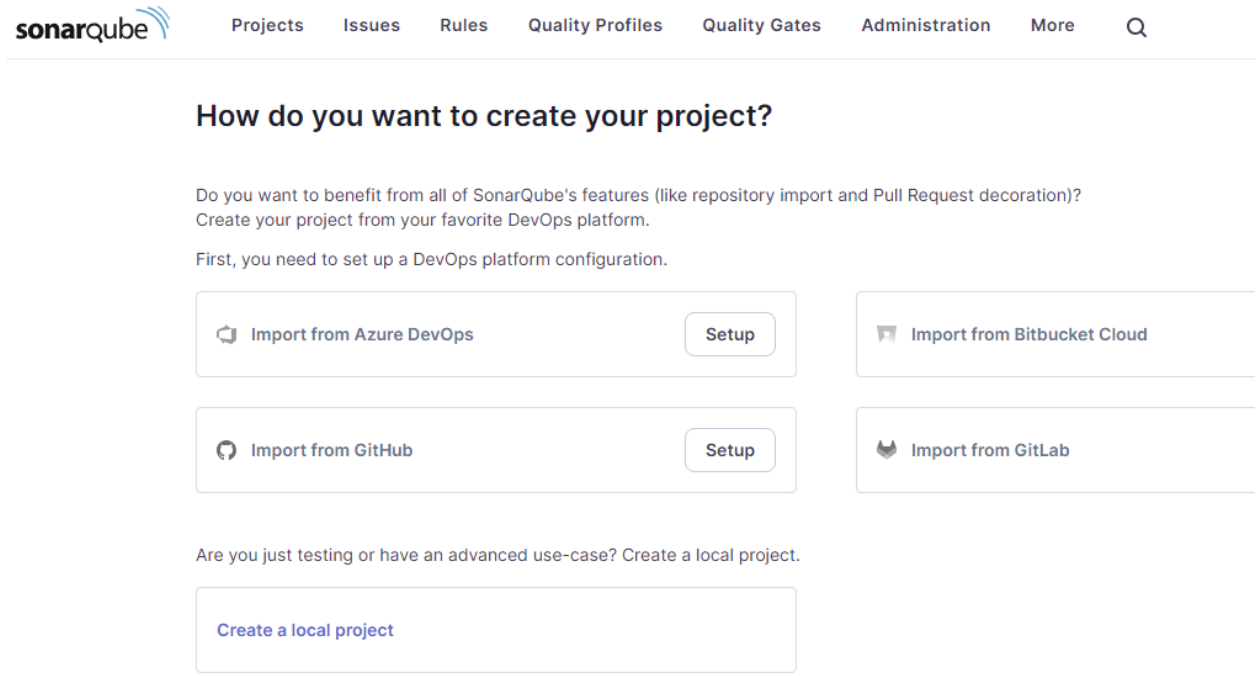
Run SonarQube image: docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest This command will run the SonarQube image that was just installed using docker

```
C:\Users\Aditya>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
102a6e51b67968db1df41bc8c6c3ce068f11506acadcbab2d306470aede30908
```

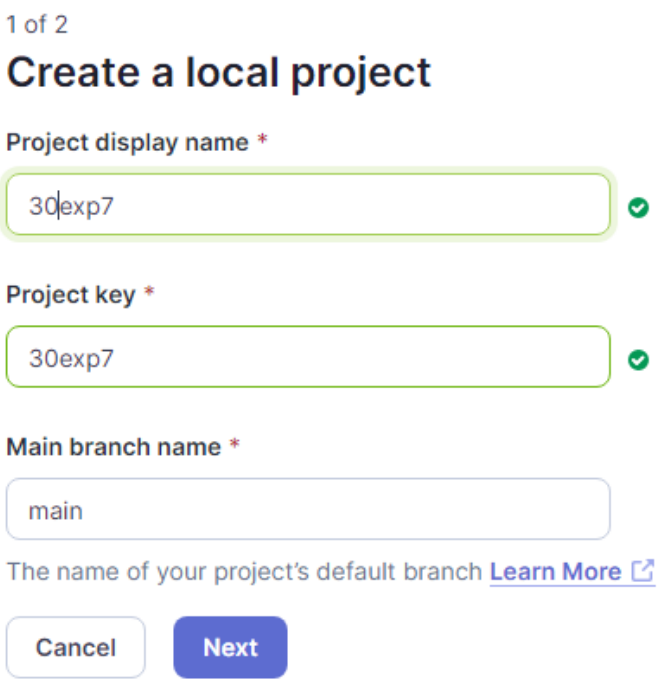
Once the SonarQube image is started, you can go to http://localhost:9000 to find the SonarQube that has started



