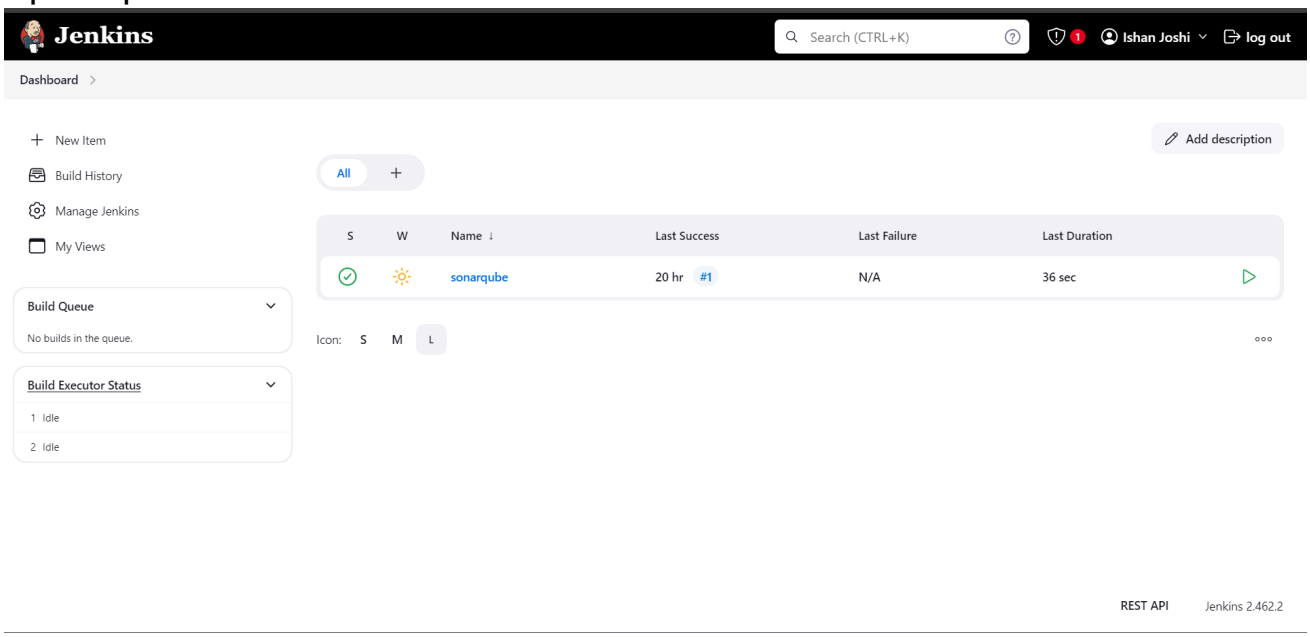
Name-Ishan Kiran Joshi Div-D15C Roll No-21 A.Y.-2024-25

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.

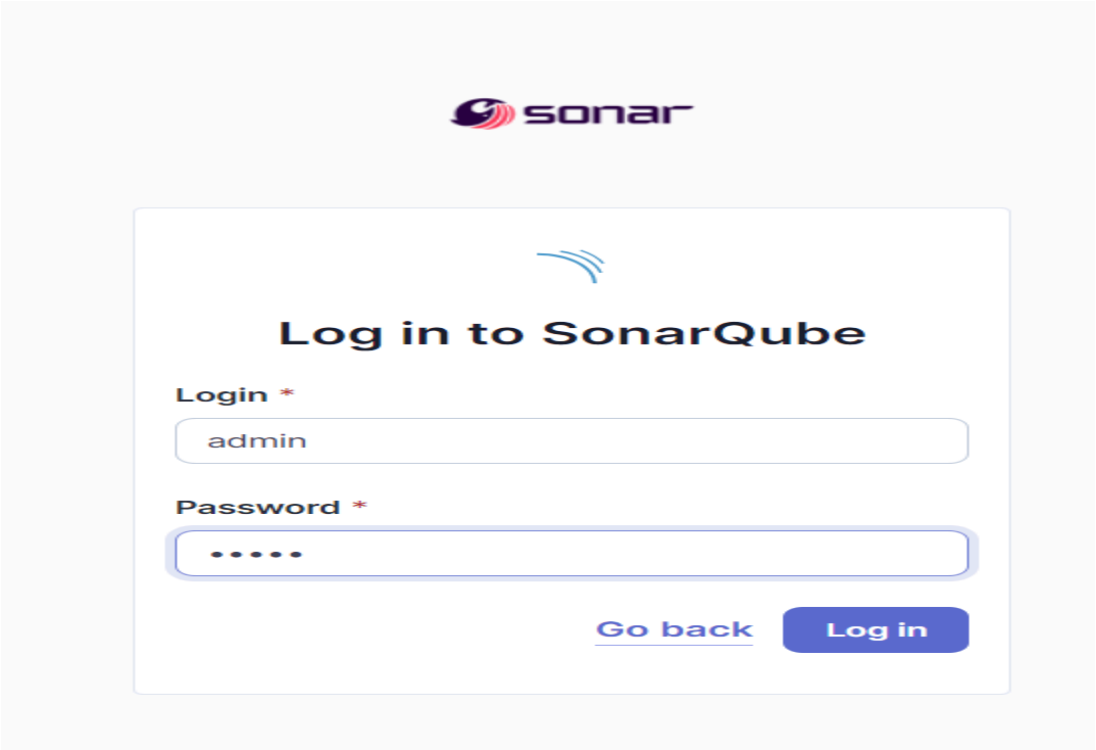


2. Run SonarQube in a Docker container using this command: a] docker -v
b] docker pull sonarqube
c] docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest

