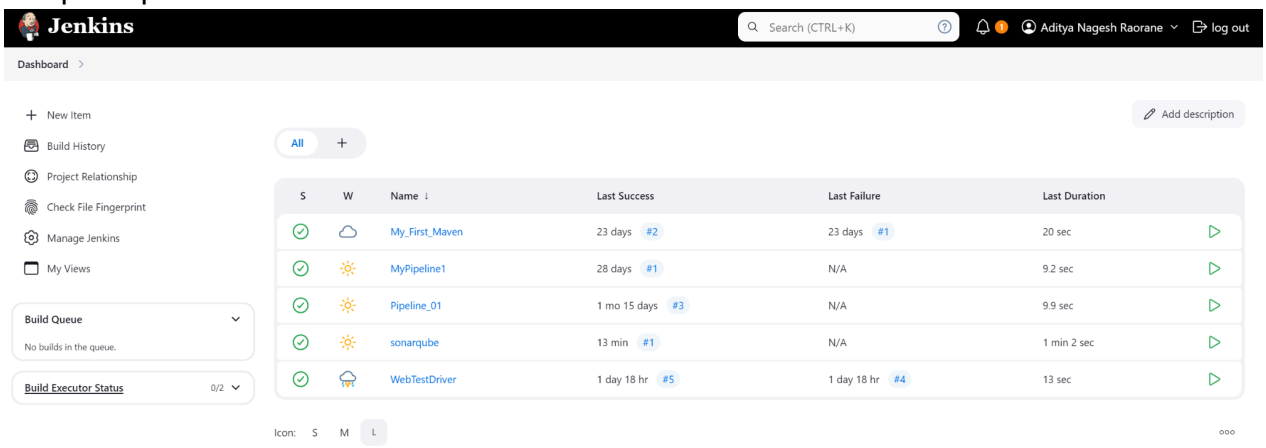
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

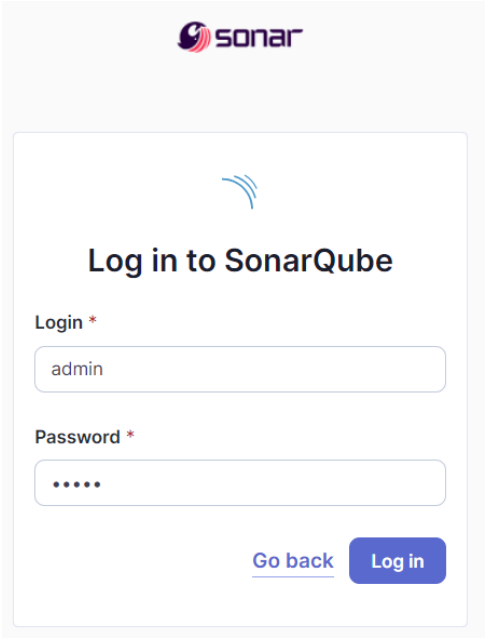
1. Open up Jenkins Dashboard on localhost:8080.



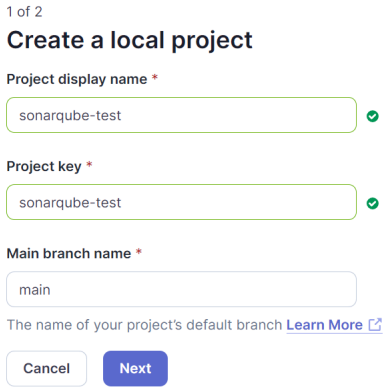
2. Run SonarQube in a Docker container using this command:
a] docker -v
b] docker pull sonarqube
c] docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest

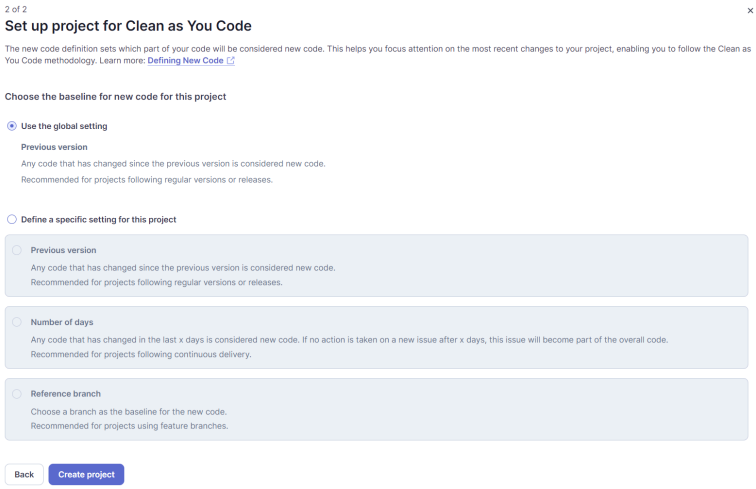
```
C:\Users\adity>docker -v
Docker version 27.0.3, build 7d4bcd8

C:\Users\adity>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
4a6e73f4472de892b1ddead1abe77372a85a7b09408cce3a0abd37c5ab6b49a4
```

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 “**aditya**”.



