Name : Advik Ashok Hegde **Div/Roll No. : D15C/15**

Experiment - 8 :

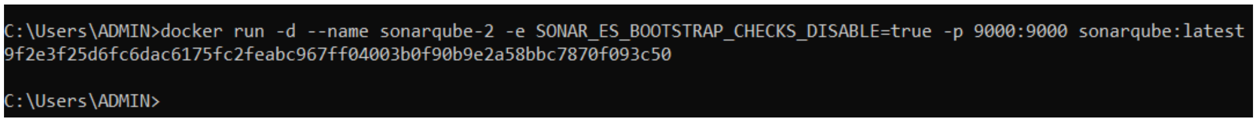
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

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

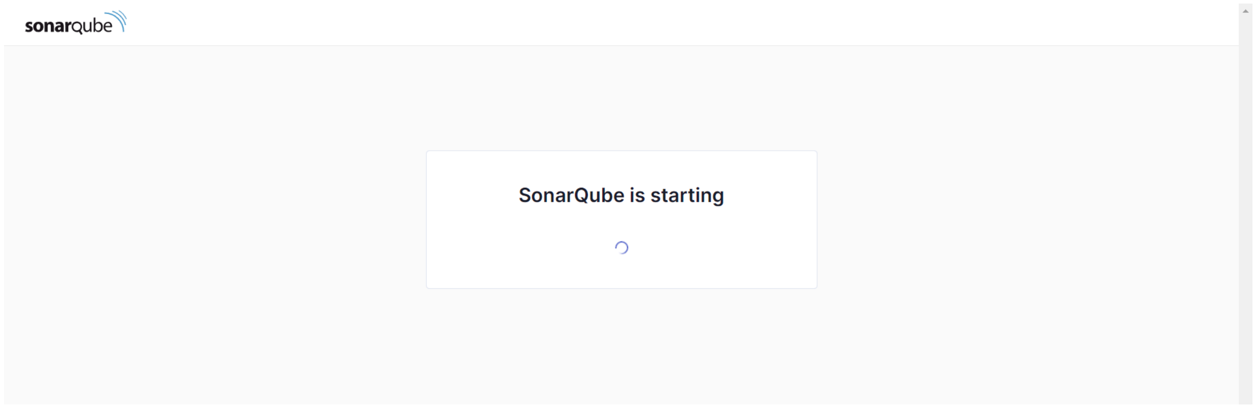
1. Open up Jenkins Dashboard on localhost, port 8080 or whichever port it is at for you.
2. Run SonarQube in a Docker container using this command -



```
C:\Users\ADMIN>docker run -d --name sonarqube-2 -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
9f2e3f25d6fc6dac6175fc2feabc967ff04003b0f90b9e2a58bbc7870f093c50

C:\Users\ADMIN>
```

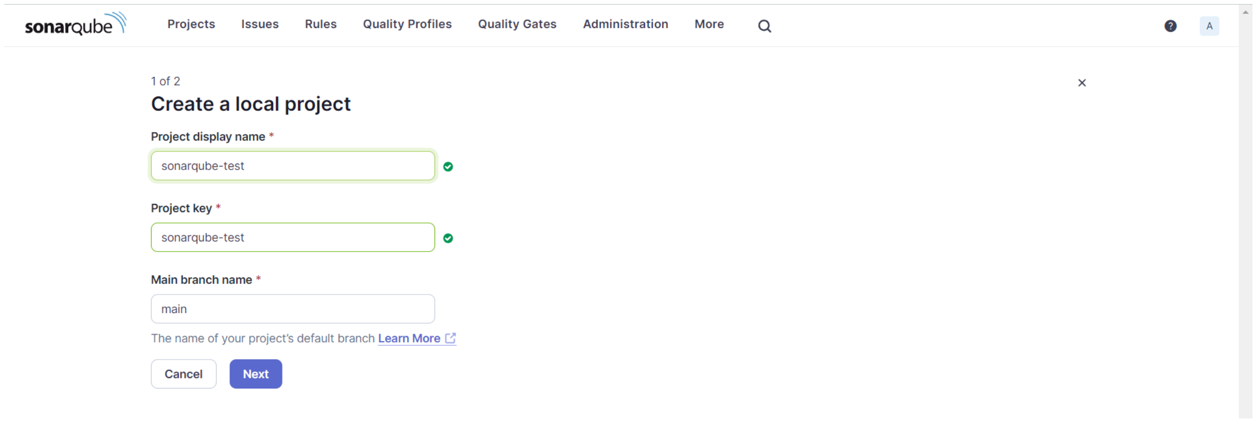
3. Once the container is up and running, you can check the status of SonarQube at localhost port 9000.