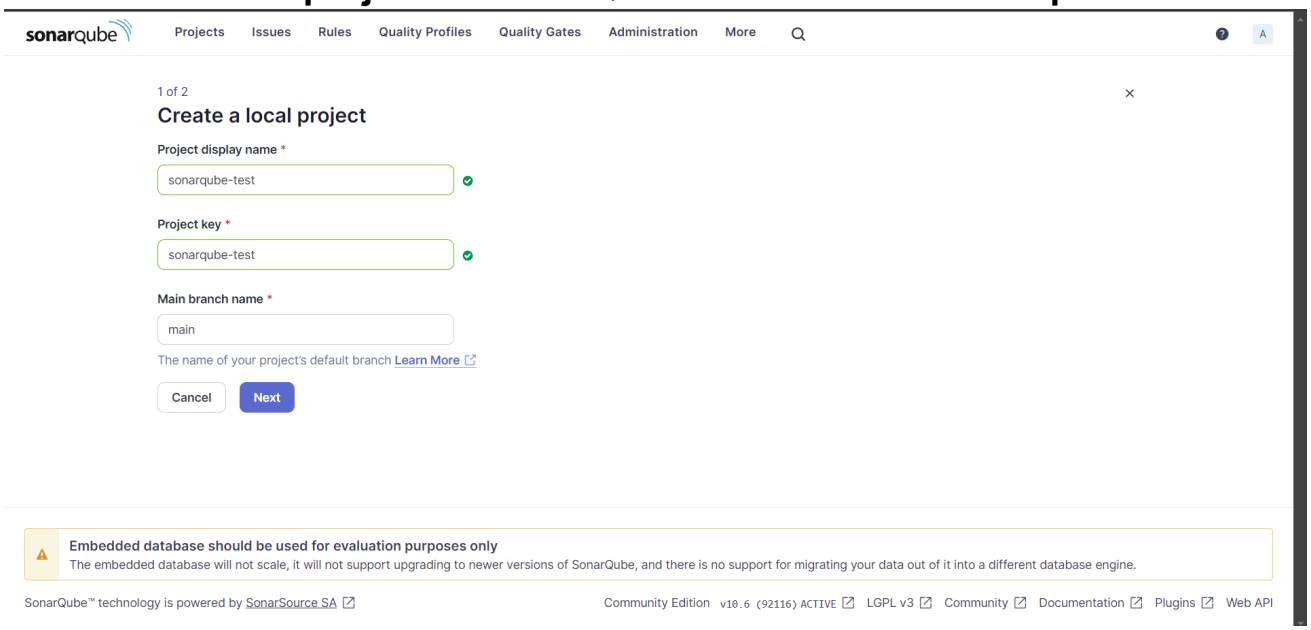
```
C:\Users\ishan>docker -v
Docker version 27.1.1, build 6312585

C:\Users\ishan>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
23c14503da77ee785f6069bfaff714939ddb794a6b846124594503f6183b4c68
```

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 "**ishan**".



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



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 the most recent changes to your project, enabling you to 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**

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

    Recommended for projects following regular versions or releases.

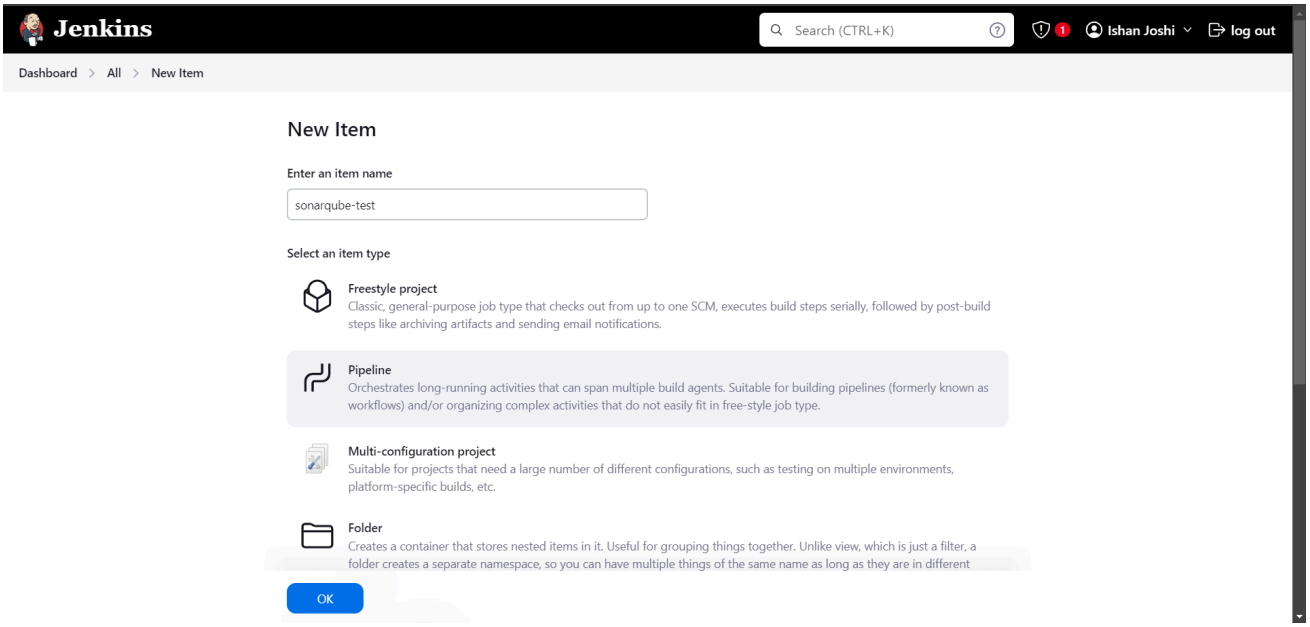
  - ( ) **Number of days**

    Any code that has changed in the last x days is considered new code. If no action is taken on a new issue after x days, this issue will become part of the overall code.

    Recommended for projects following continuous delivery.

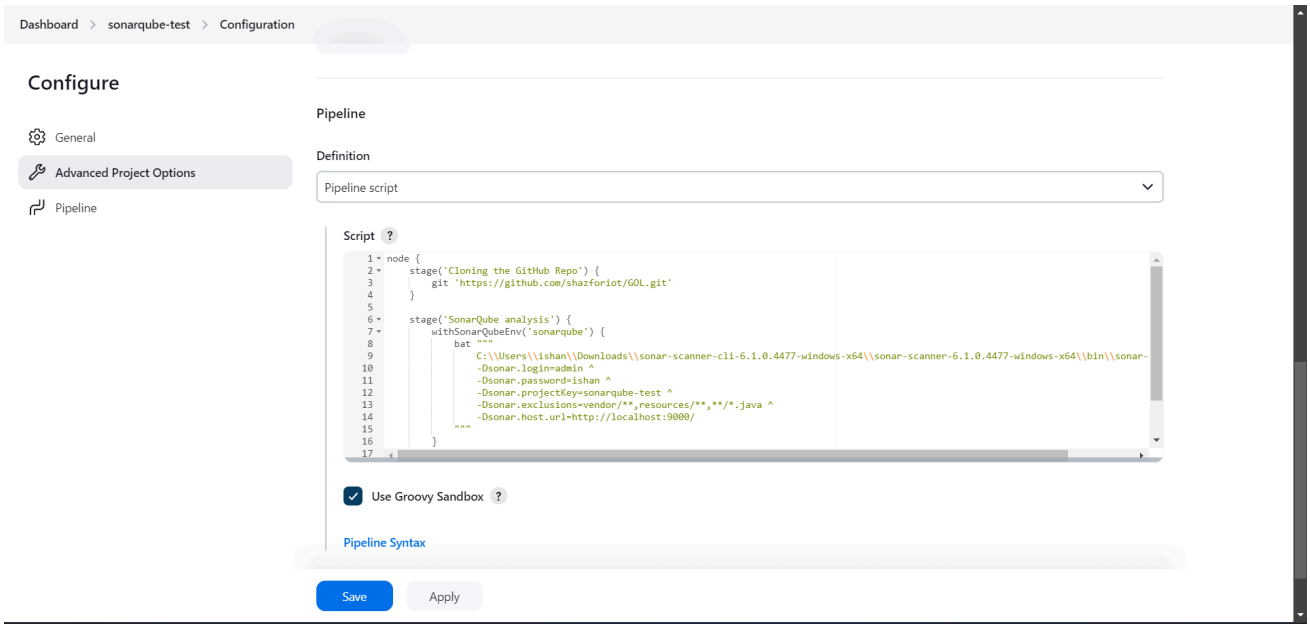
Setup the project and come back to Jenkins Dashboard.