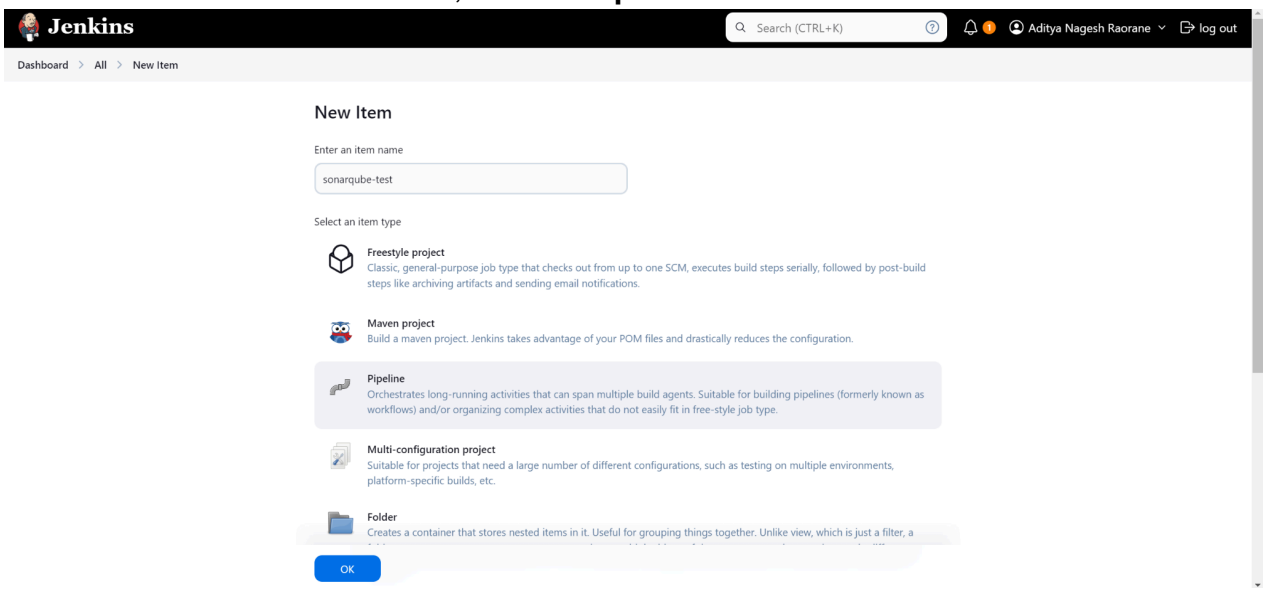
4. **Create a local project in SonarQube** with the name **sonarqube-test**.





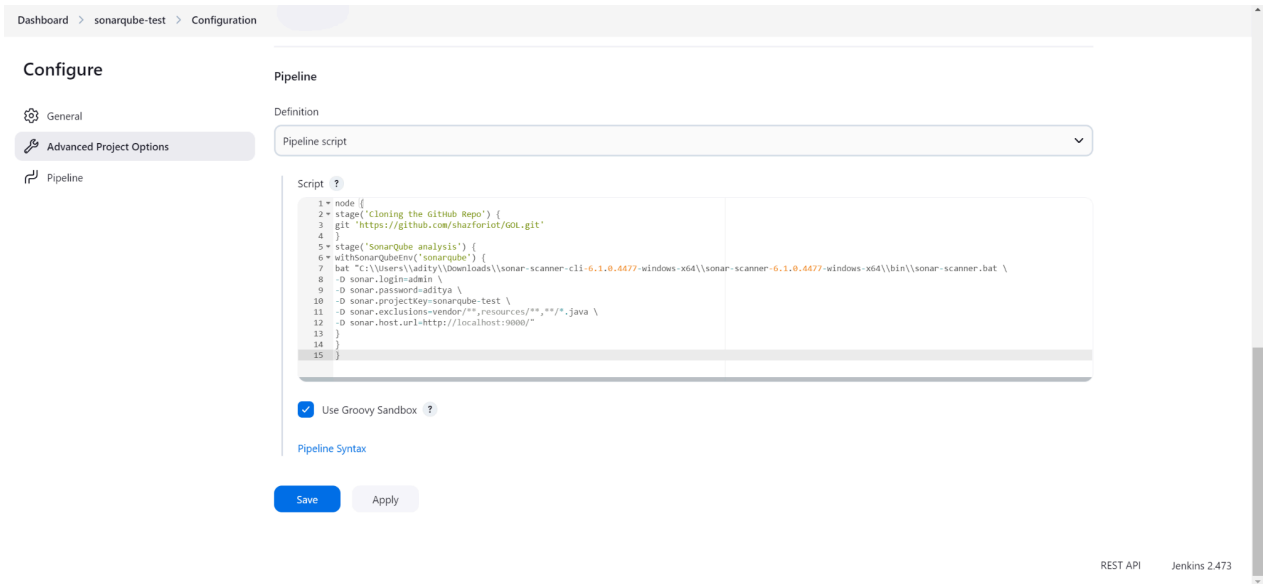
Setup the project and come back to Jenkins Dashboard.

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



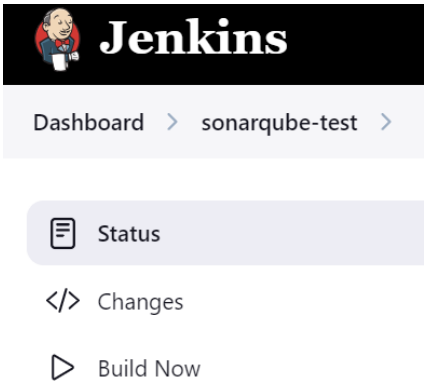
7. Under **Pipeline Script**, enter the following -

```
node {
        stage('Cloning the GitHub Repo')
        {
                git 'https://github.com/shazforiot/GOL.git'
        }
stage('SonarQube analysis') {
        withSonarQubeEnv('sonarqube') {
                bat
        "C:\\Users\\adity\\Downloads\\sonar-scanner-cli-6.1.0.4477-windows-x64\\sonar-s
        canner-6.1.0.4477-windows-x64\\bin\\sonar-scanner.bat \
                -D sonar.login=<YOUR ID> \
                -D sonar.password=<YOUR PASSWORD> \
                -D sonar.projectKey=<YOUR PROJECT KEY> \
                -D sonar.exclusions=vendor/**,resources/**,**/*.java \
                -D sonar.host.url=http://localhost:9000/"
                }
        }
}
```

