Name: Alok Yadav Div: D15C Roll
No.: 59

EXPERIMENT NO. 8

Aim: Create a Jenkins CI/CD Pipeline with SonarQube / GitLab Integration to perform a static
analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web /Java / Python application.

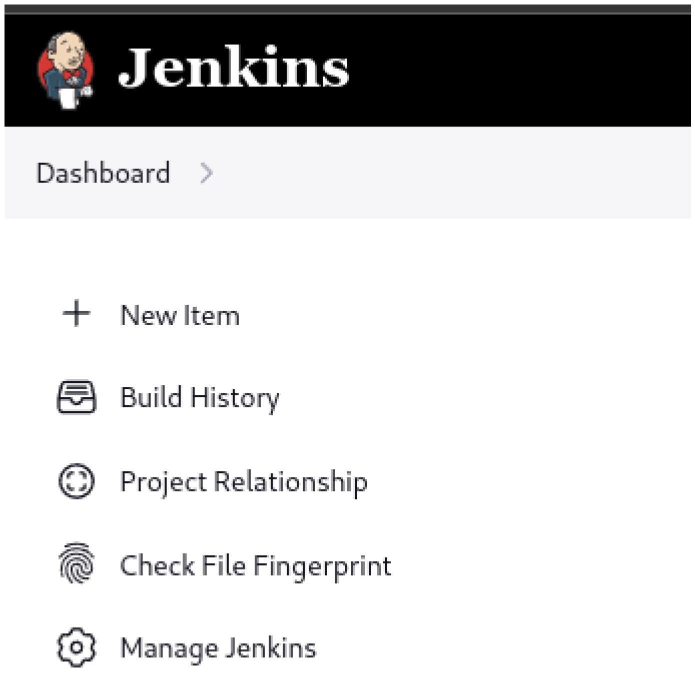
Integrating Jenkins with SonarQube:

Prerequisites:

● Jenkins installed
● Docker Installed (for SonarQube)
● SonarQube Docker Image

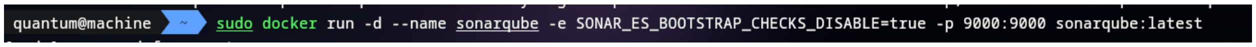
Steps to create a Jenkins CI/CD Pipeline and use SonarQube to perform SAST

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



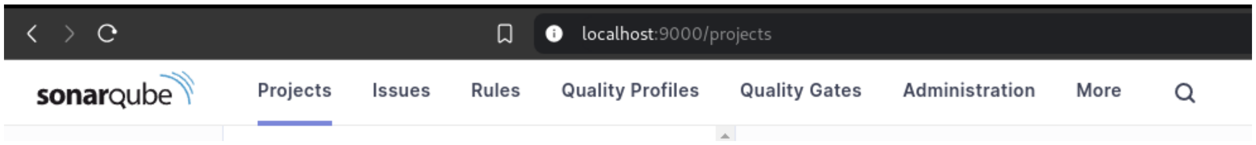
2. Run SonarQube in a Docker container using this command

Name: Alok Yadav Div: D15C Roll No.: 59



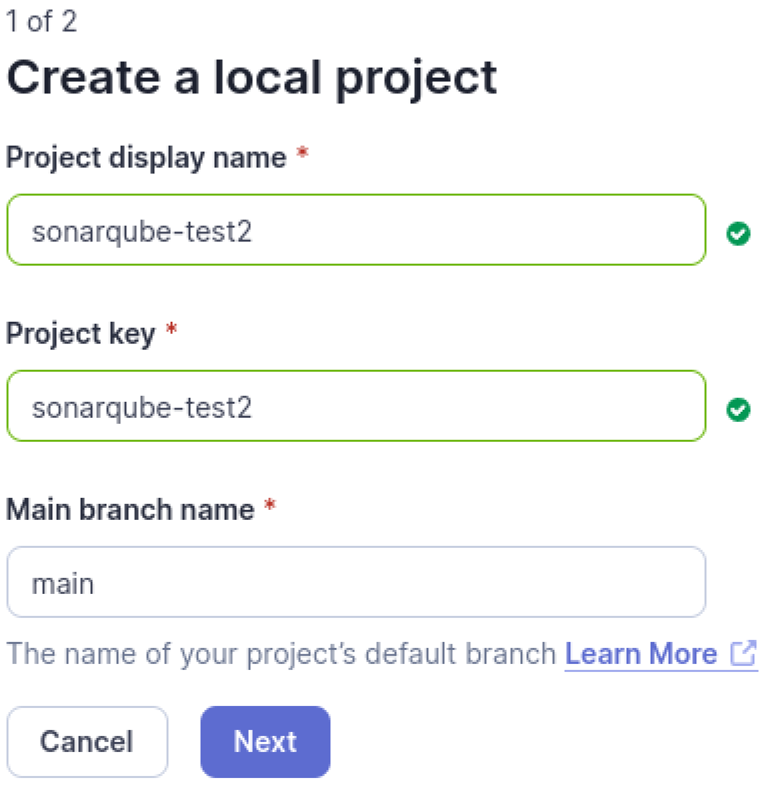
```
quantum@machine ~ sudo docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
```