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



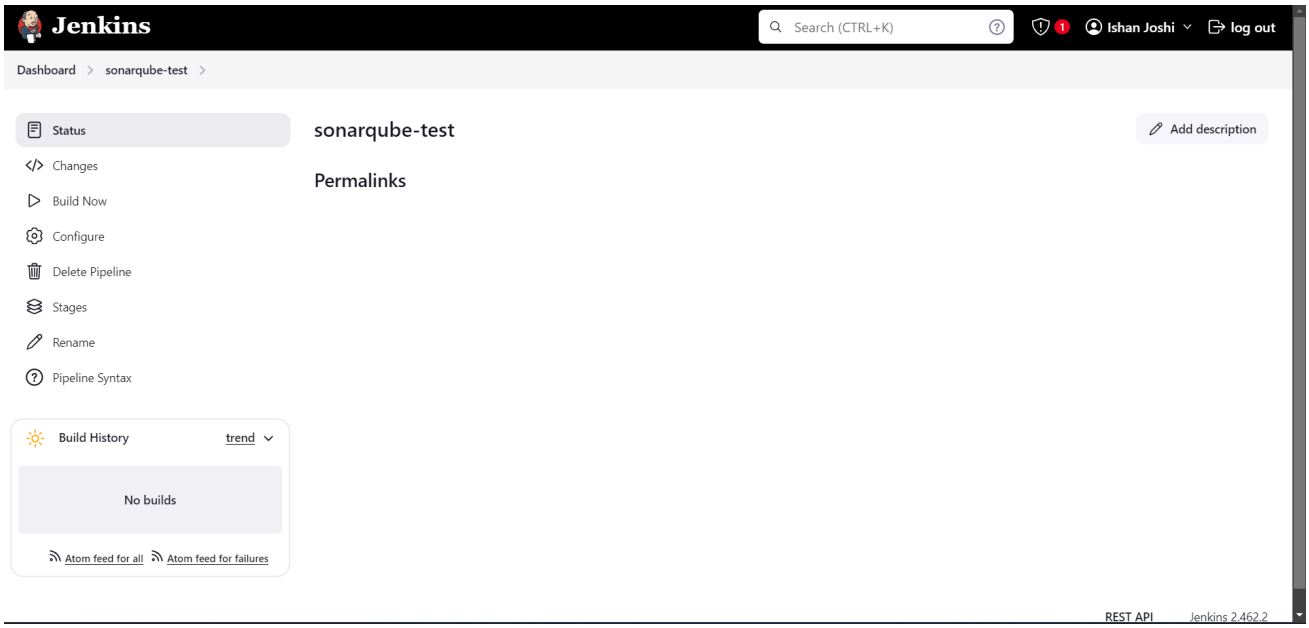
7. Under **Pipeline Script**, enter the following -

```
node {
        stage('Cloning the GitHub Repo')
        {
            git 'https://github.com/shazforiot/GOL.git'
        }
stage('SonarQube analysis') {
        withSonarQubeEnv('sonarqu
        be') {
            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/"
            }}}
```