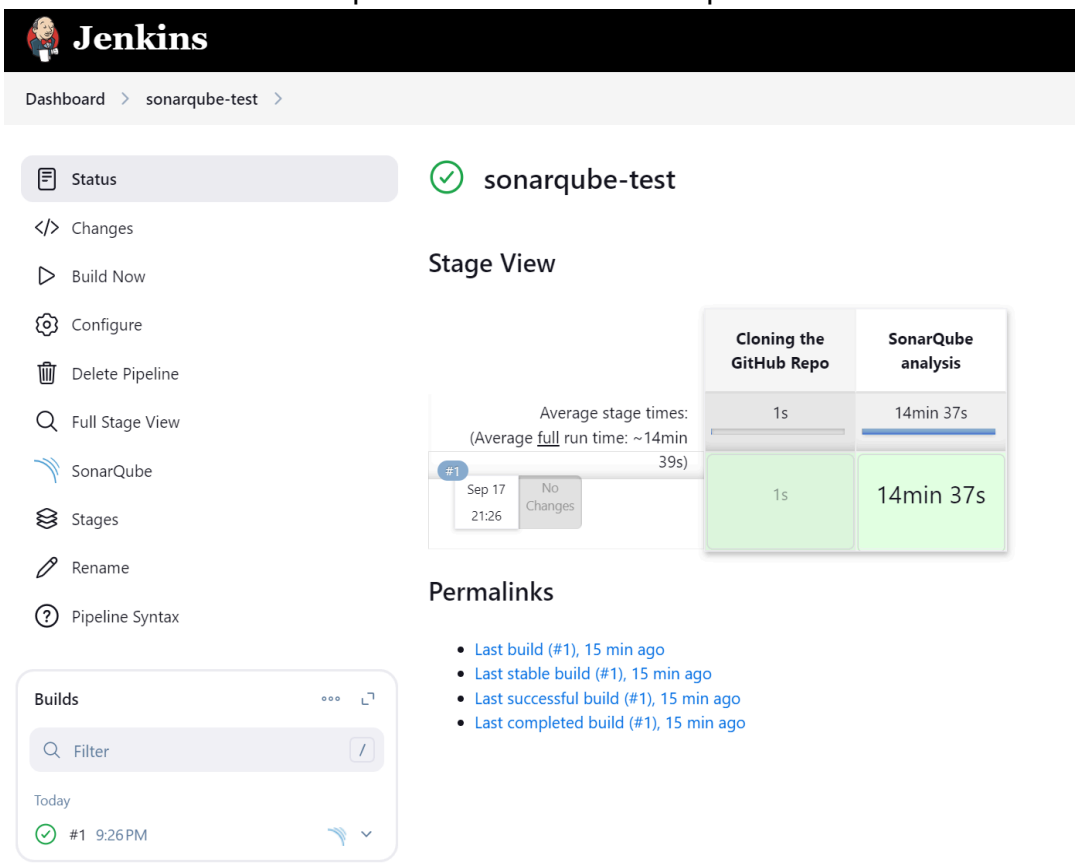


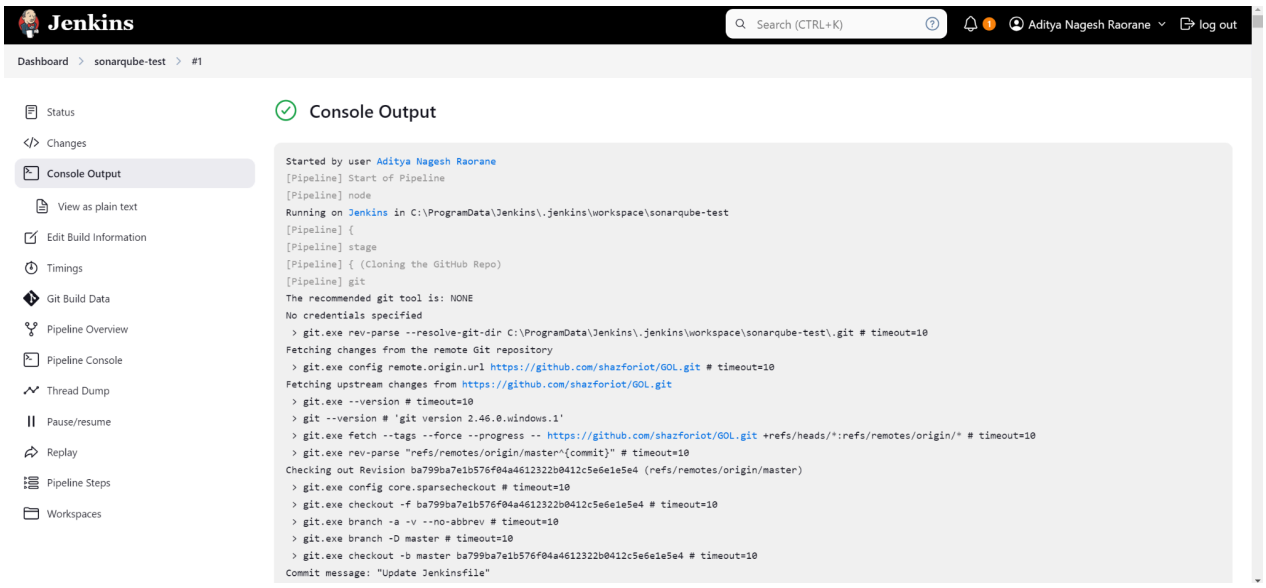
It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.