SonarQube is starting

4. Login to SonarQube using username *admin* and password which we reset to advik125!

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



1 of 2

Create a local project

Project display name *: sonarqube-test

Project key *: sonarqube-test

Main branch name *: main

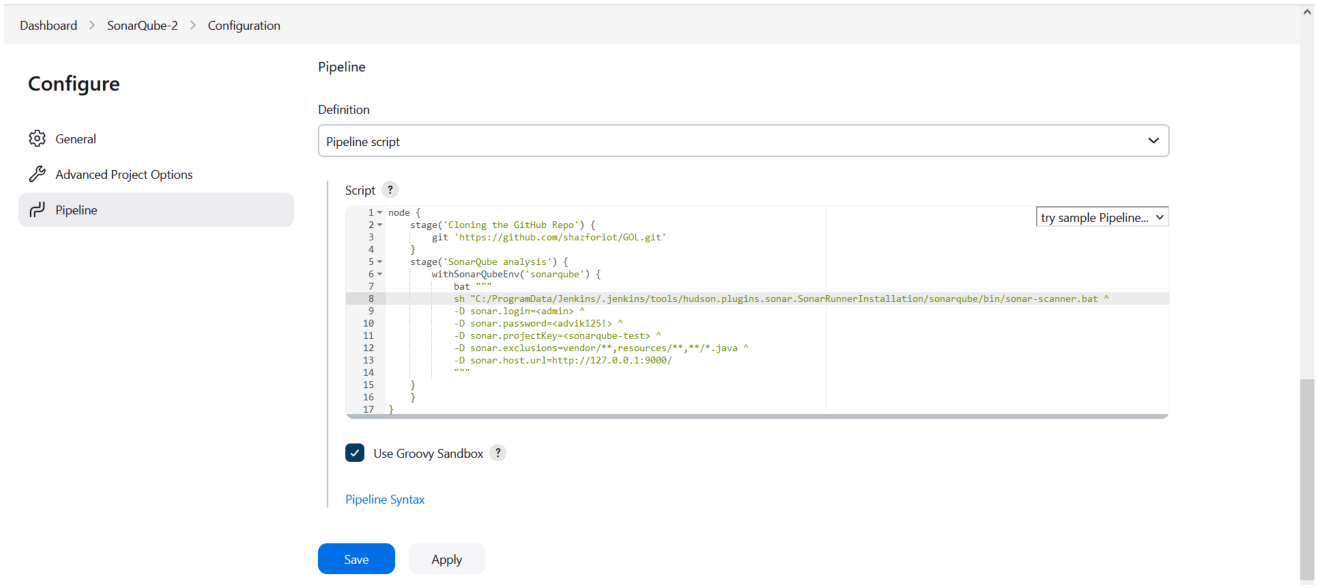
The name of your project's default branch Learn More