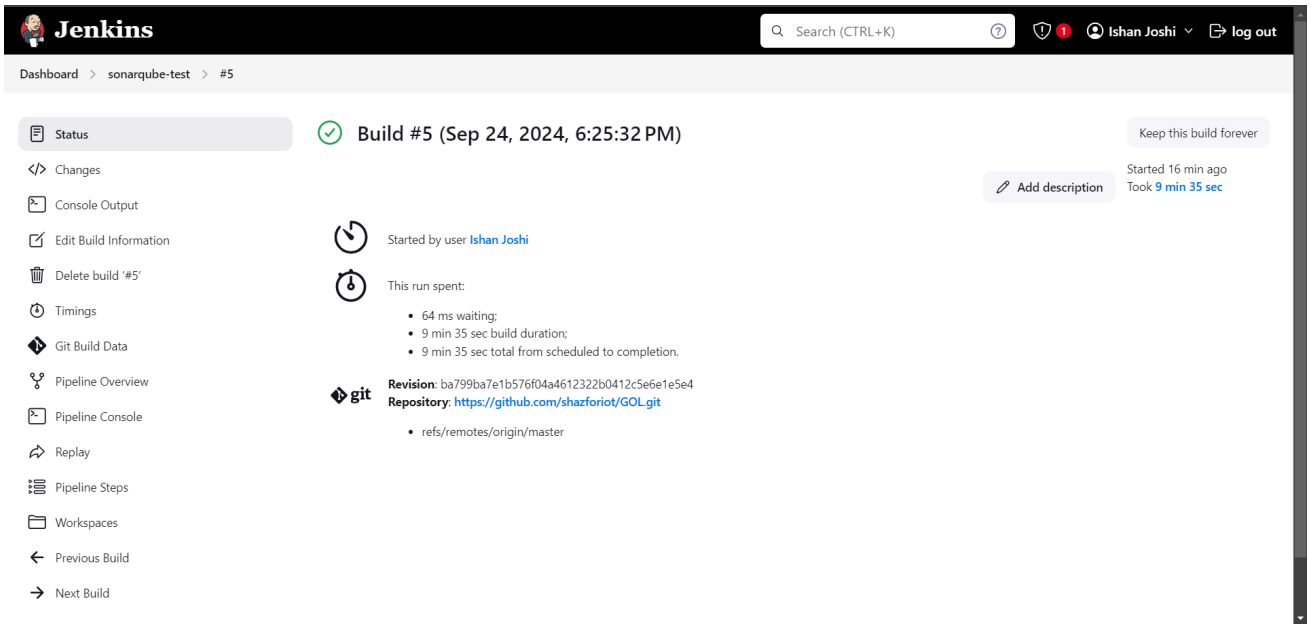


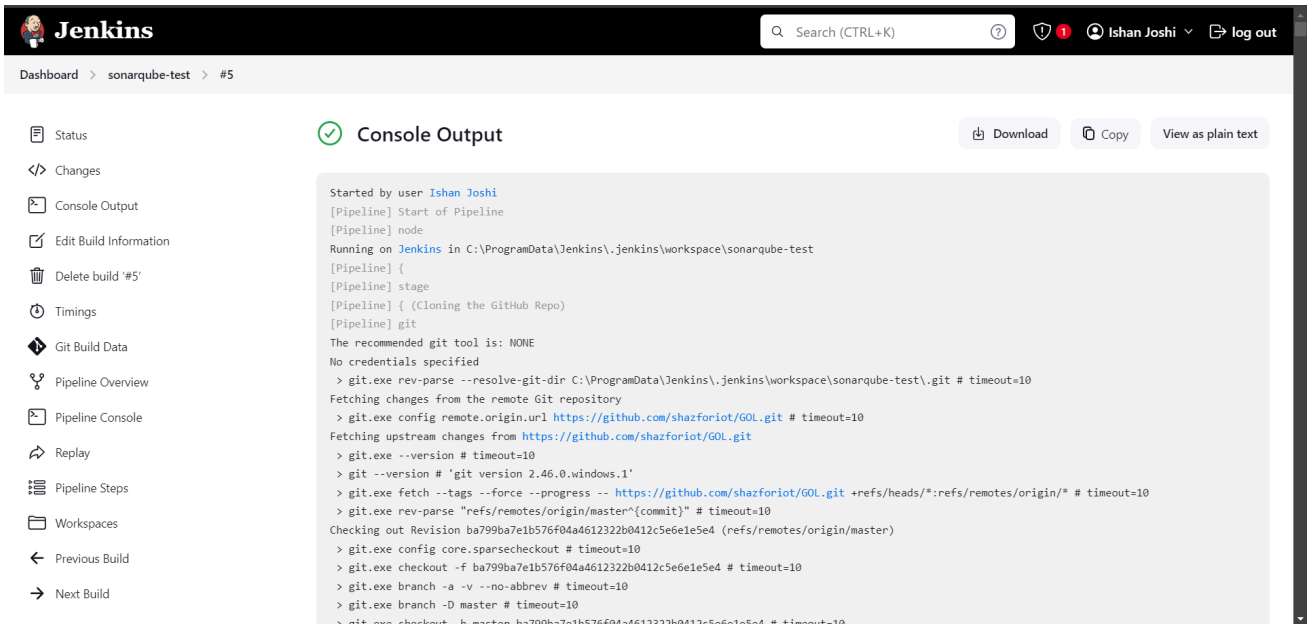
It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.