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



4. Login to SonarQube using your username and password

5. Create a manual project in SonarQube with the name sonarqube-test2



1 of 2

Create a local project

Project display name *: sonarqube-test2

Project key *: sonarqube-test2

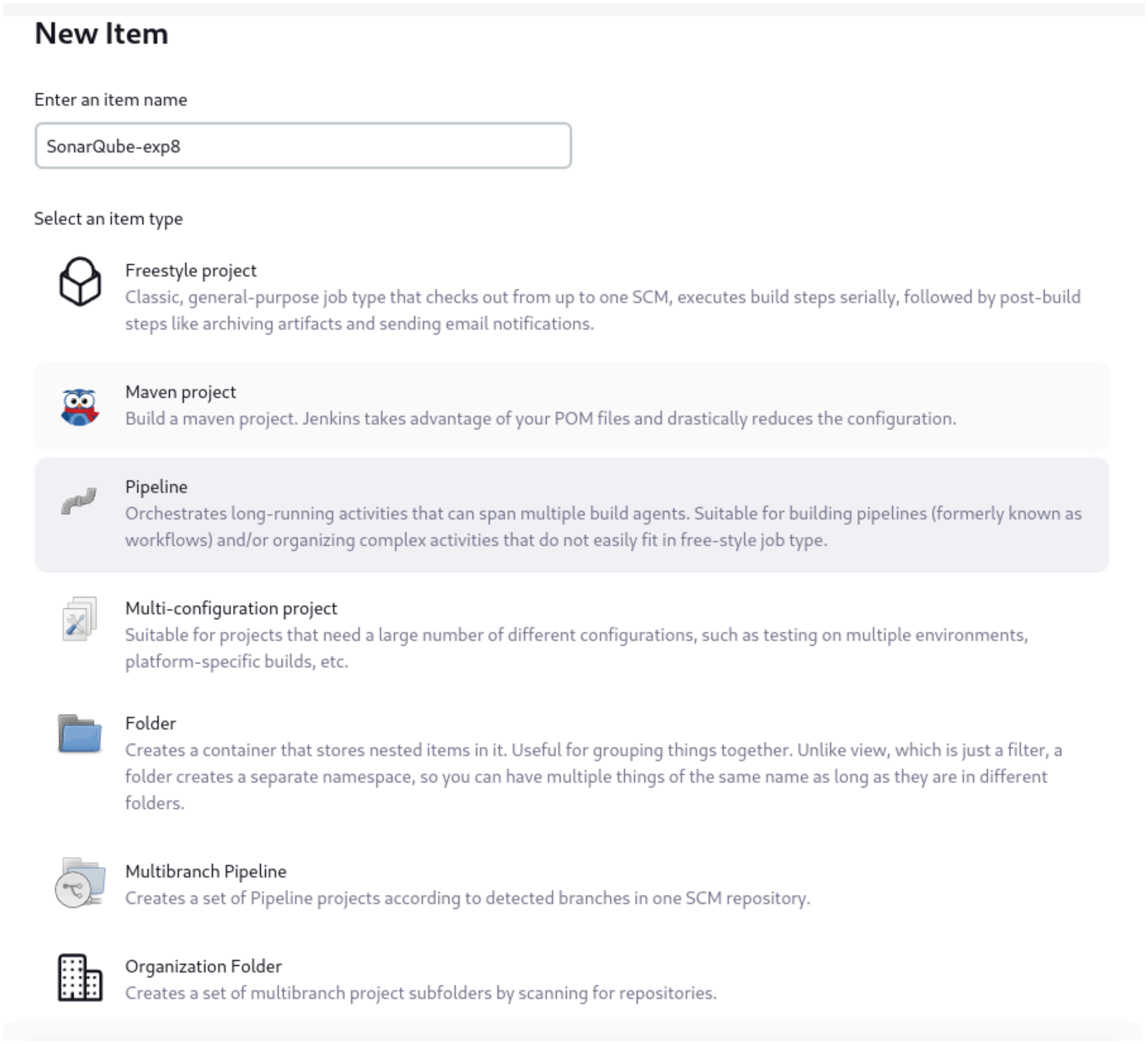
Main branch name *: main

The name of your project's default branch Learn More

Setup the project and come back to Jenkins Dashboard.

6. Create a New Item in Jenkins, choose **Pipeline**.

Name: Alok Yadav Div: D15C Roll No.: 59


New Item

Enter an item name

SonarQube-exp8

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.

Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

Multibranch Pipeline
Creates a set of Pipeline projects according to detected branches in one SCM repository.

Organization Folder
Creates a set of multibranch project subfolders by scanning for repositories.

7. Under Pipeline Script, enter the following -

```
node {
stage('Cloning the GitHub Repo') {
git 'https://github.com/shazforiot/GOL.git'
}
stage('SonarQube analysis') {
withSonarQubeEnv('sonarqube') {
sh "<PATH_TO_SONARQUBE_FOLDER>//bin//sonar-scanner \
-D sonar.login=<SonarQube_USERNAME> \
-D sonar.password=<SonarQube_PASSWORD> \
-D sonar.projectKey=<Project_KEY> \
-D sonar.exclusions=vendor/**,resources/**,**/*.java \
-D sonar.host.url=http://127.0.0.1:9000/"
```

```
        }
        }
        }
```

It is a java sample project which has a lot of repetitions and issues that will be detected by
SonarQube.