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 “””
             sh C:/ProgramData/Jenkins/.jenkins/tools/hudson.plugins.sonar.
             SonarRunnerInstallation/sonarqube/bin/sonar-scanner.bat ^
             -D sonar.login=<admin> ^
             -D sonar.password=<advik125!> ^
             -D sonar.projectKey=<sonarqube-test> ^
          -D sonar.exclusions=vendor/**,resources/**,**/*.java ^
             -D sonar.host.url=http://127.0.0.1:9000/"
             -D sonar.branch.name=main
           }
        }
      }
```



Pipeline

Definition

Pipeline script

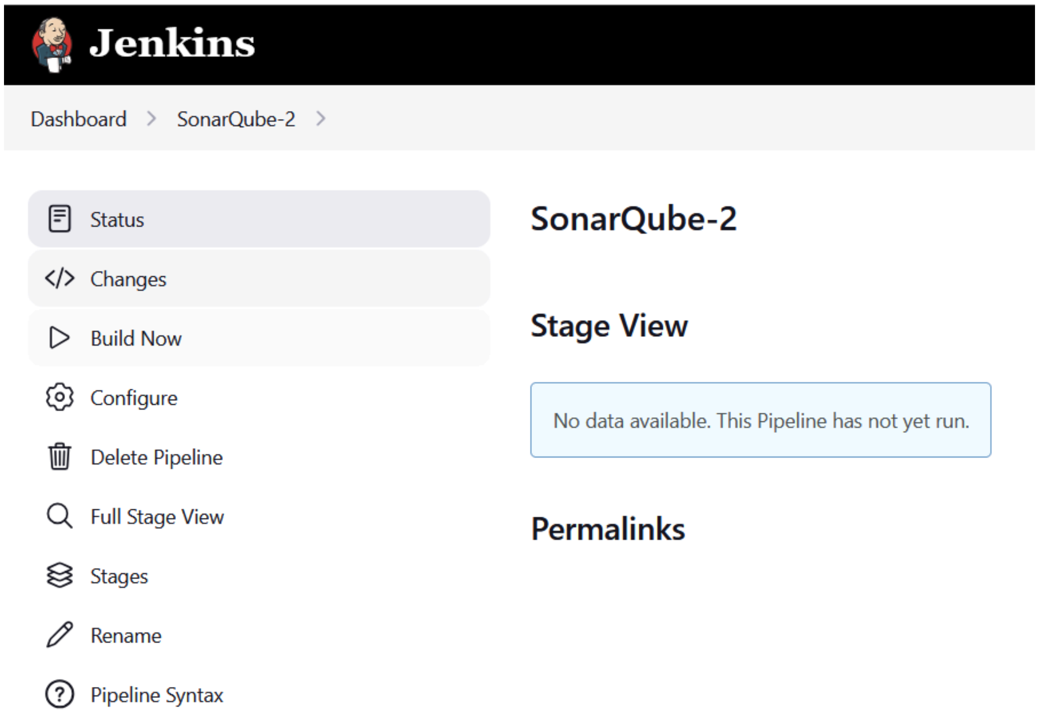
Script