8. Run The Build.



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

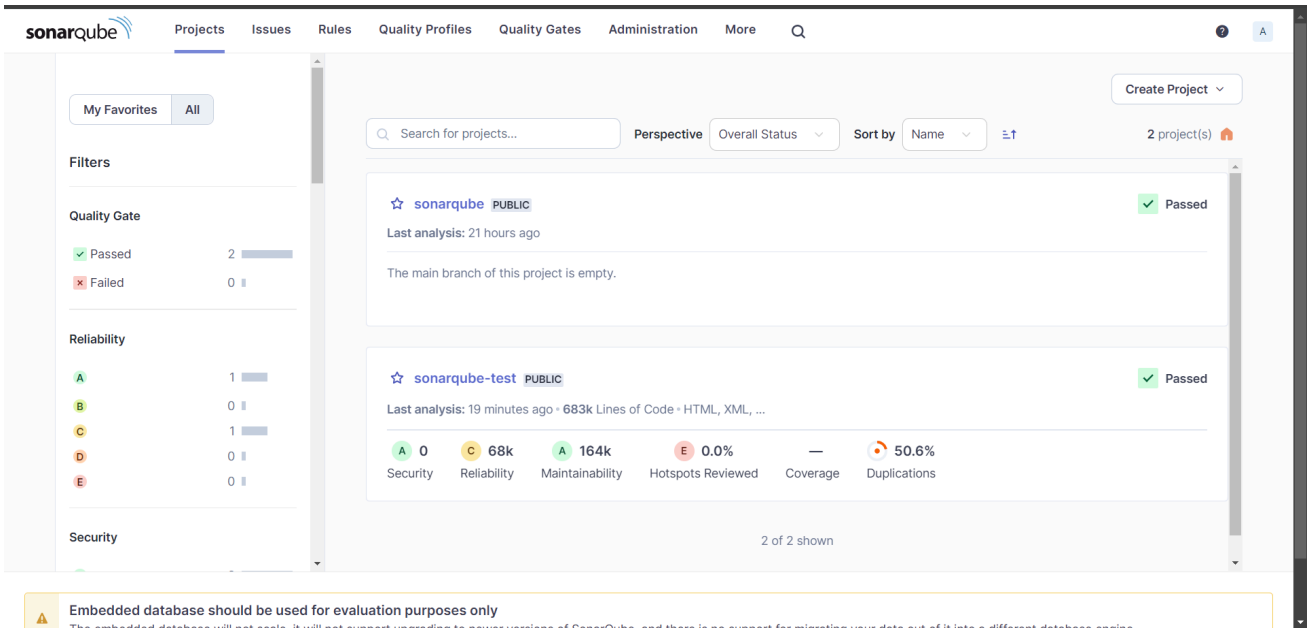


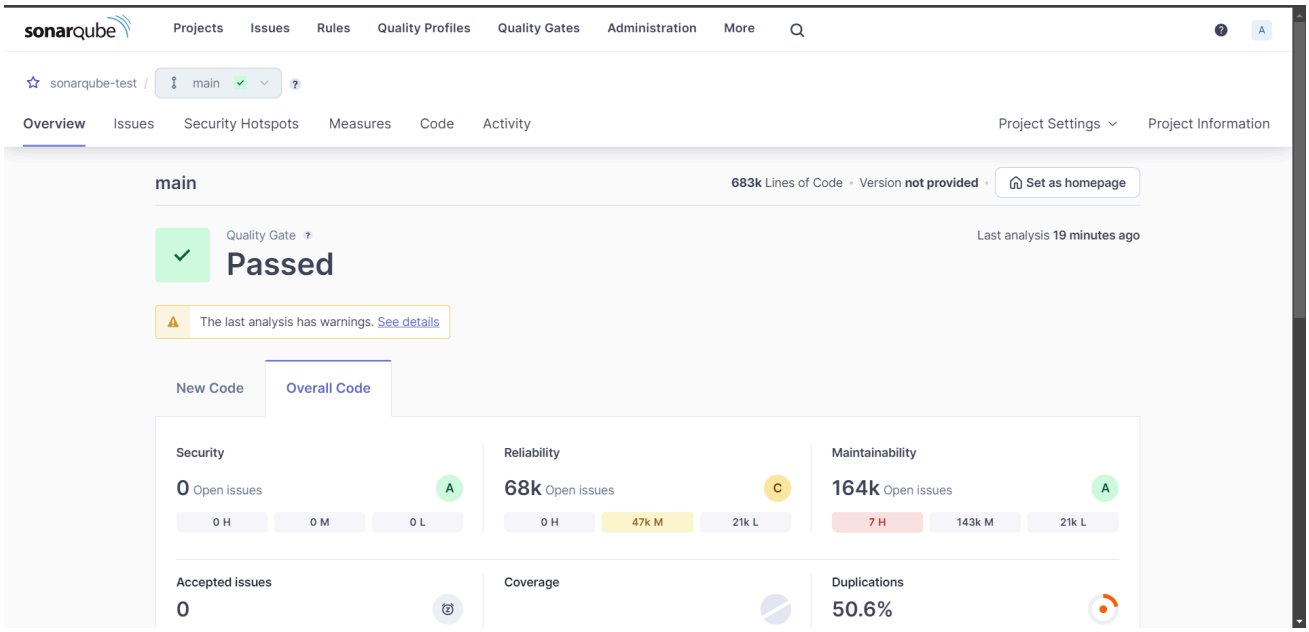


Dashboard > sonarqube-test > #5

```
18:34:27.439 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html
for block at line 75. Keep only the first 100 references.
18:34:27.439 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html
for block at line 41. Keep only the first 100 references.
18:34:27.439 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html
for block at line 17. Keep only the first 100 references.
18:34:27.439 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html
for block at line 296. Keep only the first 100 references.
18:34:27.439 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html
for block at line 75. Keep only the first 100 references.
18:34:27.440 INFO  CPD Executor CPD calculation finished (done) | time=151634ms
18:34:27.458 INFO  SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