8. Install sonar-scanner

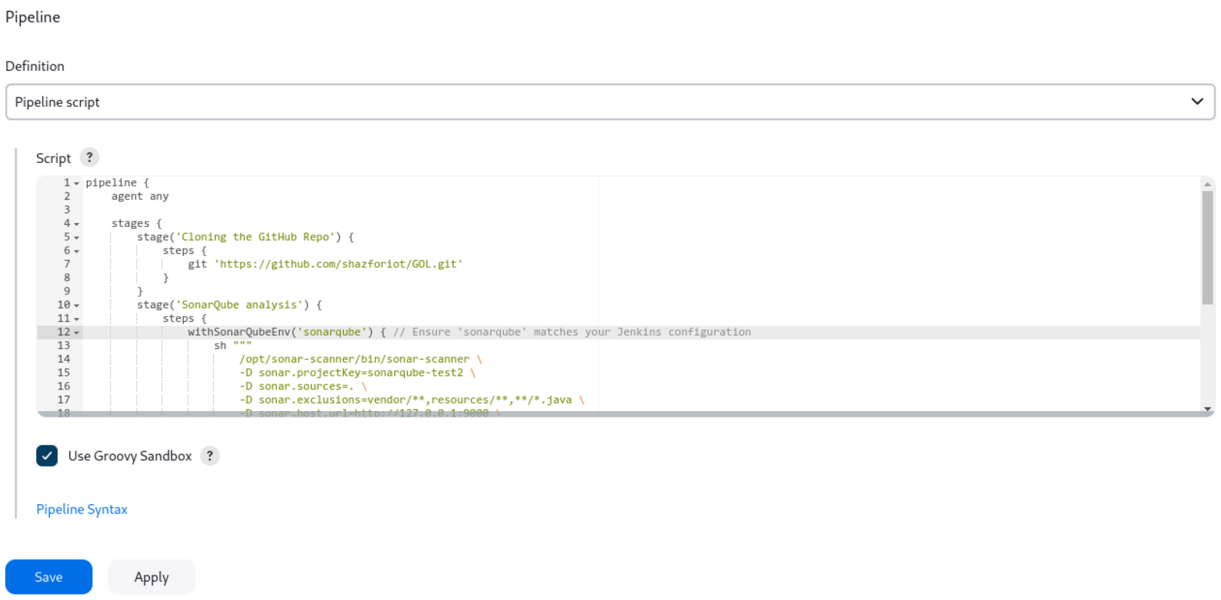
Now we need to install **sonar-scanner** binary to perform code analysis
To do so, go to
https://binaries.sonarsource.com/Distribution/sonar-scanner-cli/sonar-scanner-cli-6.2.0.4584-linux-x64.zip for linux OS
(https://binaries.sonarsource.com/Distribution/sonar-scanner-cli/sonar-scanner-cli-6.2.0.4584-windows-x64.zip for windows OS)
You will be prompted to download the zip file, download it and extract it and copy the path (absolute path) to <ROOT_DIRECTORY>/bin/sonar-scanner in my case it is /opt/sonar-scanner/bin/sonar-scanner (For linux)
For windows path would be
C:\\Users\<USER_NAME>\Downloads\sonar-scanner-cli-6.2.0.4584-windows-x64\bin\sonar-scanner

Now we need to update the required details in the pipeline script as :

```
pipeline {
   agent any
   stages {
      stage('Cloning the GitHub Repo') {
         steps {
            git 'https://github.com/shazforiot/GOL.git'
         }
      }
      stage('SonarQube analysis') {
         steps {
            withSonarQubeEnv('sonarqube') {configuration
               sh """
                  /opt/sonar-scanner/bin/sonar-scanner \   //replace with your actual path
to sonar-scanner
                  -D sonar.projectKey=sonarqube-test2 \
                  -D sonar.sources=. \
                  -D sonar.exclusions=vendor/**,resources/**,**/*.java \
```

Name: Alok Yadav Div: D15C Roll No.: 59

```
                -D sonar.host.url=http://127.0.0.1:9000 \
                -D sonar.login=admin \
                -D sonar.password=admin1
              """
            }
          }
        }
      }
```



Pipeline

Definition

Pipeline script

Script ?

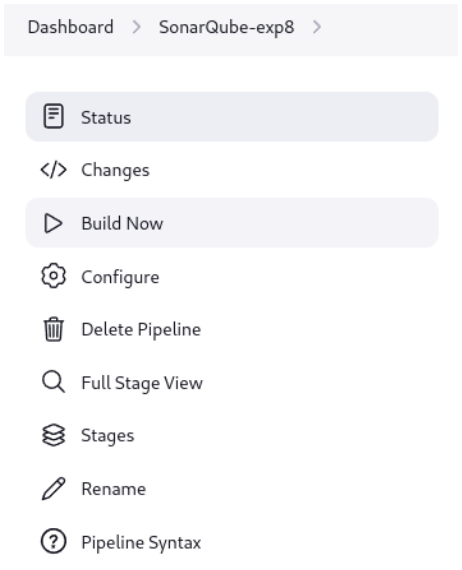
```
pipeline {
    agent any

    stages {
        stage('Cloning the GitHub Repo') {
            steps {
                git 'https://github.com/shazforiot/GOL.git'
            }
        }
        stage('SonarQube analysis') {
            steps {
                withSonarQubeEnv('sonarqube') { // Ensure 'sonarqube' matches your Jenkins configuration
                    sh """
                        /opt/sonar-scanner/bin/sonar-scanner \
                        -D sonar.projectKey=sonarqube-test2 \
                        -D sonar.sources=. \
                        -D sonar.exclusions=vendor/**,resources/**,**/*.java \
                        -D sonar.host.url=http://127.0.0.1:9000 \
```

✓ Use Groovy Sandbox ?