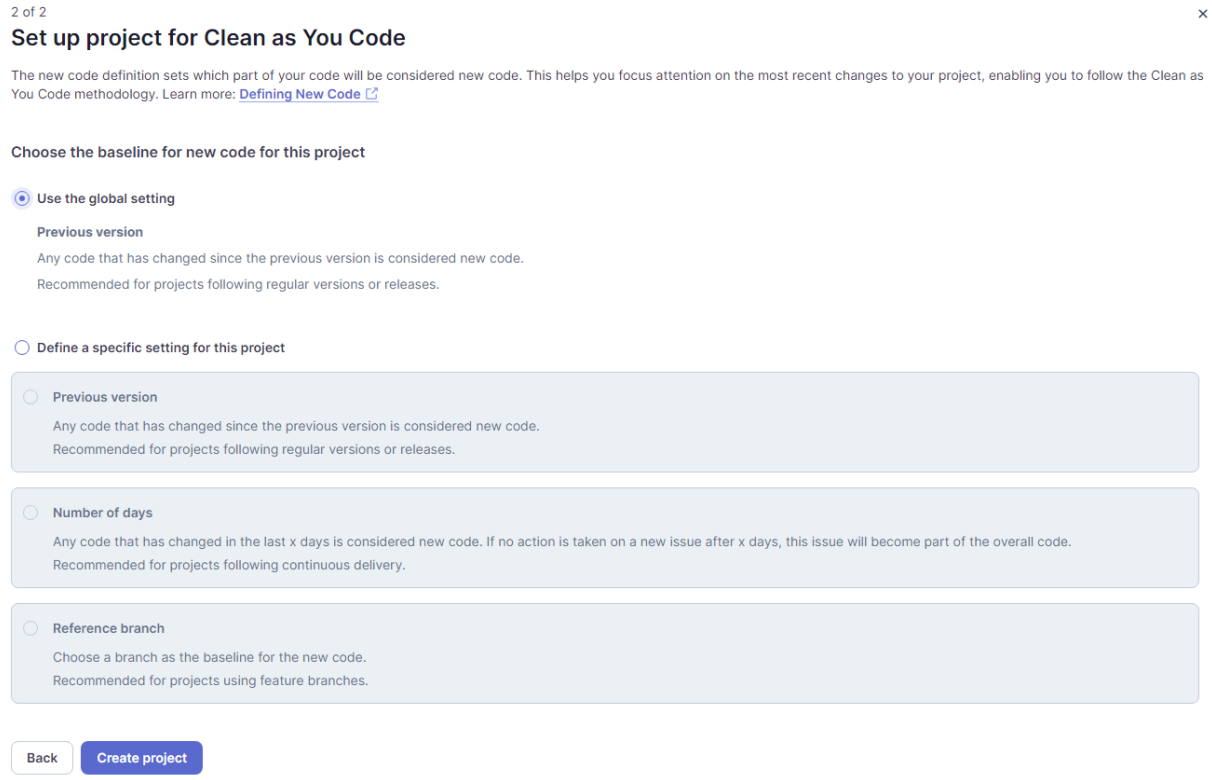
After changing the password, you will be directed to this screen. Click on Create a Local Project.