```
node {
    stage('Cloning the GitHub Repo') {
        git 'https://github.com/shazforiot/GOL.git'
    }
    stage('SonarQube analysis') {
        withSonarQubeEnv('sonarqube') {
            bat """
            sh "C:/ProgramData/Jenkins/.jenkins/tools/hudson.plugins.sonar.SonarRunnerInstallation/sonarqube/bin/sonar-scanner.bat ^
            -D sonar.login=<admin> ^
            -D sonar.password=<advik125!> ^
            -D sonar.projectKey=<sonarqube-test> ^
            -D sonar.exclusions=vendor/**,resources/**,**/*.java ^
            -D sonar.host.url=http://127.0.0.1:9000/
            """
    }
    }
}
```

[✓] Use Groovy Sandbox

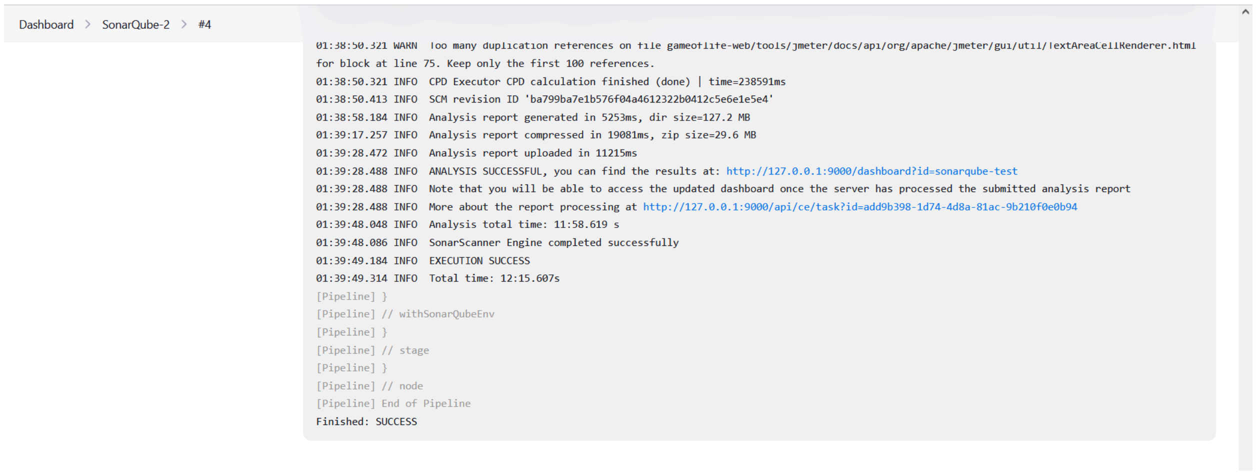
It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.

8. Run The Build.



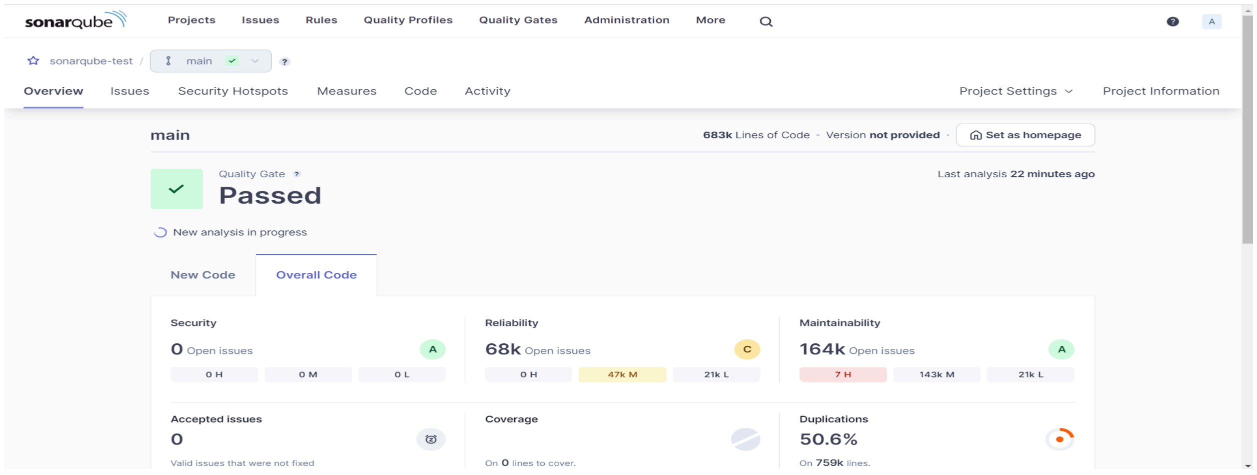
No data available. This Pipeline has not yet run.

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


Dashboard > SonarQube-2 > #4

```
01:38:50.321 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.
01:38:50.321 INFO  CPD Executor CPD calculation finished (done) | time=238591ms
01:38:50.413 INFO  SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
01:38:58.184 INFO  Analysis report generated in 5253ms, dir size=127.2 MB
01:39:17.257 INFO  Analysis report compressed in 19081ms, zip size=29.6 MB
01:39:28.472 INFO  Analysis report uploaded in 11215ms
01:39:28.488 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://127.0.0.1:9000/dashboard?id=sonarqube-test
01:39:28.488 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
01:39:28.488 INFO  More about the report processing at http://127.0.0.1:9000/api/ce/task?id=add9b398-1d74-4d8a-81ac-9b210f0e0b94
01:39:48.048 INFO  Analysis total time: 11:58.619 s
01:39:48.086 INFO  SonarScanner Engine completed successfully
01:39:49.184 INFO  EXECUTION SUCCESS
01:39:49.314 INFO  Total time: 12:15.607s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