Pipeline Syntax

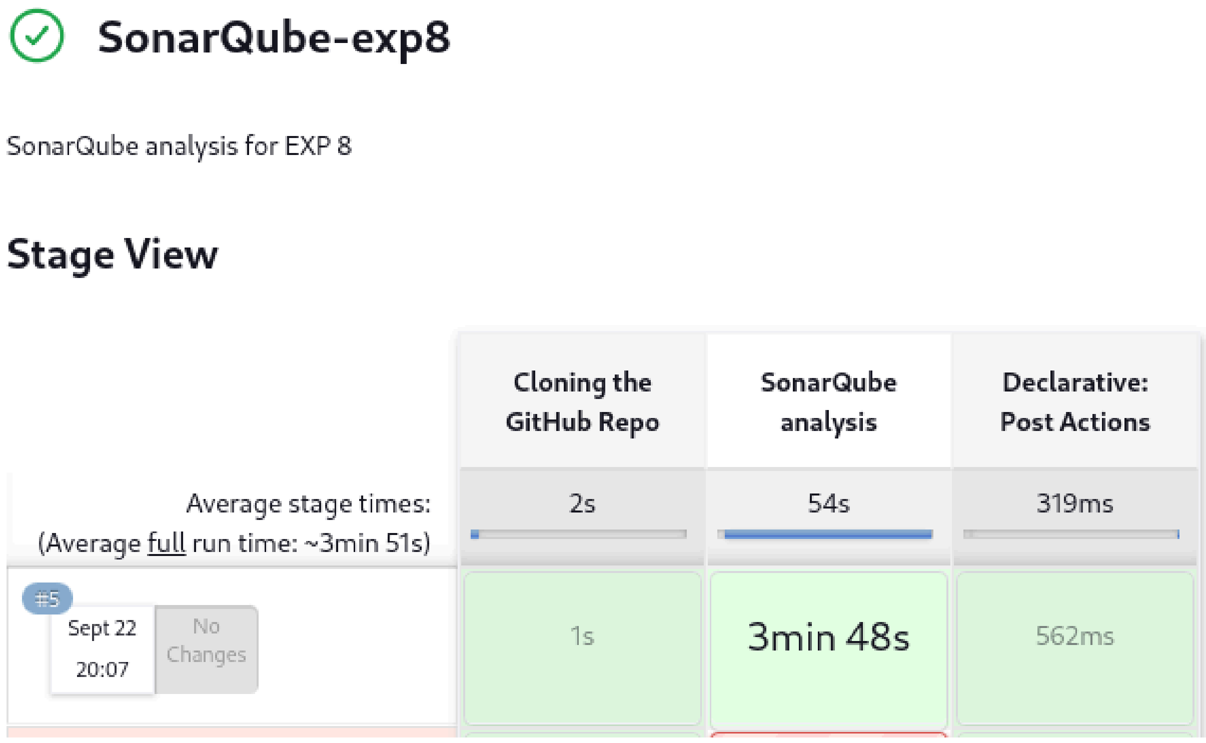
Save Apply

9. Run the build



Name: Alok Yadav Div: D15C Roll No.: 59

Check the status of Build



SonarQube-exp8

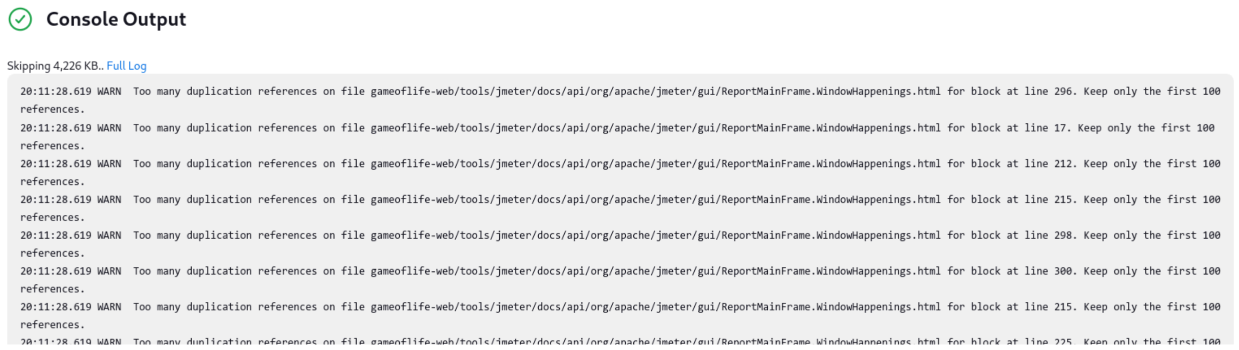
SonarQube analysis for EXP 8

Stage View

	Cloning the GitHub Repo	SonarQube analysis	Declarative: Post Actions
Average stage times: (Average full run time: ~3min 51s)	2s	54s	319ms
#5 Sept 22 20:07 No Changes	1s	3min 48s	562ms