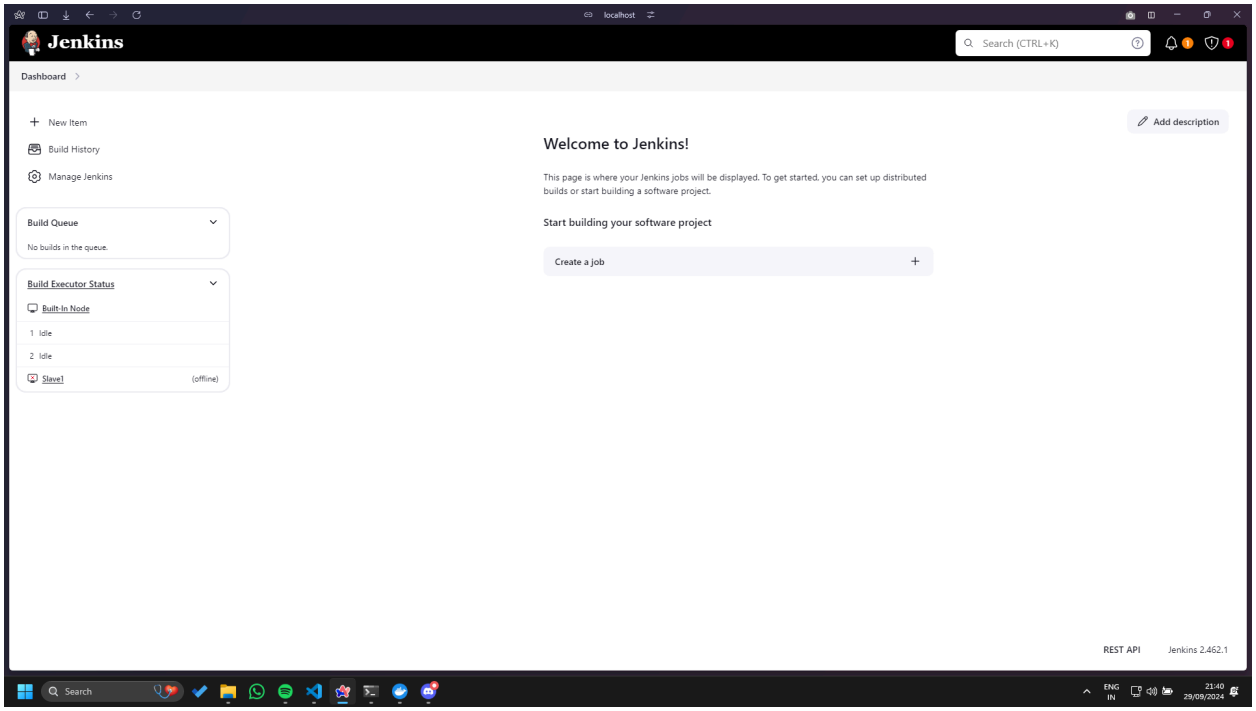
Give the project a display name and project key



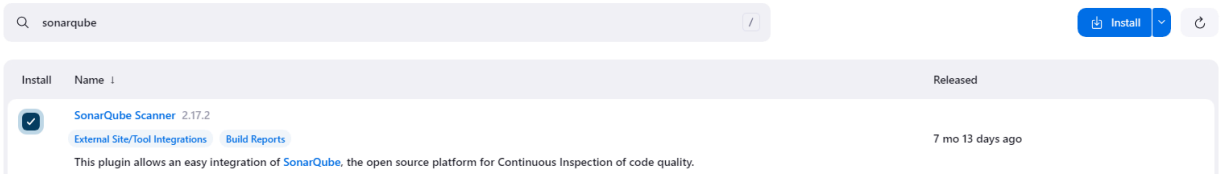
Set up the project as required and click on create.



Open Jenkins on whichever port it is installed. (http://loaclhost:).



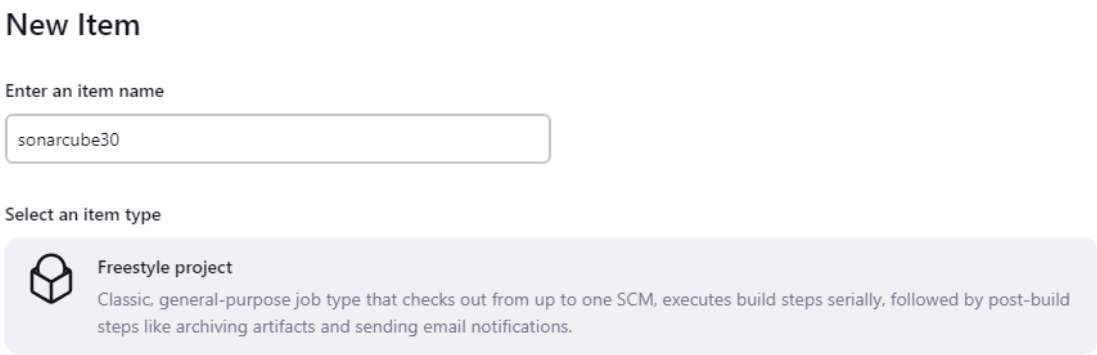
Go to manage jenkins → Search for Sonarqube Scanner for Jenkins and install it.



Now, go to Manage Jenkins → System. Under Sonarqube servers, add a server. Add server authentication token if needed.