10. After that, check the project in SonarQube.



main

683k Lines of Code · Version not provided

Quality Gate

Passed

Last analysis 22 minutes ago

New analysis in progress

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

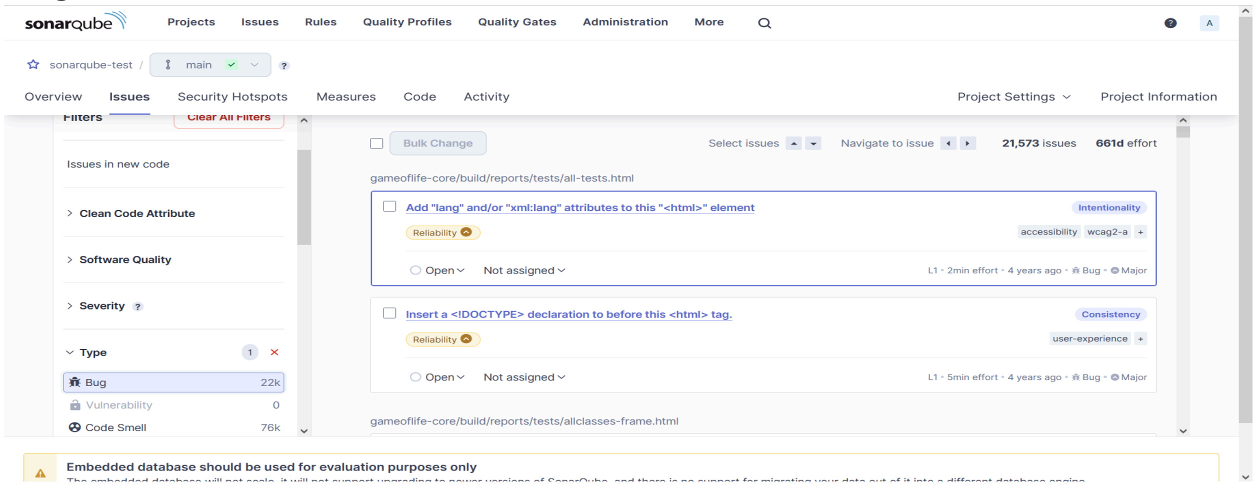
Accepted issues: 0 — Valid issues that were not fixed

Coverage: On 0 lines to cover.

Duplications: 50.6% — On 759k lines.

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

11. **Code Problems -**
Bugs :



Type 1

Bug 22k

Vulnerability 0

Code Smell 76k

21,573 issues 661d 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

Insert a <!DOCTYPE> declaration to before this <html> tag. Consistency

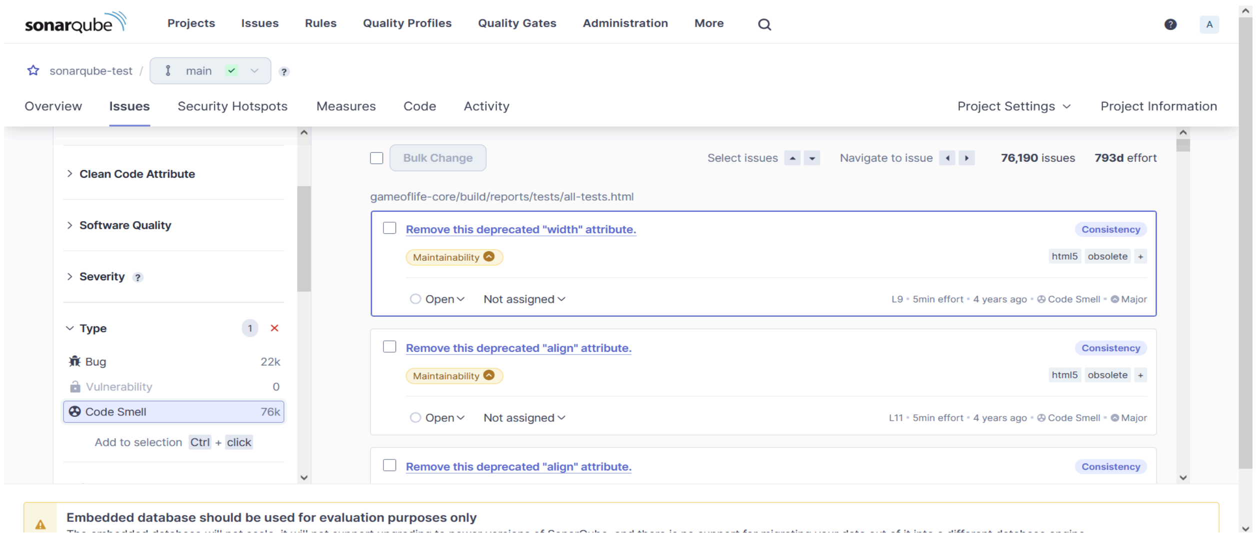
Reliability user-experience +

Open Not assigned L1 · 5min effort · 4 years ago · Bug · Major

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

Embedded database should be used for evaluation purposes only

Code smells :



sonarqube-test / main

Clean Code Attribute
Software Quality
Severity
Type 1
Bug 22k
Vulnerability 0
Code Smell 76k
Add to selection Ctrl + click