As we can see the SonarQube analysis is completed

10. Check the console output once the build is complete.

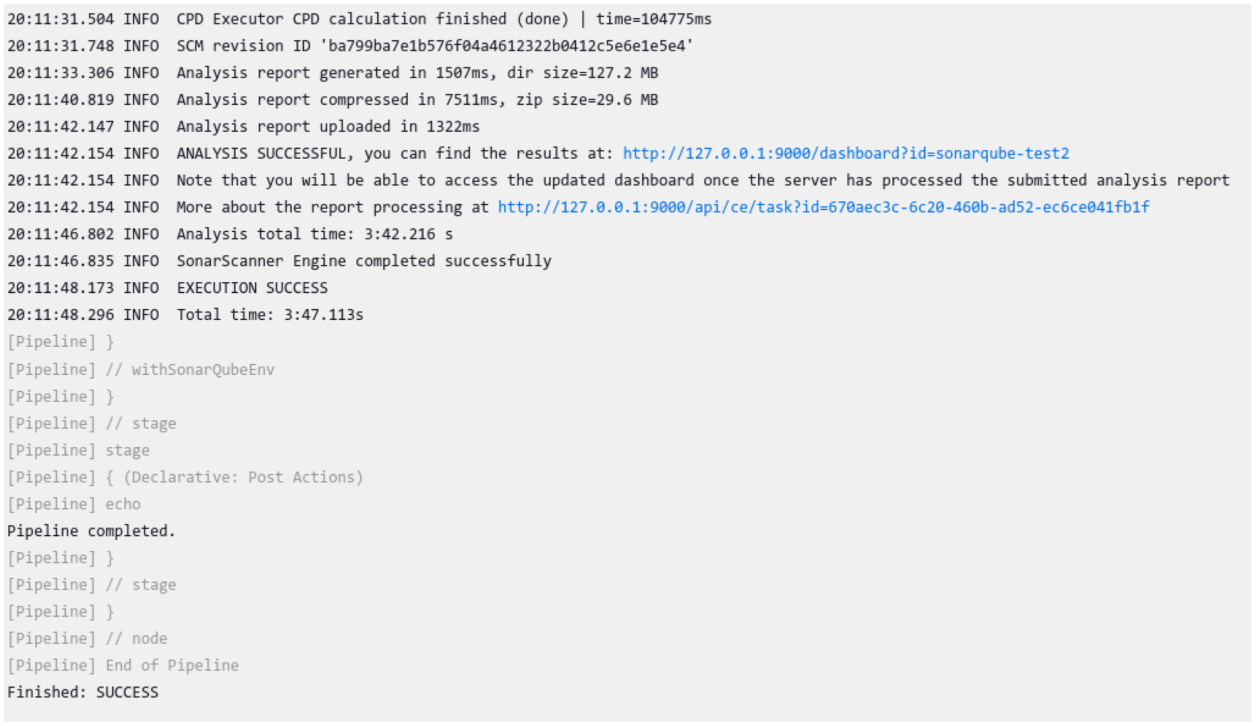


Console Output

Skipping 4,226 KB.. Full Log

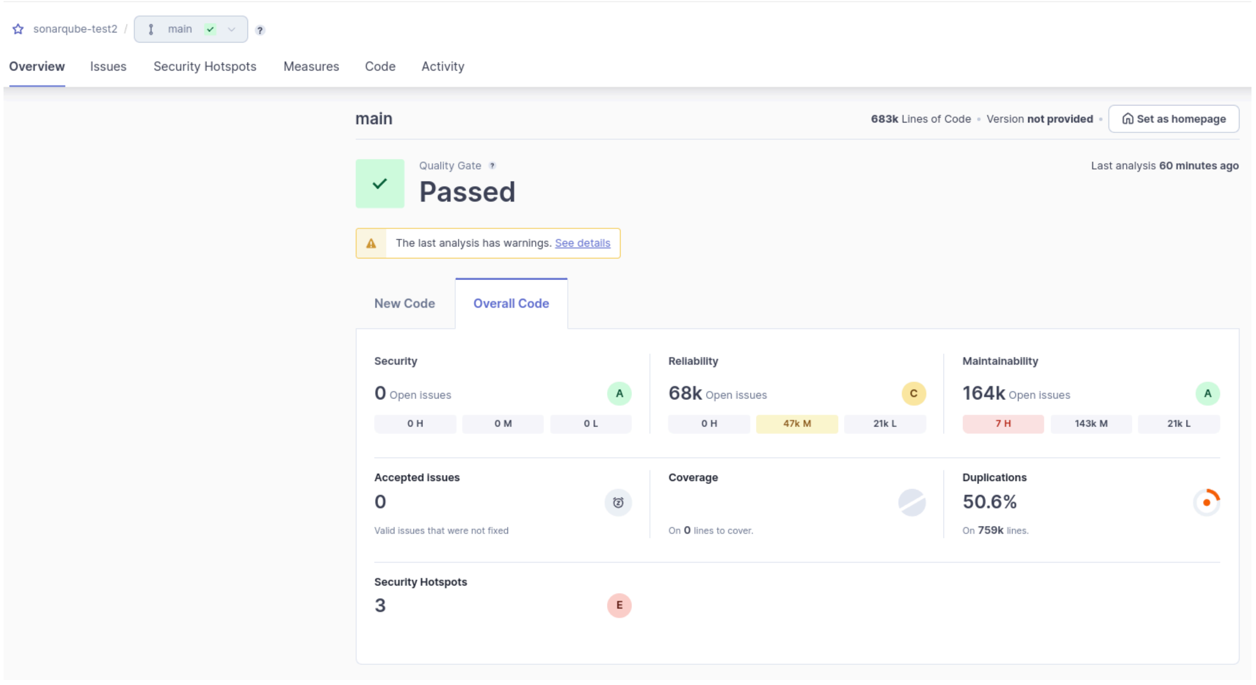
```
20:11:28.619 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/ReportMainFrame.WindowHappenings.html for block at line 296. Keep only the first 100
references.
20:11:28.619 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/ReportMainFrame.WindowHappenings.html for block at line 17. Keep only the first 100
references.
20:11:28.619 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/ReportMainFrame.WindowHappenings.html for block at line 212. Keep only the first 100
references.
20:11:28.619 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/ReportMainFrame.WindowHappenings.html for block at line 215. Keep only the first 100
references.
20:11:28.619 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/ReportMainFrame.WindowHappenings.html for block at line 298. Keep only the first 100
references.
20:11:28.619 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/ReportMainFrame.WindowHappenings.html for block at line 300. Keep only the first 100
references.
20:11:28.619 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/ReportMainFrame.WindowHappenings.html for block at line 215. Keep only the first 100
references.
20:11:28.619 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/ReportMainFrame.WindowHappenings.html for block at line 225. Keep only the first 100
```