Go to Manage Jenkins → Tools. Go to SonarQube scanner, choose the latest configuration and choose install automatically

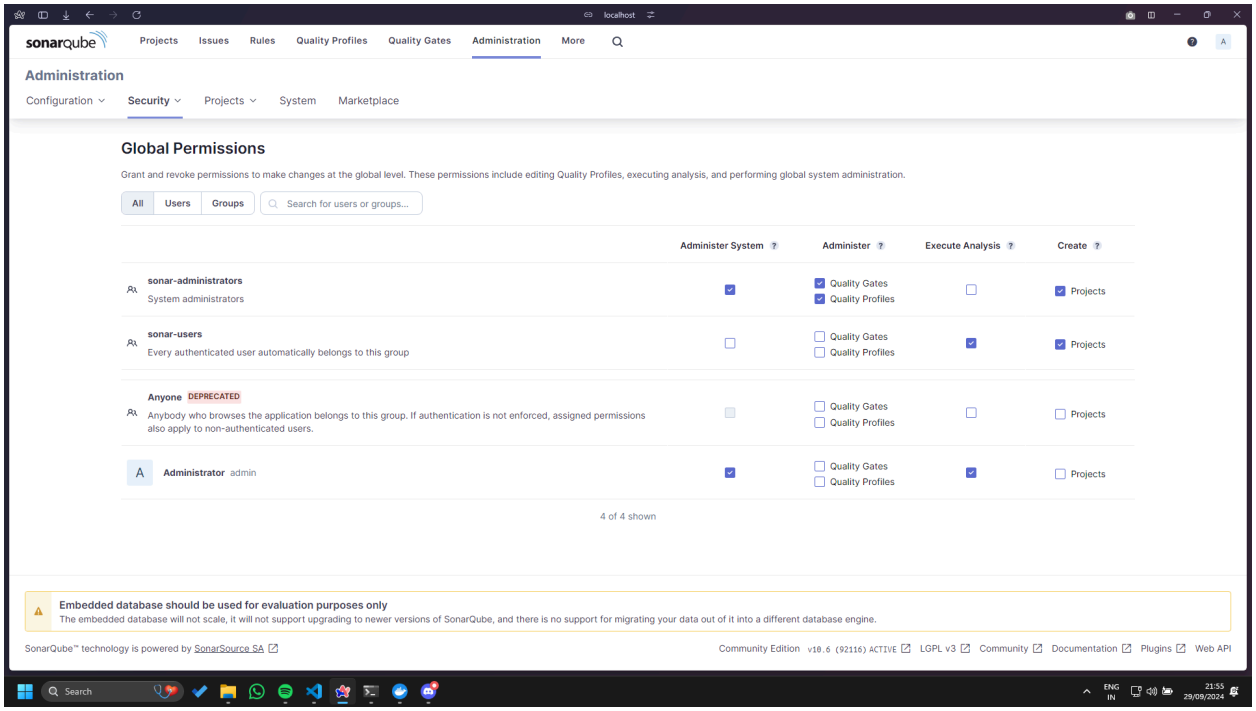
After configuration, create a New Item → choose a freestyle project.



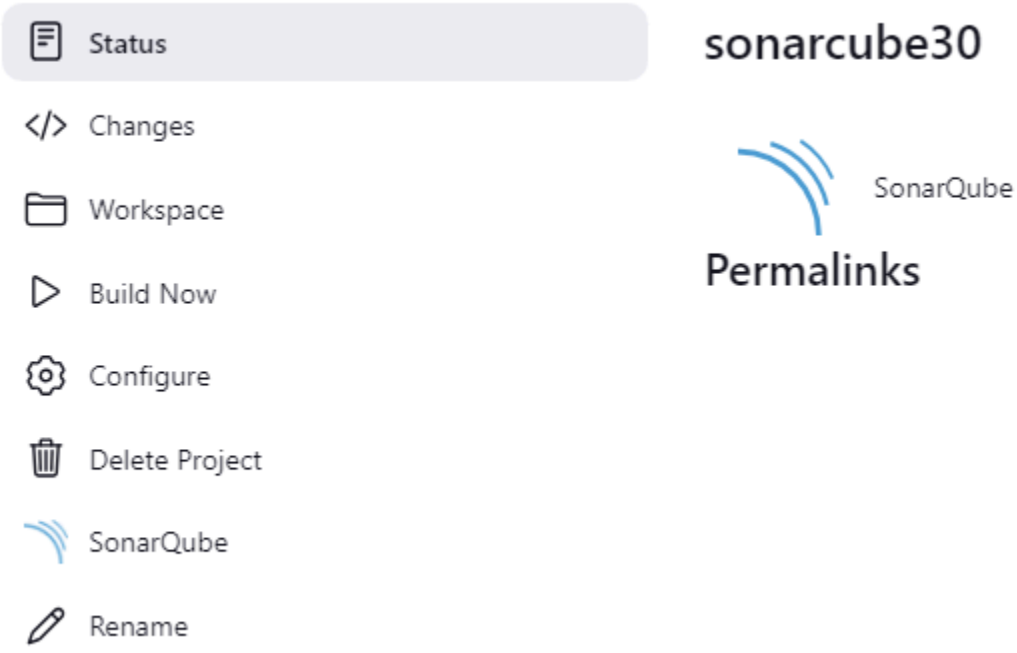
Use this github repository in Source Code Management.
https://github.com/shazforiot/MSBuild_firstproject It is a sample hello-world project with no vulnerabilities.