Bulk Change   Select issues   Navigate to issue   76,190 issues   793d effort

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

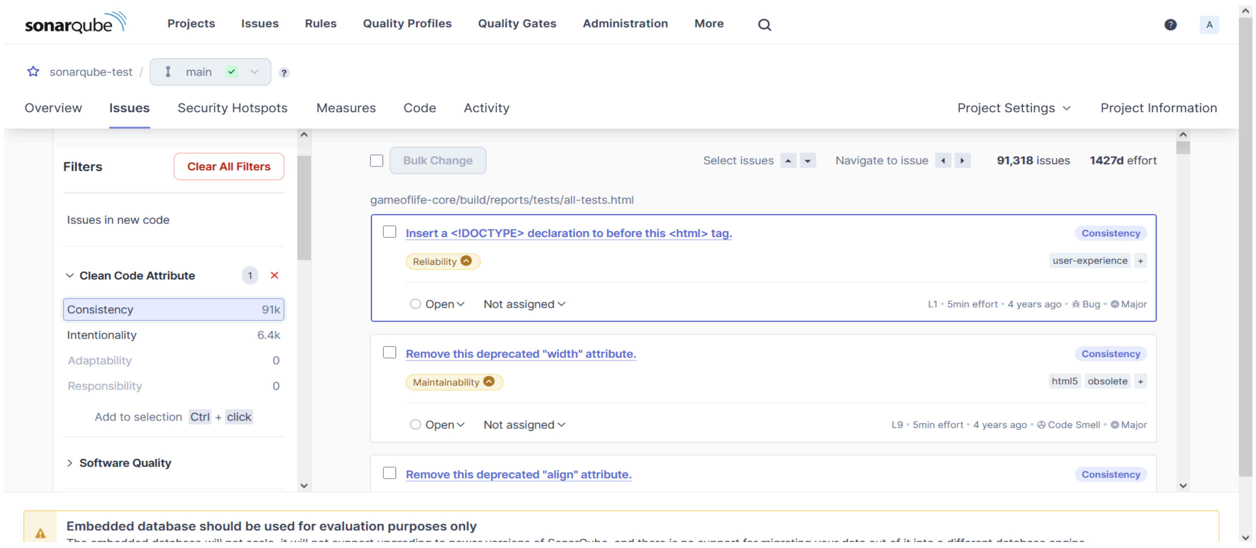
Remove this deprecated "width" attribute. — Consistency — Maintainability — html5 obsolete — Open — Not assigned — L9 · 5min effort · 4 years ago · Code Smell · Major

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

Embedded database should be used for evaluation purposes only

Clean Code Consistency issues:



sonarqube-test / main

Filters   Clear All Filters
Issues in new code
Clean Code Attribute 1
Consistency 91k
Intentionality 6.4k
Adaptability 0
Responsibility 0
Add to selection Ctrl + click
Software Quality

Bulk Change   Select issues   Navigate to issue   91,318 issues   1427d effort

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

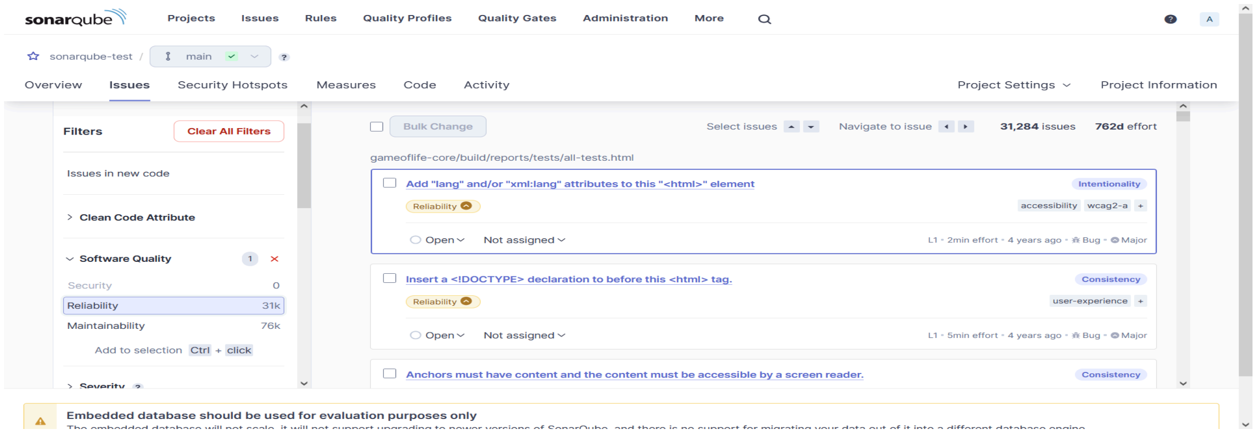
Insert a <!DOCTYPE> declaration to before this <html> tag. — Consistency — Reliability — user-experience — Open — Not assigned — L1 · 5min effort · 4 years ago · Bug · Major