Name: Alok Yadav   Div: D15C   Roll No.: 59



```
20:11:31.504 INFO  CPD Executor CPD calculation finished (done) | time=104775ms
20:11:31.748 INFO  SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
20:11:33.306 INFO  Analysis report generated in 1507ms, dir size=127.2 MB
20:11:40.819 INFO  Analysis report compressed in 7511ms, zip size=29.6 MB
20:11:42.147 INFO  Analysis report uploaded in 1322ms
20:11:42.154 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://127.0.0.1:9000/dashboard?id=sonarqube-test2
20:11:42.154 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
20:11:42.154 INFO  More about the report processing at http://127.0.0.1:9000/api/ce/task?id=670aec3c-6c20-460b-ad52-ec6ce041fb1f
20:11:46.802 INFO  Analysis total time: 3:42.216 s
20:11:46.835 INFO  SonarScanner Engine completed successfully
20:11:48.173 INFO  EXECUTION SUCCESS
20:11:48.296 INFO  Total time: 3:47.113s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] stage
[Pipeline] { (Declarative: Post Actions)
[Pipeline] echo
Pipeline completed.
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

11. After that, check the project in SonarQube.



main

683k Lines of Code • Version not provided • Set as homepage

Quality Gate

Passed

Last analysis 60 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
68k Open issues C
0 H | 47k M | 21k L

Maintainability
164k Open issues A
7 H | 143k M | 21k L

Accepted issues
0
Valid issues that were not fixed

Coverage
On 0 lines to cover.

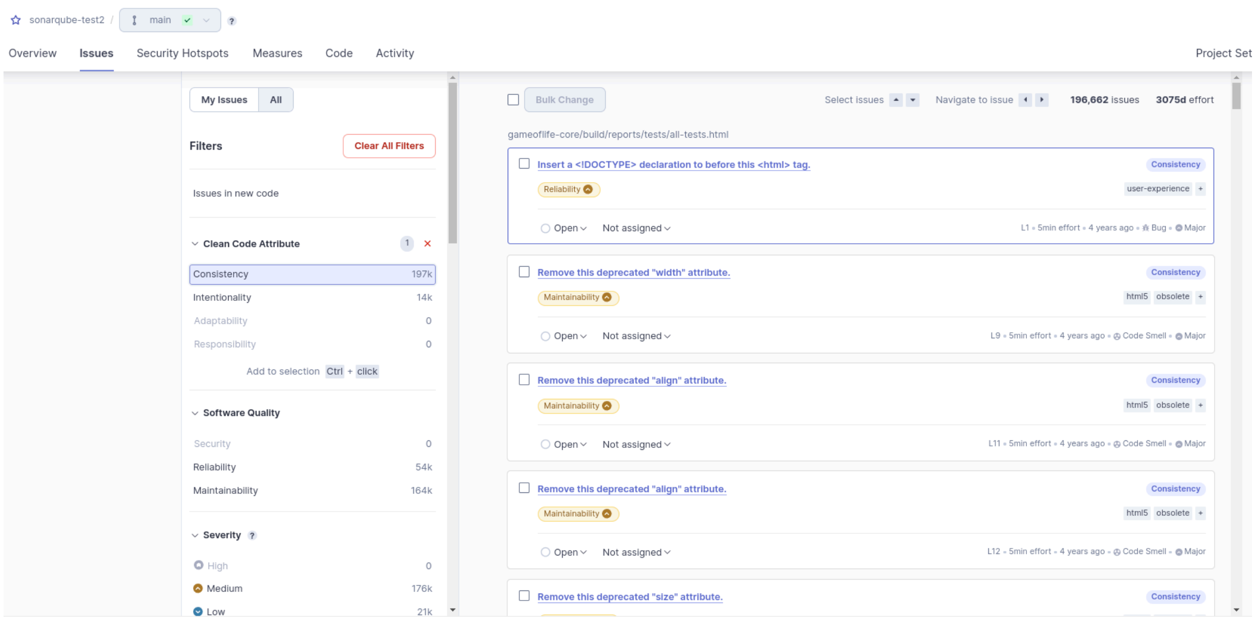
Duplications
50.6%
On 759k lines.

Security Hotspots
3 E

Under different tabs, check all different issues with the code

12. Code Problems-

Name: Alok Yadav Div: D15C Roll No.: 59



sonarqube-test2 / main ?

Overview | Issues | Security Hotspots | Measures | Code | Activity | Project Set

My Issues | All

Filters — Clear All Filters

Issues in new code

Clean Code Attribute 1 ✕

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection Ctrl + click

Software Quality

Security	0