8. Run The Build.

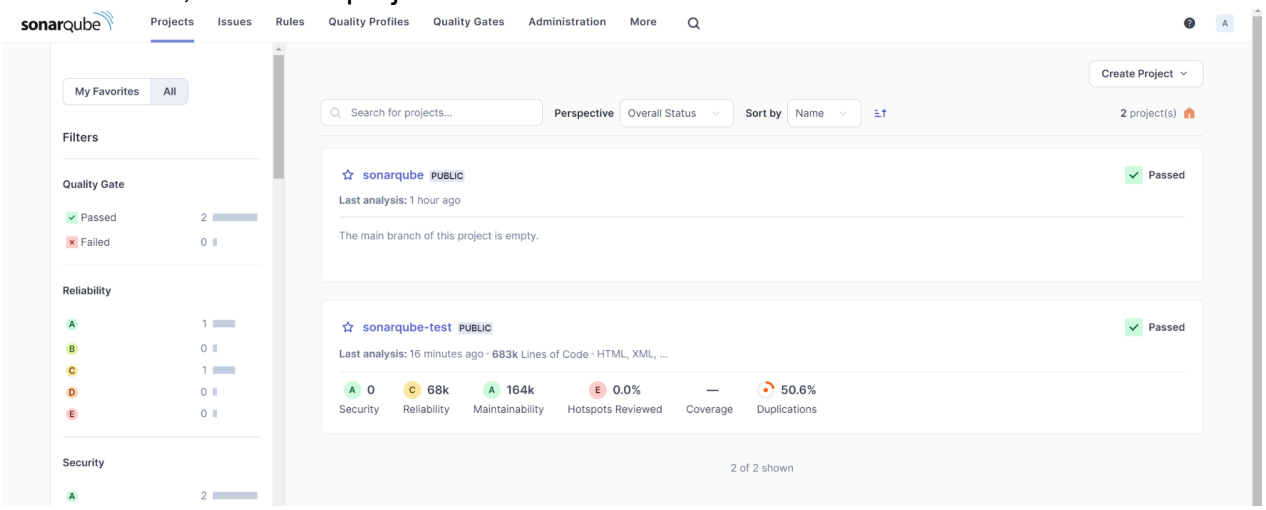


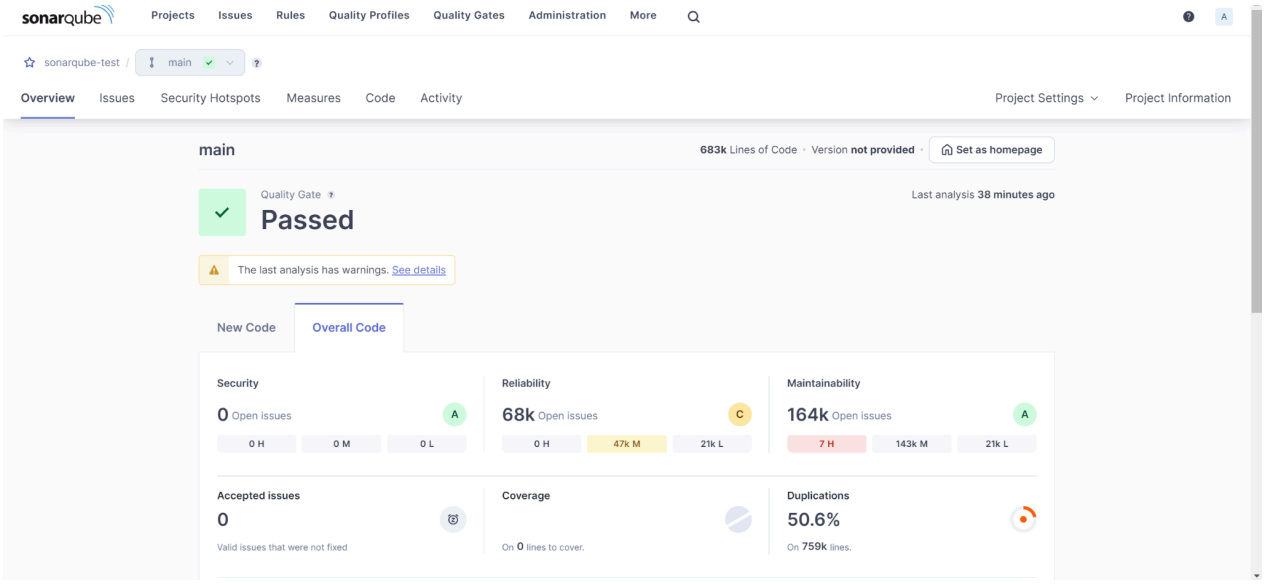
9. Check the console output once the build is complete.





