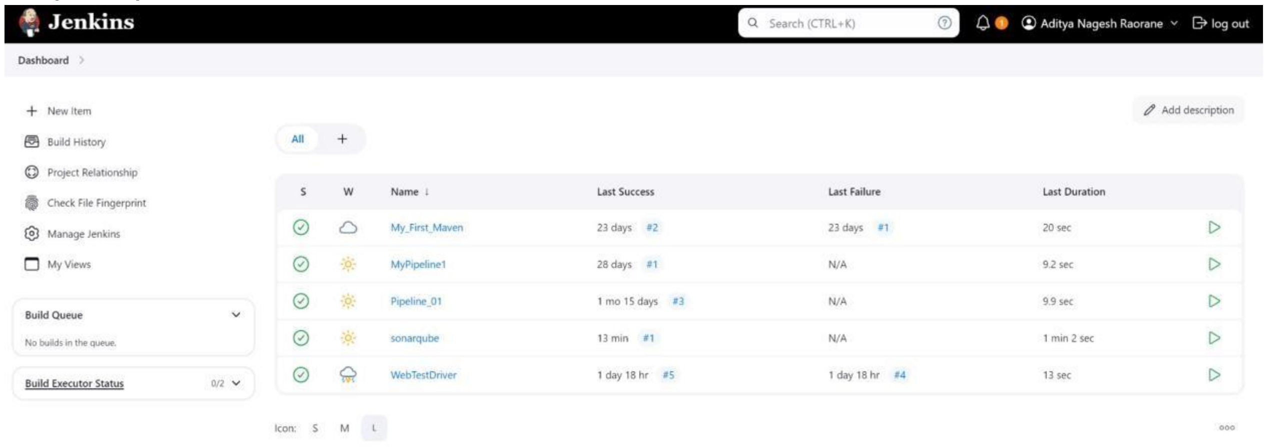
Name: Muskan chandiramani Class: D15C Roll No: 5

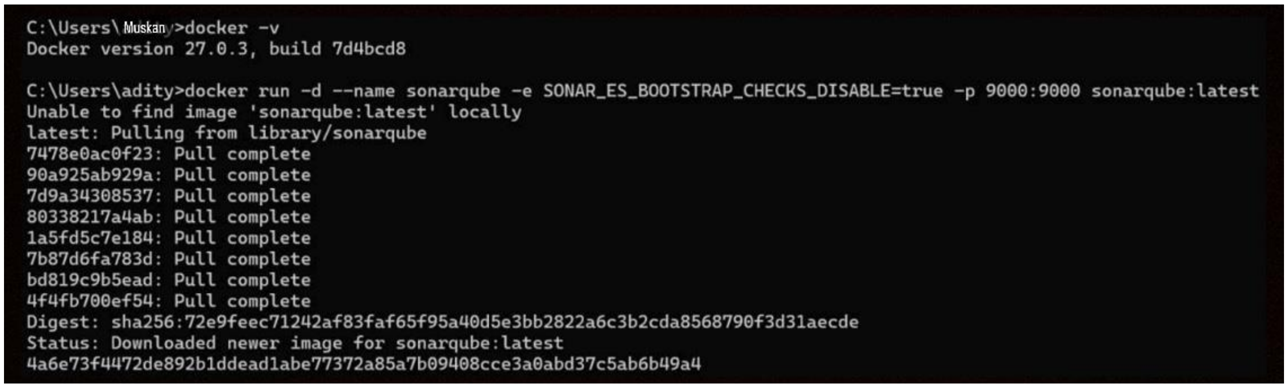
<u>Aim</u>: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

1. Open up Jenkins Dashboard on localhost:8080.



S	W	Name ↓	Last Success	Last Failure	Last Duration
✓		My_First_Maven	23 days #2	23 days #1	20 sec
✓		MyPipeline1	28 days #1	N/A	9.2 sec
✓		Pipeline_01	1 mo 15 days #3	N/A	9.9 sec
✓		sonarqube	13 min #1	N/A	1 min 2 sec
✓		WebTestDriver	1 day 18 hr #5	1 day 18 hr #4	13 sec