Reliability	54k
Maintainability	164k

Severity ?

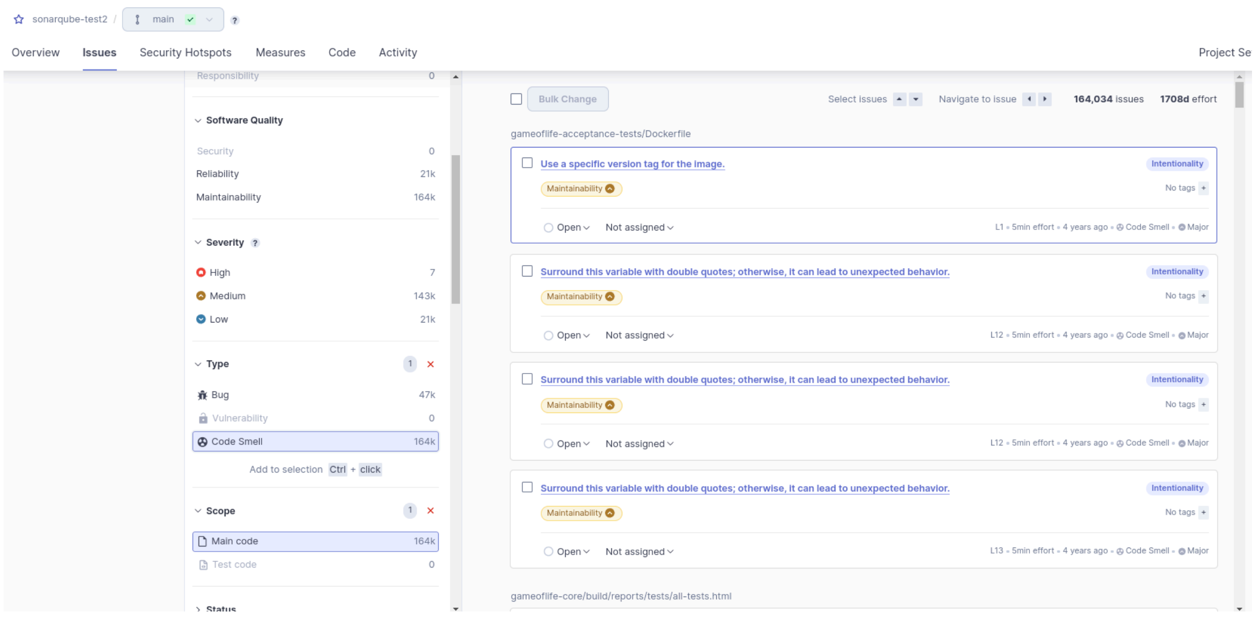
High	0
Medium	176k
Low	21k

Bulk Change — Select issues — Navigate to issue — **196,662** issues **3075d** effort

gameoflife-core/build/reports/tests/all-tests.html

- Insert a <!DOCTYPE> declaration to before this <html> tag. — Consistency — Reliability — user-experience — Open — Not assigned — L1 • 5min effort • 4 years ago • Bug • Major
- Remove this deprecated "width" attribute. — Consistency — Maintainability — html5 obsolete — Open — Not assigned — L9 • 5min effort • 4 years ago • Code Smell • Major
- Remove this deprecated "align" attribute. — Consistency — Maintainability — html5 obsolete — Open — Not assigned — L11 • 5min effort • 4 years ago • Code Smell • Major
- Remove this deprecated "align" attribute. — Consistency — Maintainability — html5 obsolete — Open — Not assigned — L12 • 5min effort • 4 years ago • Code Smell • Major
- Remove this deprecated "size" attribute. — Consistency

Code Smells



sonarqube-test2 / main ?

Overview | Issues | Security Hotspots | Measures | Code | Activity | Project Se

Responsibility 0

Software Quality

Security	0
Reliability	21k
Maintainability	164k

Severity ?

High	7
Medium	143k
Low	21k

Type 1 ✕

Bug	47k
Vulnerability	0
Code Smell	164k

Add to selection Ctrl + click

Scope 1 ✕

Main code	164k
Test code	0

Status

Bulk Change — Select issues — Navigate to issue — **164,034** issues **1708d** effort

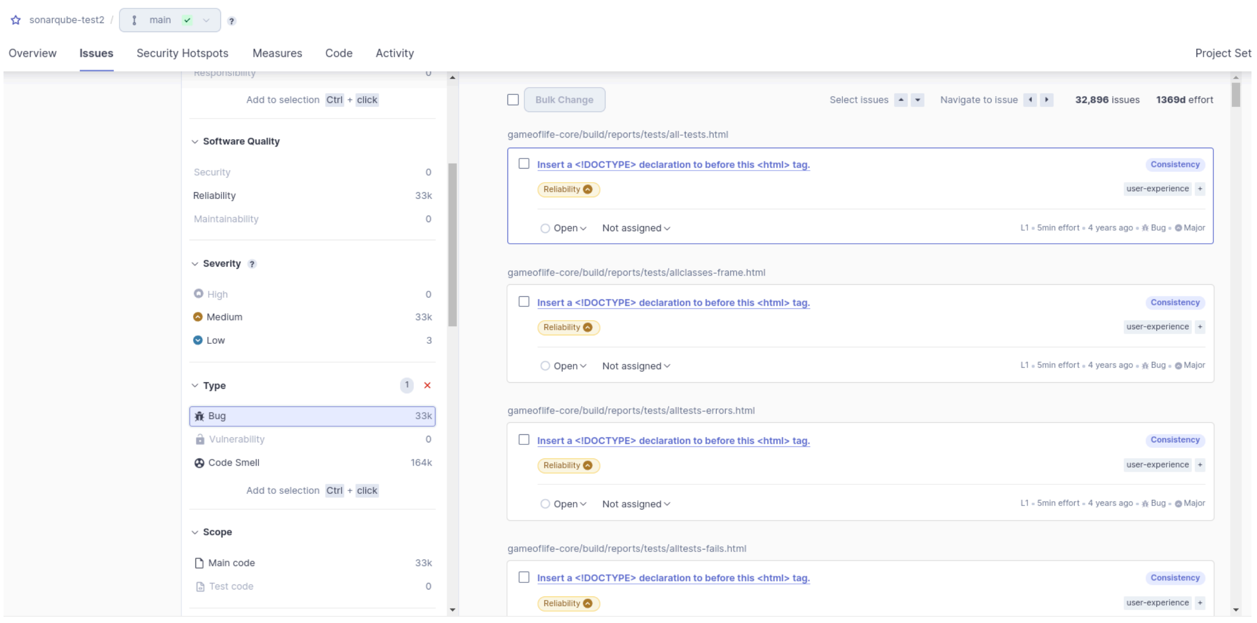
gameoflife-acceptance-tests/Dockerfile

- Use a specific version tag for the image. — Intentionality — Maintainability — No tags — Open — Not assigned — L1 • 5min effort • 4 years ago • Code Smell • Major
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. — Intentionality — Maintainability — No tags — Open — Not assigned — L12 • 5min effort • 4 years ago • Code Smell • Major
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. — Intentionality — Maintainability — No tags — Open — Not assigned — L12 • 5min effort • 4 years ago • Code Smell • Major