10. After that, check the project in SonarQube.

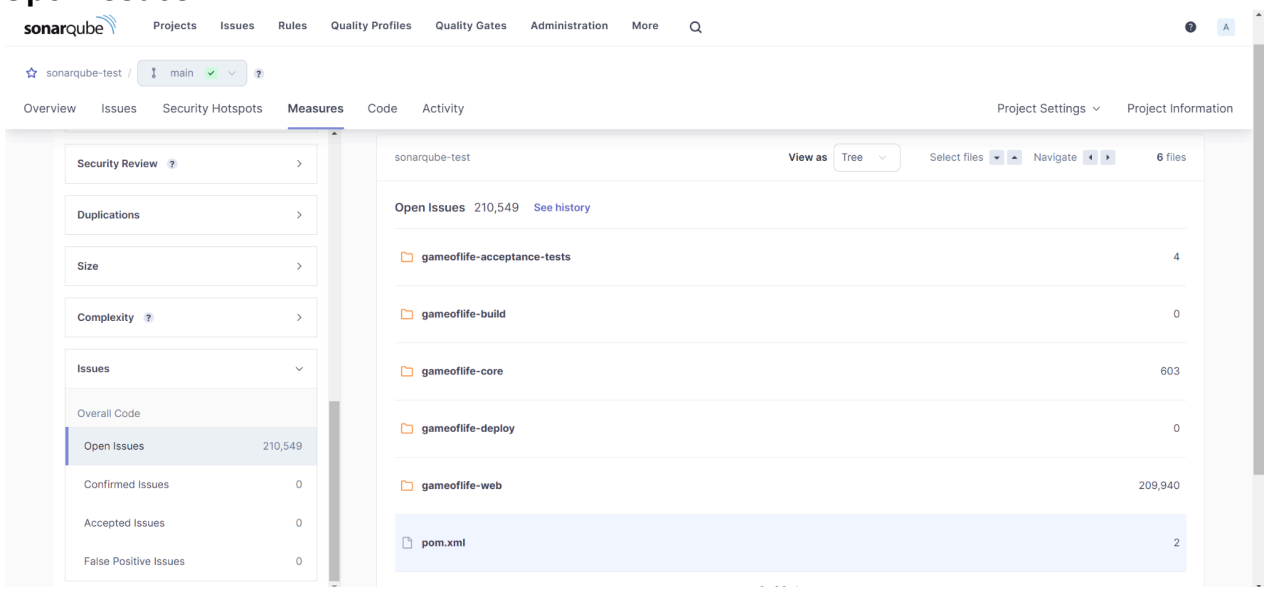




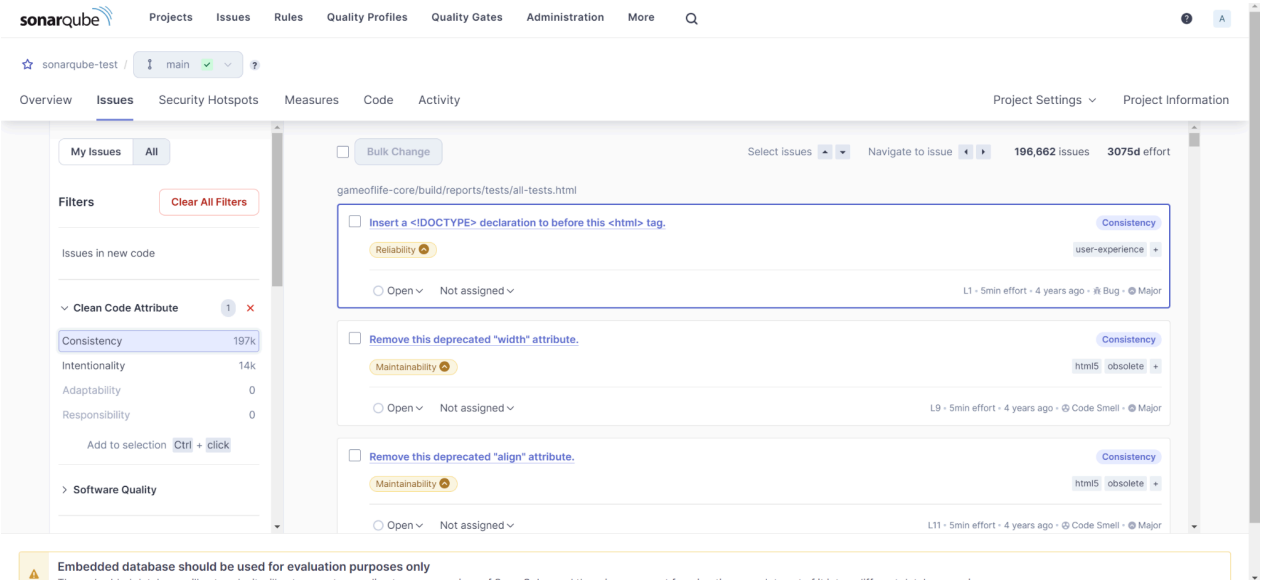
Under different tabs, check all different issues with the code.