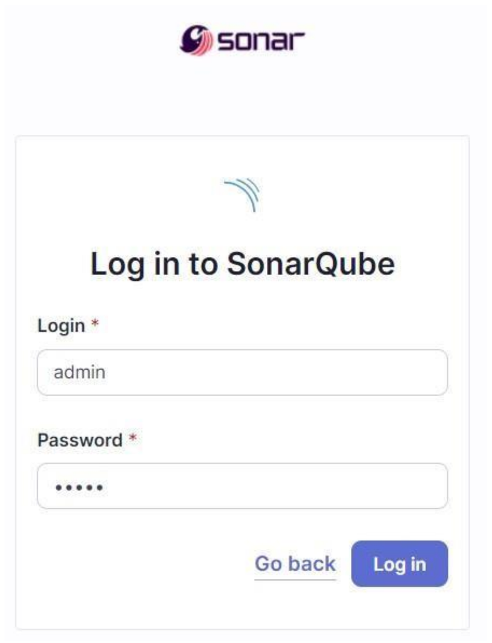
2. Run SonarQube in a Docker container using this command: a] docker -v b] docker pull sonarqube c] docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest



```
C:\Users\Muskan>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 “**mus12**”.



Log in to SonarQube

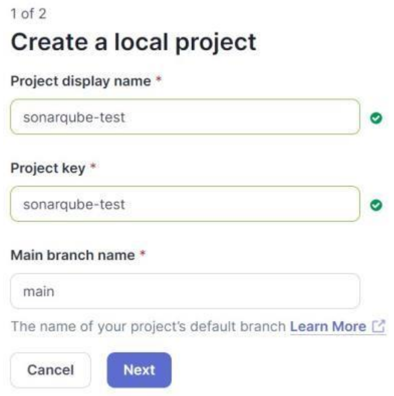
Login *

admin

Password *

•••••

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



1 of 2

Create a local project

Project display name *

sonarqube-test

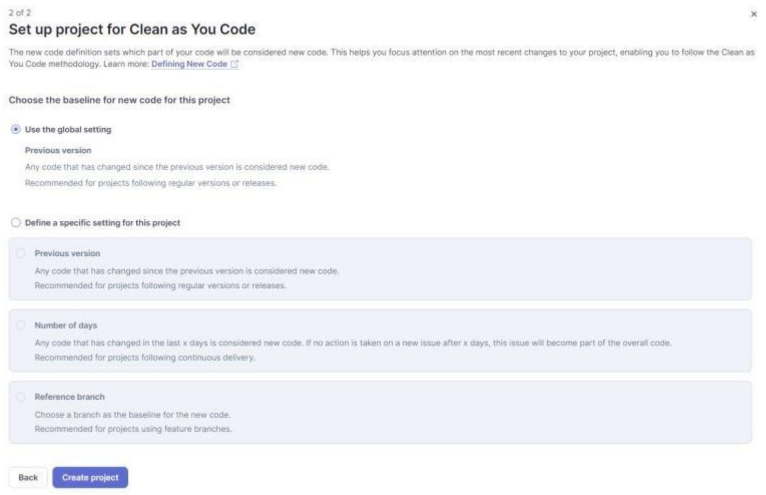
Project key *

sonarqube-test

Main branch name *

main

The name of your project's default branch Learn More



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

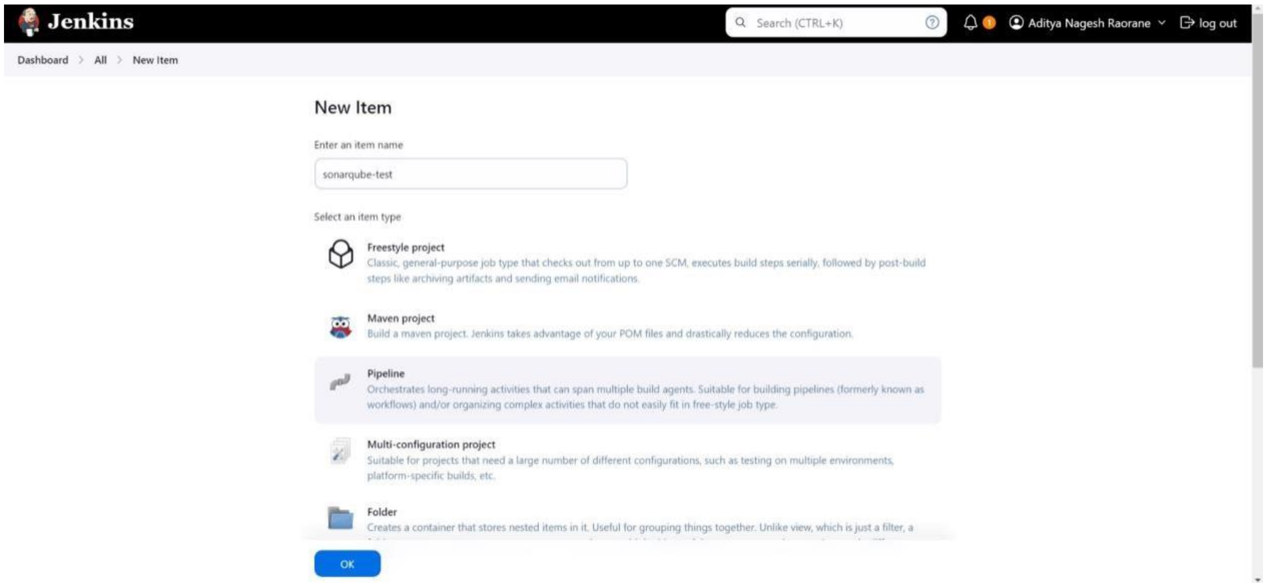
Any code that has changed in the last x days is considered new code. If no action is taken on a new issue after x days, this issue will become part of the overall code.