18:34:33.719 INFO  Analysis report generated in 4472ms, dir size=127.2 MB
18:34:51.097 INFO  Analysis report compressed in 17377ms, zip size=29.6 MB
18:34:51.752 INFO  Analysis report uploaded in 655ms
18:34:51.754 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube-test
18:34:51.754 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
18:34:51.754 INFO  More about the report processing at http://localhost:9000/api/ce/task?id=a383e6c0-5738-44c0-9305-9a27b39ce19a
18:35:06.143 INFO  Analysis total time: 9:26.800 s
18:35:06.147 INFO  SonarScanner Engine completed successfully
18:35:06.832 INFO  EXECUTION SUCCESS
18:35:06.862 INFO  Total time: 9:29.562s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

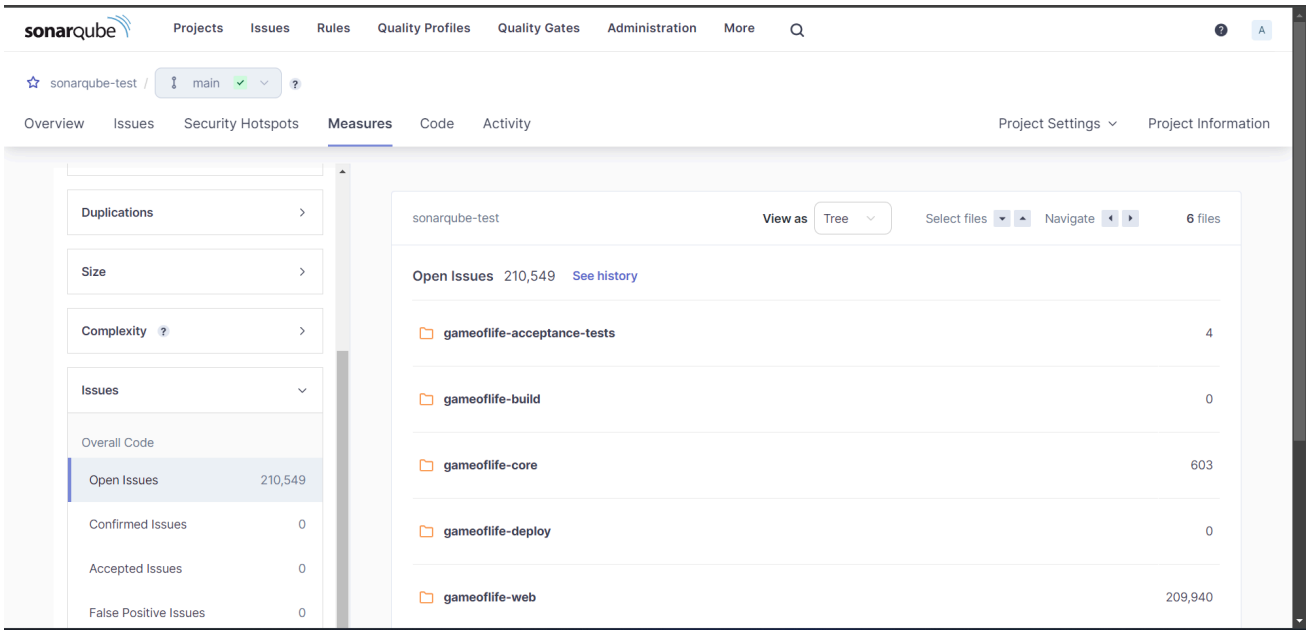
10. After that, check the project in SonarQube



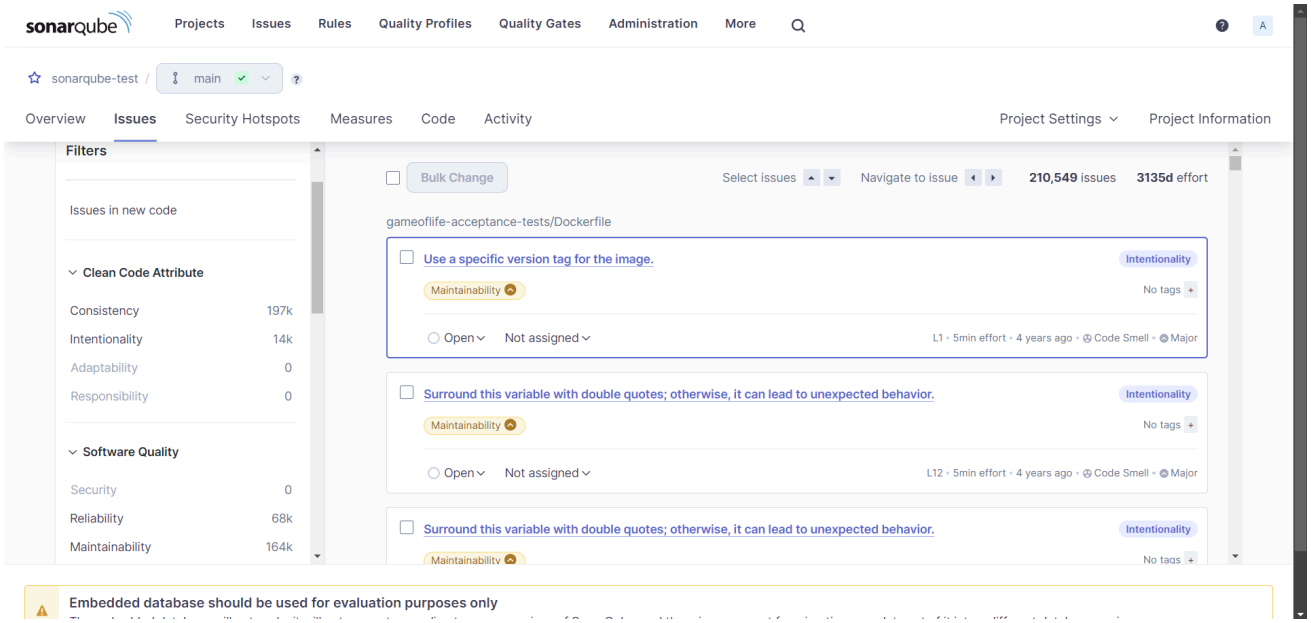


Under different tabs, check all different issues with the code.

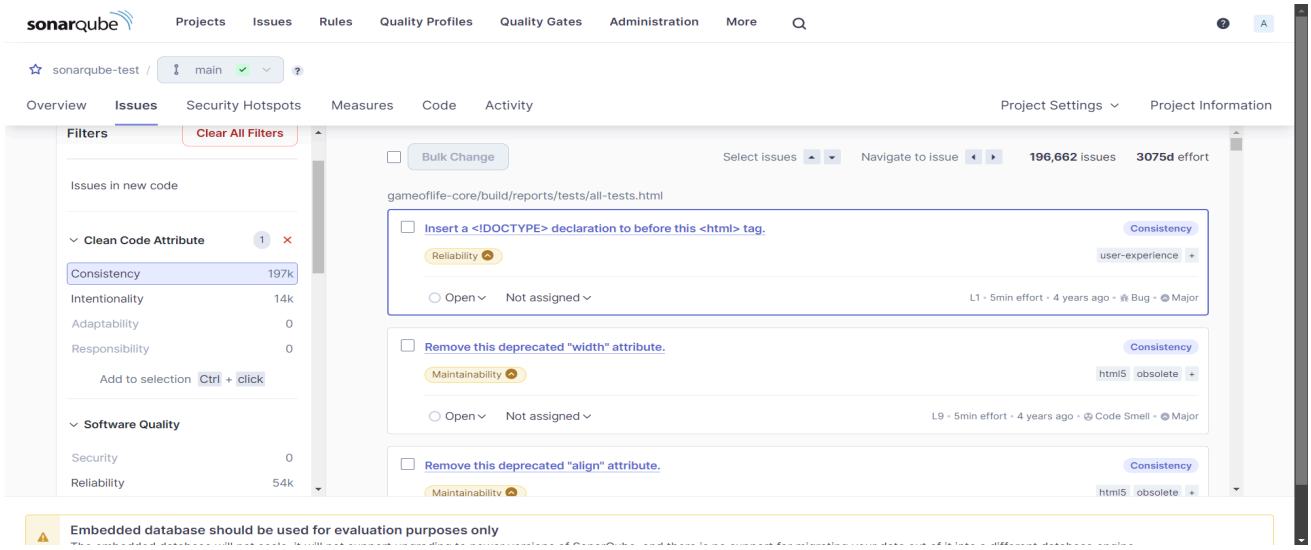