11. **Code Problems -**

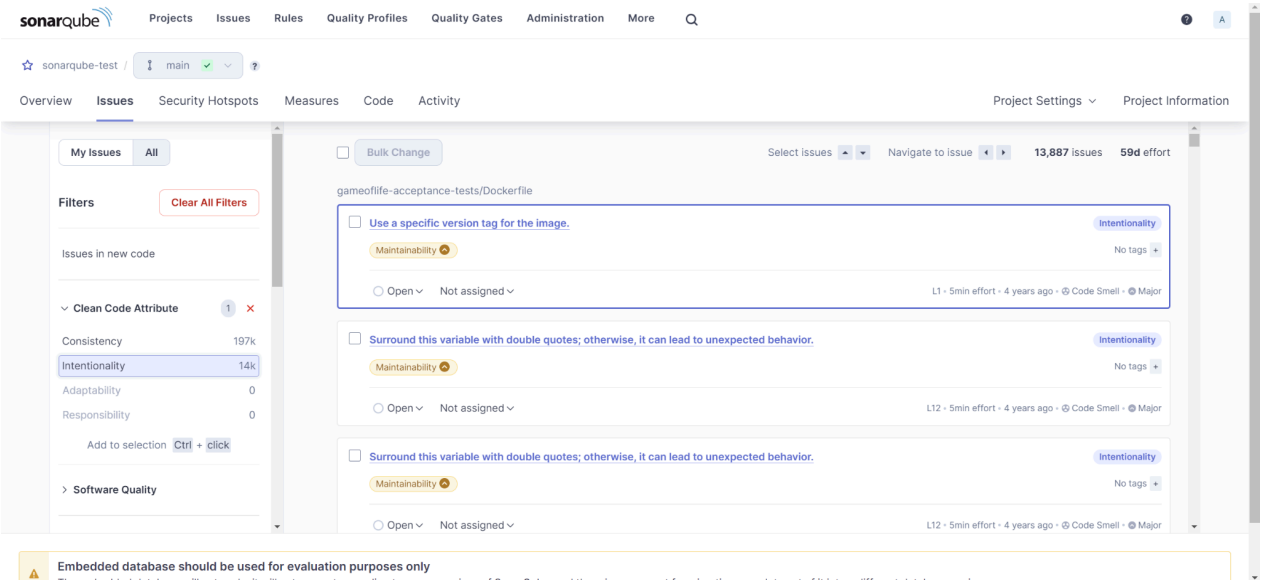
Open Issues



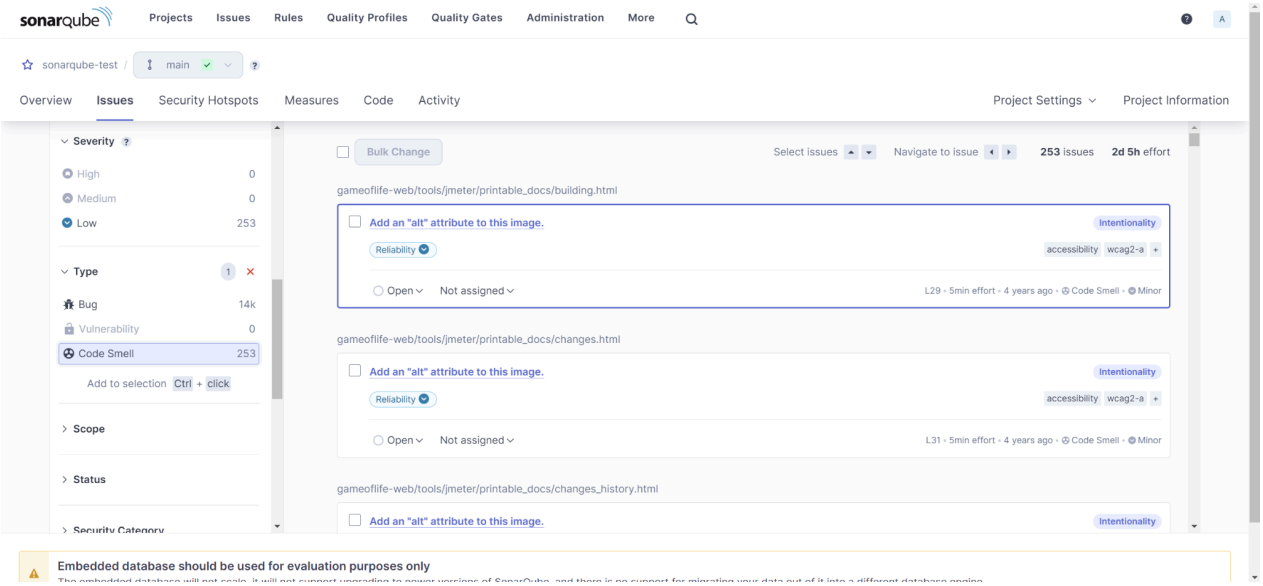
Consistency



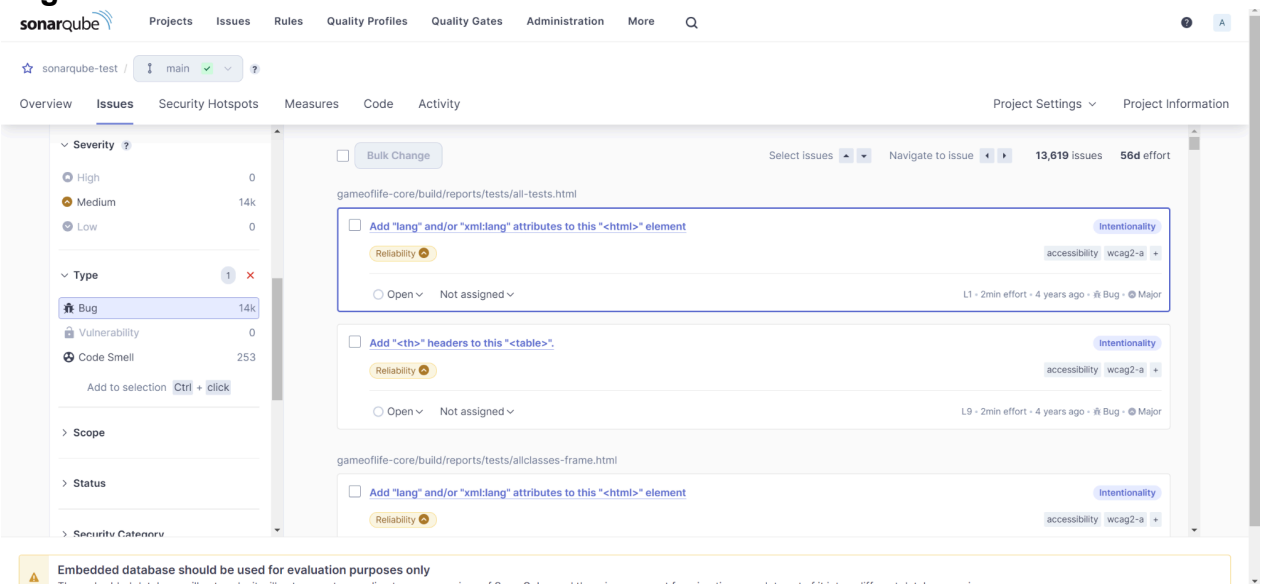
Intentionality



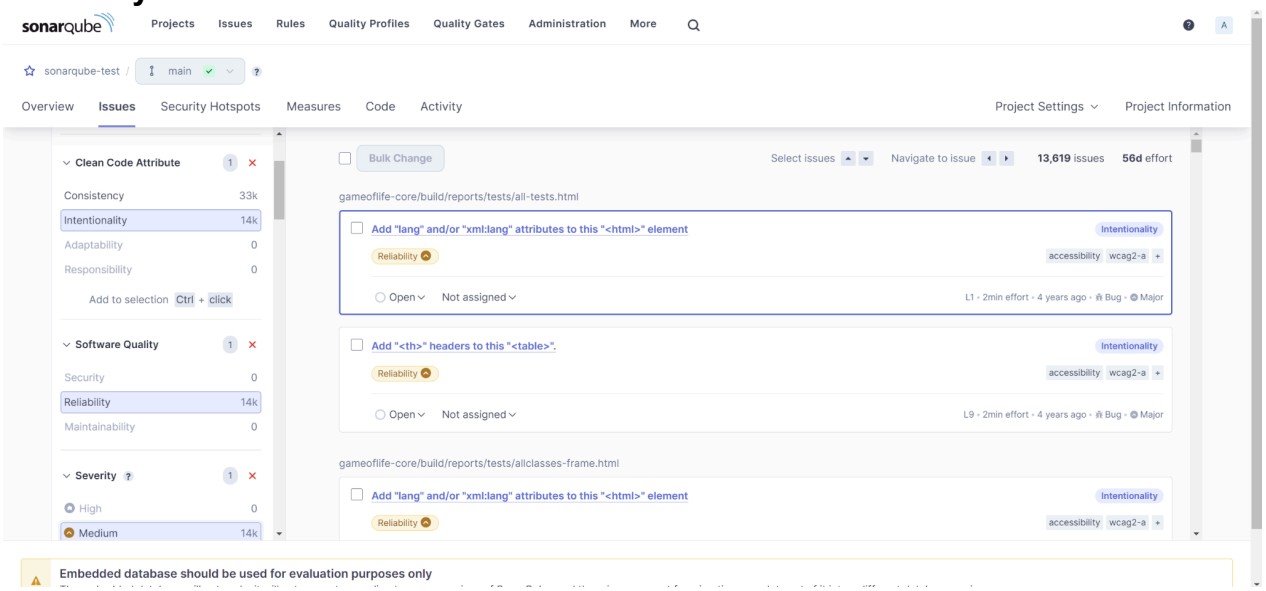
Code Smells


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-test / main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
Severity
High 0
Medium 0
Low 253
Type
Bug 14k
Vulnerability 0
Code Smell 253
Add to selection Ctrl + click
Scope
Status
Bulk Change
Select issues
Navigate to issue
253 issues
2d 5h effort
gameoflife-web/tools/jmeter/printable_docs/building.html
Add an "alt" attribute to this image.
Intentionality
Reliability
accessibility wcag2-a
Open
Not assigned
L29 • 5min effort • 4 years ago • Code Smell • Minor
gameoflife-web/tools/jmeter/printable_docs/changes.html
Add an "alt" attribute to this image.
Intentionality
Reliability
accessibility wcag2-a
Open
Not assigned
L31 • 5min effort • 4 years ago • Code Smell • Minor
gameoflife-web/tools/jmeter/printable_docs/changes_history.html
Add an "alt" attribute to this image.
Intentionality