Under Build Steps, enter Sonarqube Scanner, enter these Analysis properties. Mention the SonarQube Project Key, Login, Password, Source path and Host URL.

Now, you need to grant the locl user (here admin user) permissions to Execute the Analysis stage on SoanrQube. For this, go to http://loaclhost:9000/admin/permissions and check the 'Execute Analysis' checkbox under Administrator.



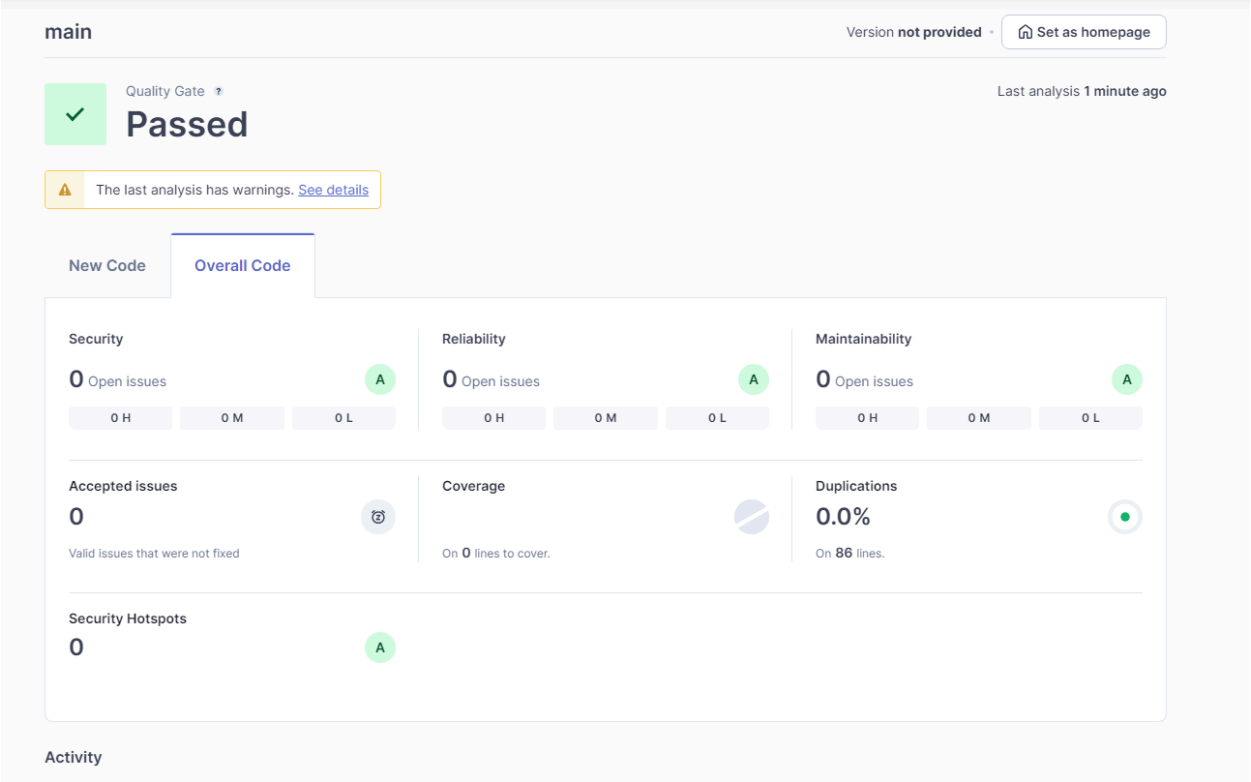
Go back to jenkins. Go to the job you had just built and click on Build Now.



Check the console output

```
22:04:00.599 INFO  SonarScanner Engine completed successfully
22:04:00.665 INFO  EXECUTION SUCCESS
22:04:00.667 INFO  Total time: 16.886s
Finished: SUCCESS
```

Once the build is complete, go back to SonarQube and check the project linked.



Conclusion: In this experiment, we have learned how to perform Jenkins SAST using SonarQube. For this, we used a docker image of SonarQube so as to not install it locally on our system. After installing the required configurations on Jenkins, using a coe from a gihub repository, we analyze its code using SonarQube. Once we build the project, we can see that SonarQube project displays that the code has no errors.