11. Code Problems - Open



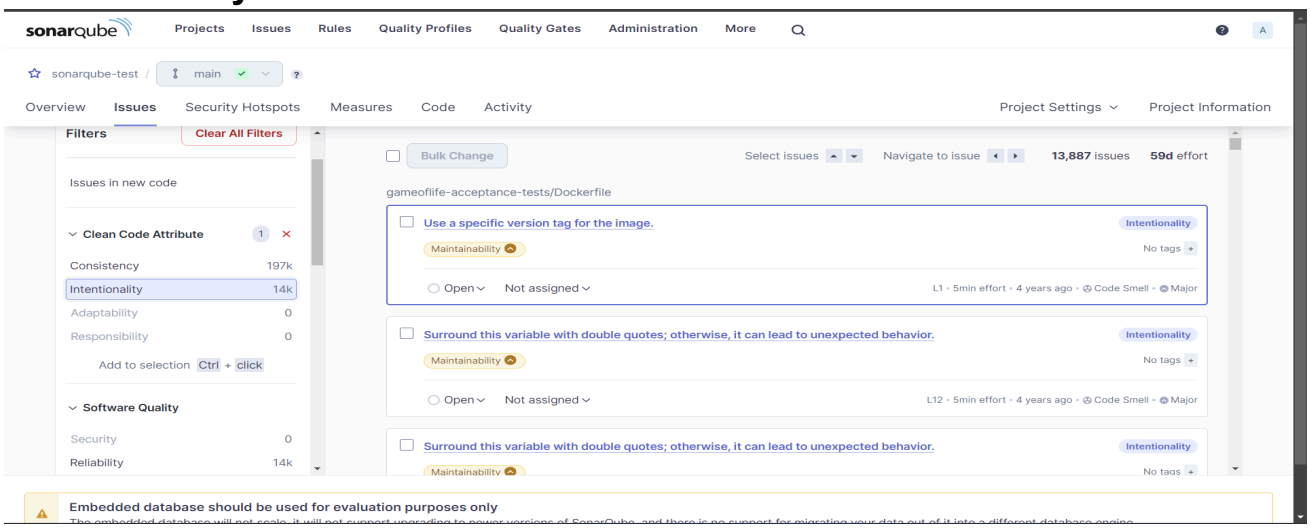
Issues



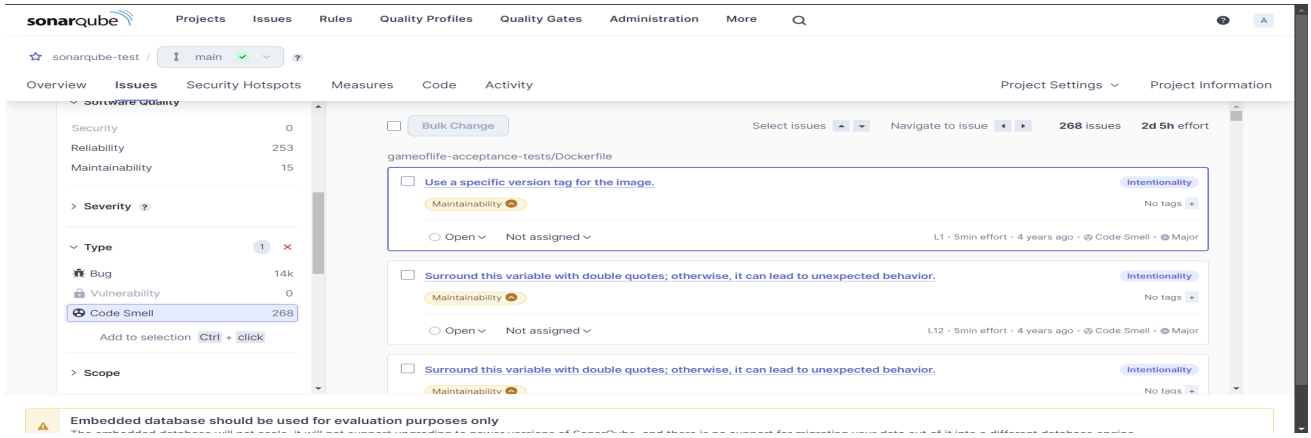
Consistency



Intentionality



Code Smells



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

Software Quality

Security 0
Reliability 14k
Maintainability 0

Severity

Type 1

Bug 14k
Vulnerability 0
Code Smell 268

Add to selection Ctrl + click

Scope

Bulk Change | Select issues | Navigate to issue | 13,619 issues | 56d effort

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

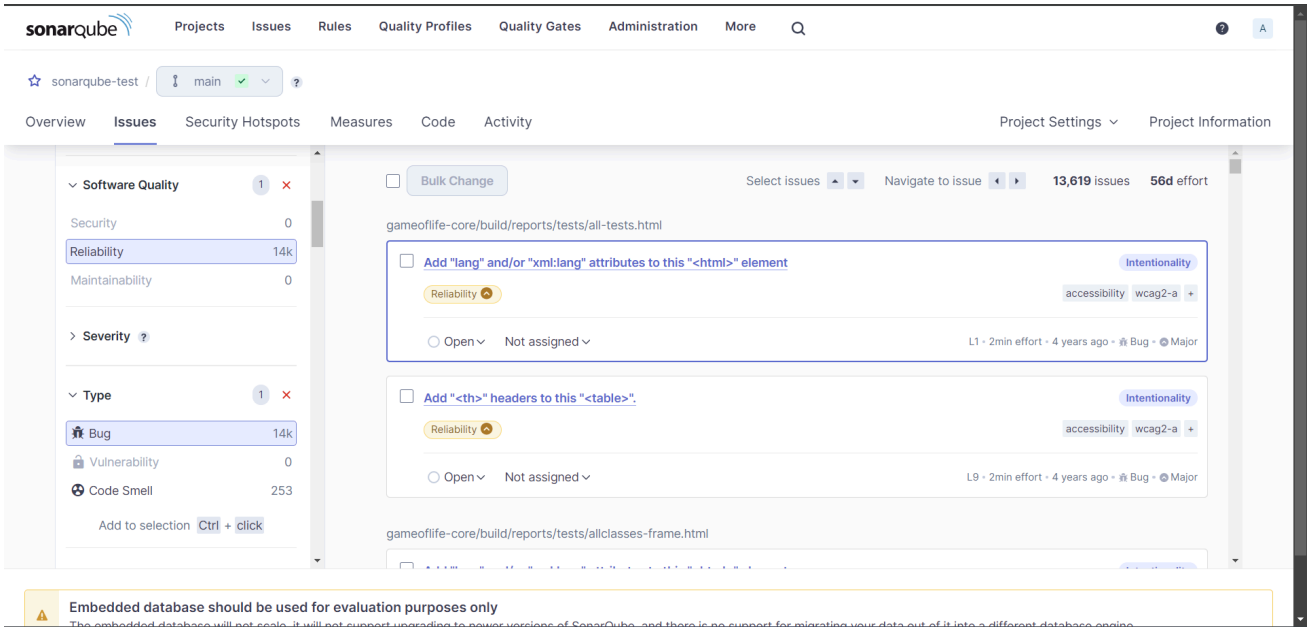
Add "lang" and/or "xml:lang" attributes to this "<html>" element — Intentionality
Reliability — accessibility wcag2-a
Open — Not assigned — L1 · 2min effort · 4 years ago · Bug · Major

Add "<th>" headers to this "<table>". — Intentionality
Reliability — accessibility wcag2-a
Open — Not assigned — L9 · 2min effort · 4 years ago · Bug · Major

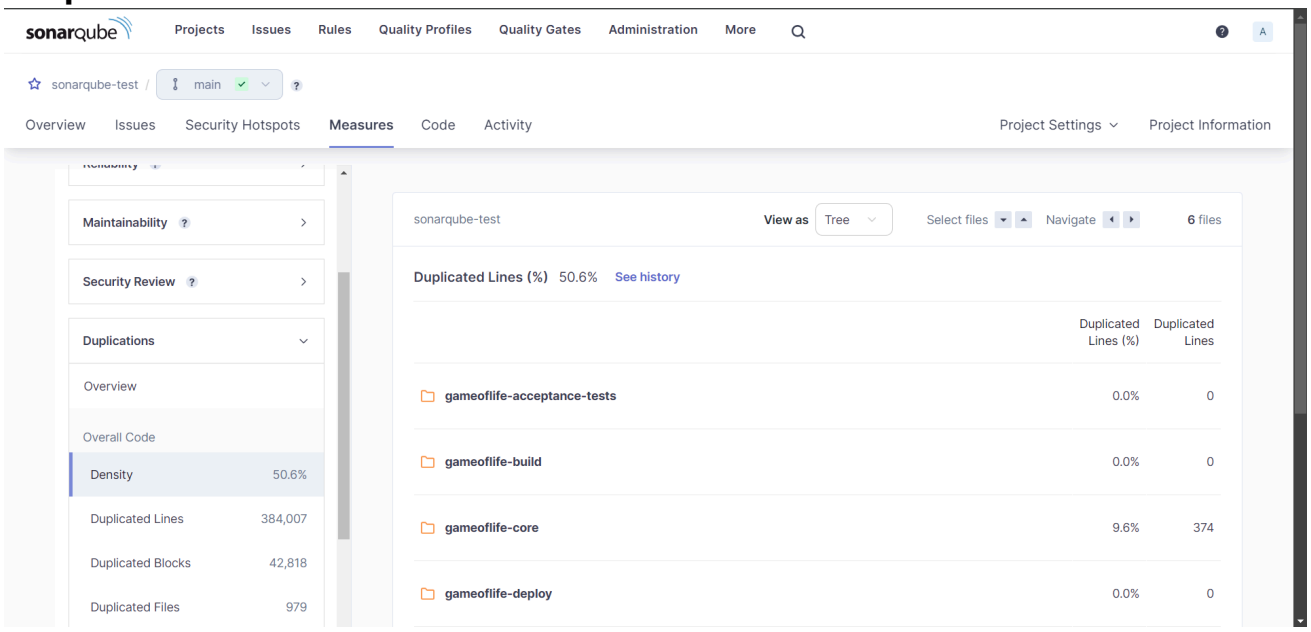