Embedded database should be used for evaluation purposes only

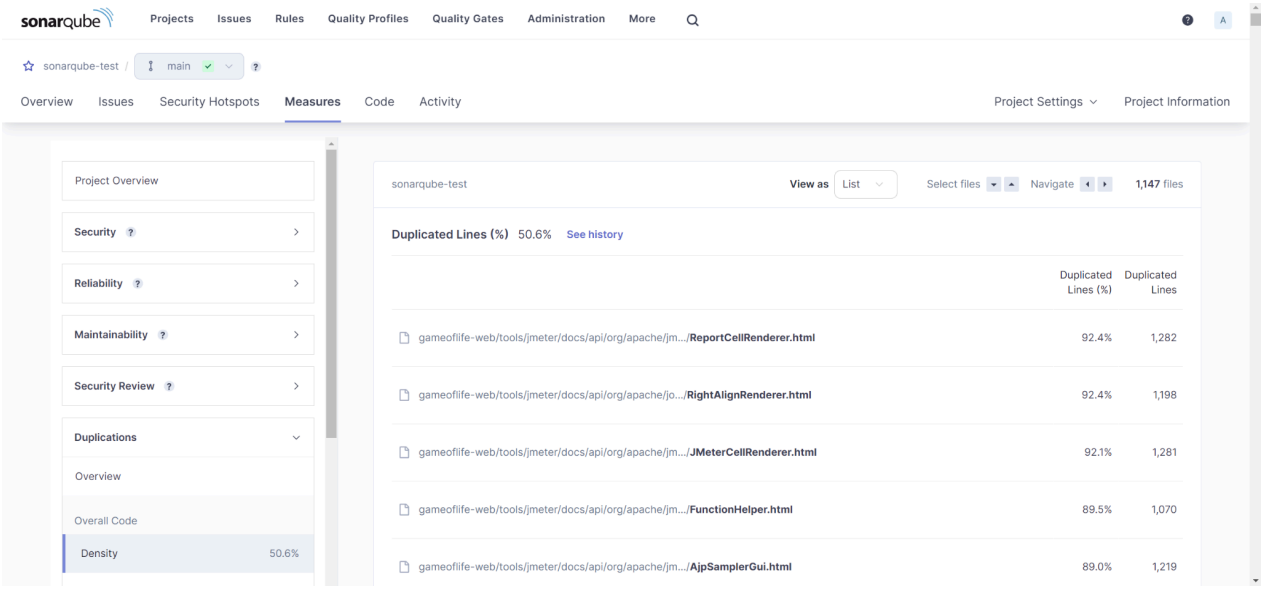
Bugs


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Administration
More
sonarqube-test / main
Overview
Issues
Security Hotspots
Measures
Code
Activity
Project Settings
Project Information
Severity
High 0
Medium 14k
Low 0
Type
Bug 14k
Vulnerability 0
Code Smell 253
Add to selection Ctrl + click
Scope
Status
Bulk Change
Select issues
Navigate to issue
13,619 issues
56d effort
gameoflife-core/build/reports/tests/all-tests.html
Add "lang" and/or "xml:lang" attributes to this "<html>" element
Intentionality
Reliability
accessibility wcag2-a
Open
Not assigned
L1 • 2min effort • 4 years ago • Bug • Major
Add "<th>" headers to this "<table>".
Intentionality
Reliability
accessibility wcag2-a
Open
Not assigned
L9 • 2min effort • 4 years ago • Bug • Major
gameoflife-core/build/reports/tests/allclasses-frame.html
Add "lang" and/or "xml:lang" attributes to this "<html>" element
Intentionality
Reliability
accessibility wcag2-a
Embedded database should be used for evaluation purposes only