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

Embedded database should be used for evaluation purposes only

Reliability Issues:



sonarqube-test / main

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

Filters Clear All Filters
Software Quality
Security 0
Reliability 31k
Maintainability 76k

31,284 issues 762d effort

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

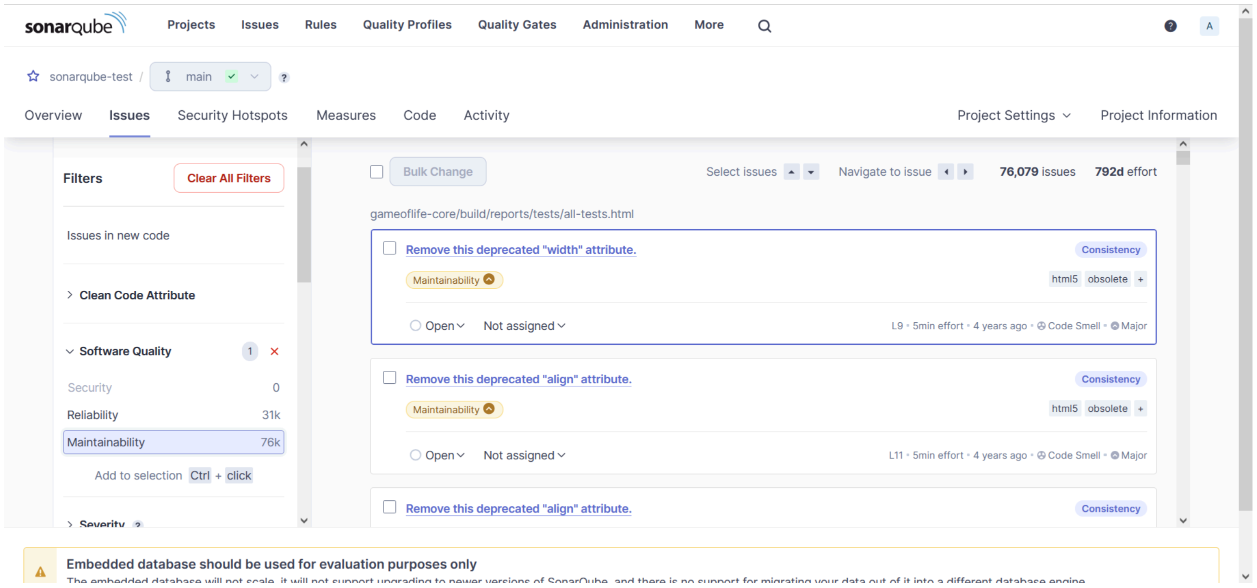
Insert a <!DOCTYPE> declaration to before this <html> tag. Consistency
Reliability user-experience
Open Not assigned L1 · 5min effort · 4 years ago · Bug · Major

Anchors must have content and the content must be accessible by a screen reader. Consistency

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.

Maintainability Issues:



sonarqube-test / main

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

Filters Clear All Filters
Software Quality
Security 0
Reliability 31k
Maintainability 76k

76,079 issues 792d effort

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

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.

Conclusion:

In this experiment, we set up a Jenkins CI/CD pipeline integrated with SonarQube to automate static analysis on a sample application. Jenkins was configured to trigger builds and run SonarQube's analysis with every code change, detecting bugs, code smells, and security vulnerabilities. This pipeline provided continuous monitoring and ensured early detection of issues, improving code quality and security. The experiment showcased how integrating CI/CD pipelines with SonarQube enhances development efficiency and ensures better, more reliable software.