gameoflife-core/build/reports/tests/allclasses-frame.html

Embedded database should be used for evaluation purposes only
The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine

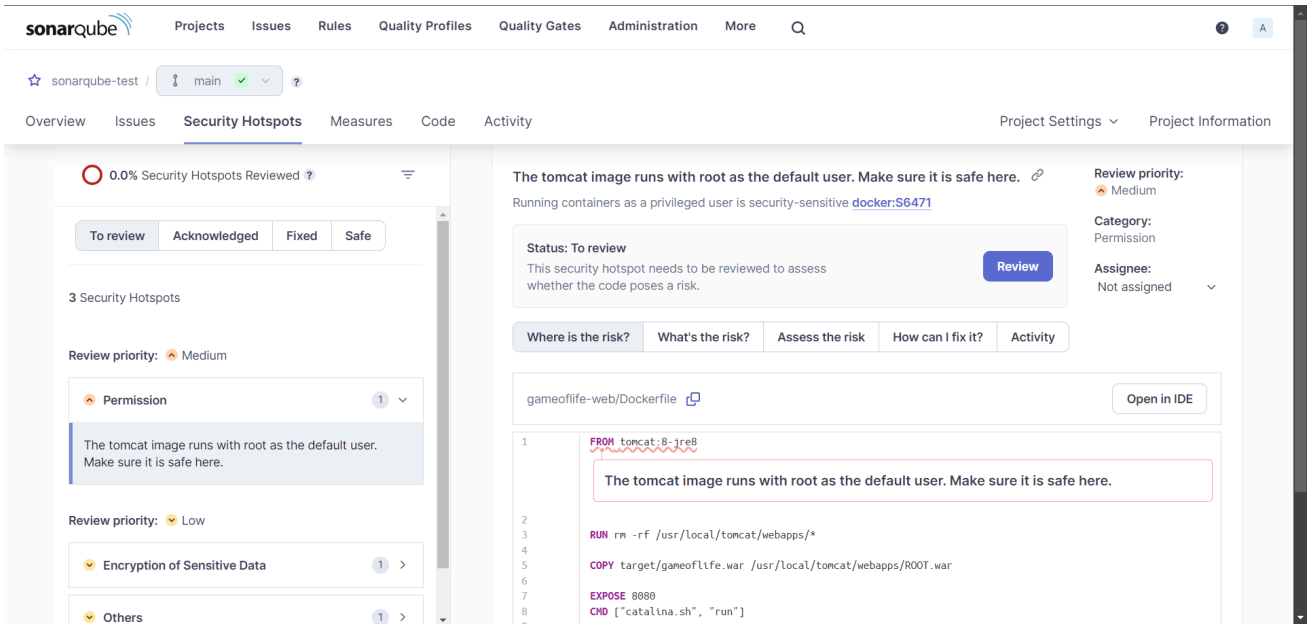
Reliability



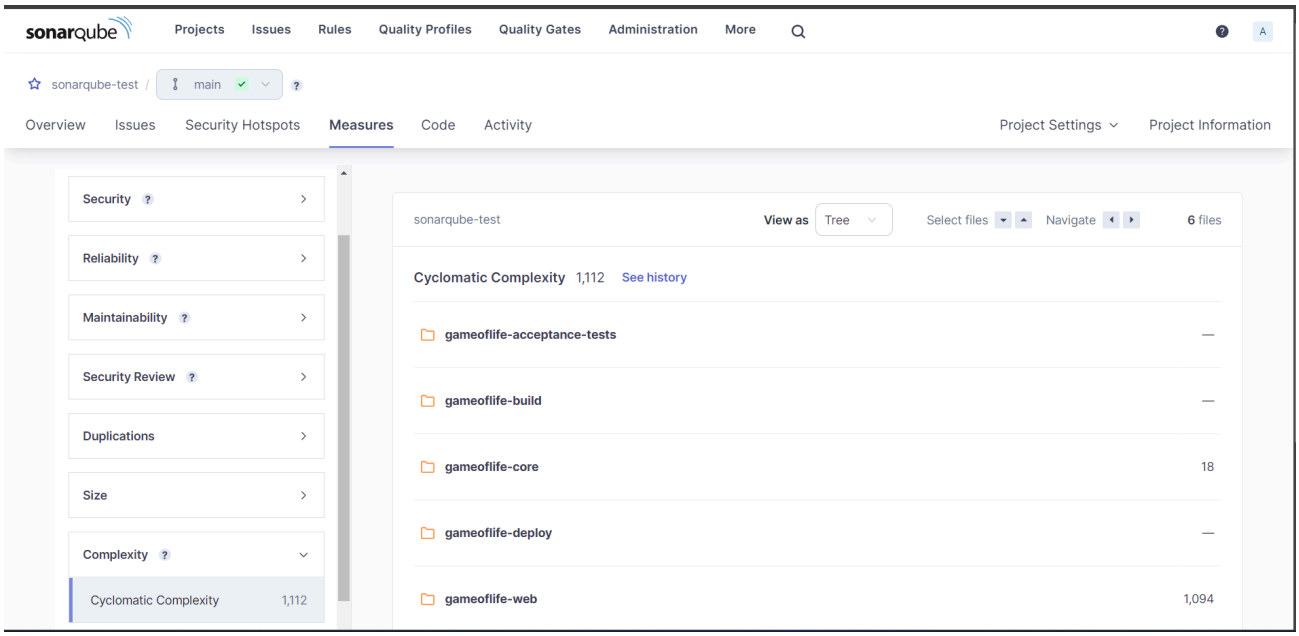
Duplicates



Security Hotspot



Cyclomatic Complexity



We have established a CI/CD pipeline using Jenkins and connected it with SonarQube to identify problems in the code, including bugs, code smells, duplicates, cyclomatic complexities, and more.

Conclusion:

In this experiment, we conducted a static code analysis on our sample Java application. This analysis aimed to identify various issues, including bugs, code smells, and security vulnerabilities. By leveraging tools like SonarQube, we gained insights into the code's quality and potential risks. The findings highlight areas for improvement and ensure better code maintainability. Overall, this process enhances the reliability of our application.