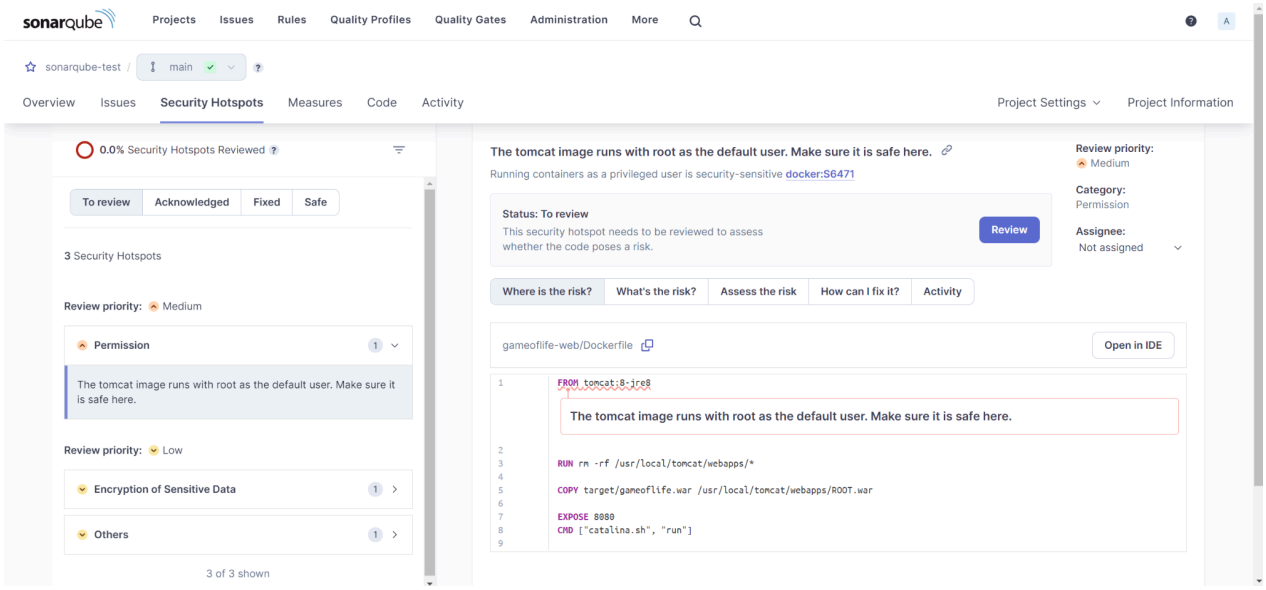
Reliability



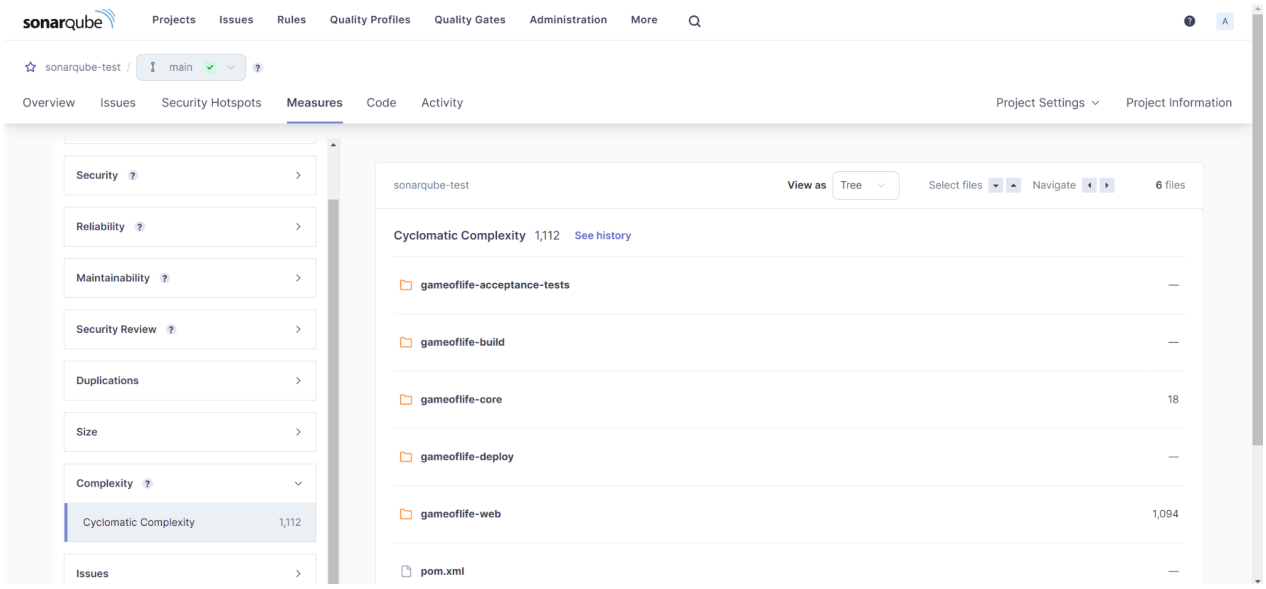
Duplicates



Security Hotspot



Cyclomatic Complexity



In this way, we have created a CI/CD Pipeline with Jenkins and integrated it with SonarQube to find issues in the code like bugs, code smells, duplicates, cyclomatic complexities, etc.

Conclusion:

In this experiment, we performed a static analysis of the code to detect bugs, code smells, and security vulnerabilities on our sample Java application.