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. — Intentionality — Maintainability — No tags — Open — Not assigned — L13 • 5min effort • 4 years ago • Code Smell • Major

gameoflife-core/build/reports/tests/all-tests.html

Bugs

Name: Alok Yadav Div: D15C Roll No.: 59



sonarqube-test2 / main

Overview · Issues · Security Hotspots · Measures · Code · Activity · Project Set

Add to selection Ctrl + click

Software Quality

Security	0
Reliability	33k
Maintainability	0

Severity

High	0
Medium	33k
Low	3

Type 1

Bug	33k
Vulnerability	0
Code Smell	164k

Add to selection Ctrl + click

Scope

Main code	33k
Test code	0

Bulk Change · Select issues · Navigate to issue · **32,896** issues · **1369d** effort

gameoflife-core/build/reports/tests/all-tests.html

Insert a <!DOCTYPE> declaration to before this <html> tag.
Consistency
Reliability
user-experience
Open · Not assigned · L1 · 5min effort · 4 years ago · Bug · Major

gameoflife-core/build/reports/tests/allclasses-frame.html

Insert a <!DOCTYPE> declaration to before this <html> tag.
Consistency
Reliability
user-experience
Open · Not assigned · L1 · 5min effort · 4 years ago · Bug · Major

gameoflife-core/build/reports/tests/alltests-errors.html

Insert a <!DOCTYPE> declaration to before this <html> tag.
Consistency
Reliability
user-experience
Open · Not assigned · L1 · 5min effort · 4 years ago · Bug · Major

gameoflife-core/build/reports/tests/alltests-fails.html

Insert a <!DOCTYPE> declaration to before this <html> tag.
Consistency
Reliability
user-experience

Conclusion: We began the experiment with creating a new project in SonarQube and setting up a new Pipeline in Jenkins with proper configuration of pipeline script. Then we installed Sonar Scanner CLI so that jenkins can do code analysis of Git Repository. We can also configure the pipeline to use the installed Sonar Scanner plugin instead of locally installed Binary of Sonar Scanner.The pipeline ran successfully with all tests passed in SonarQube