Recommended for projects following continuous delivery.

Reference branch

Choose a branch as the baseline for the new code.
Recommended for projects using feature branches.

Setup the project and come back to Jenkins Dashboard.

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



New Item

Enter an item name: sonarqube-test

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.

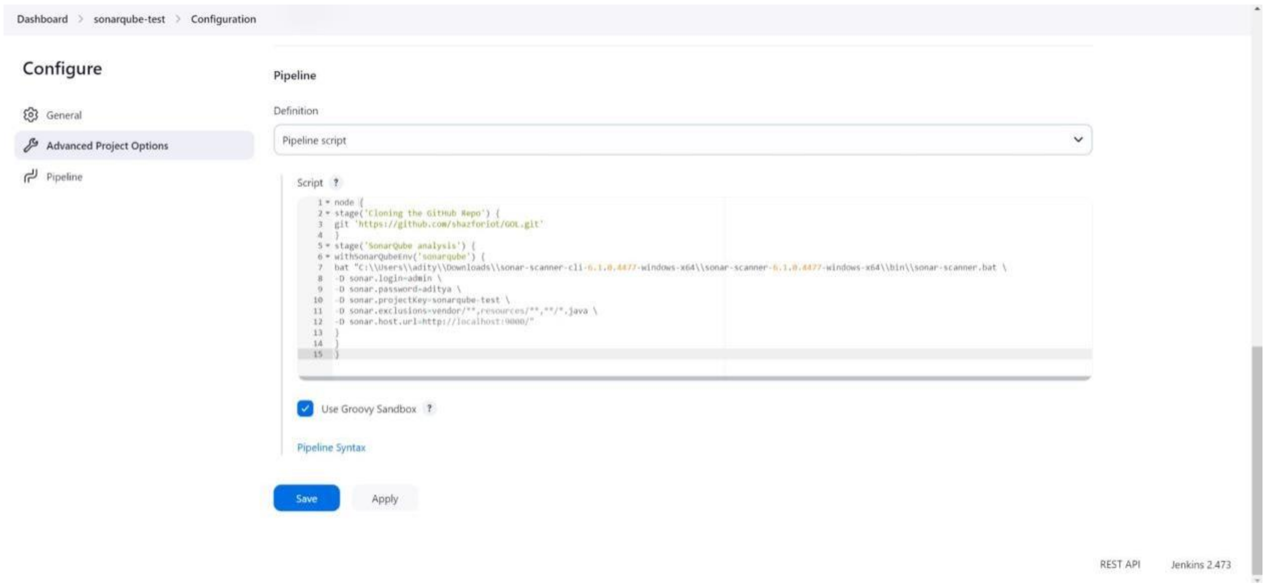
Pipeline
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

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

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/"
                }
        }
}
```



Pipeline

Definition: Pipeline script

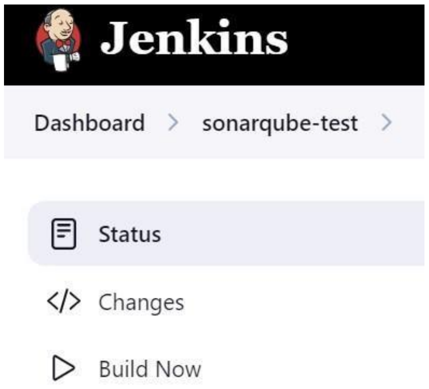
Script

```
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-scanner-6.1.0.4477-windows-x64\\bin\\sonar-scanner.bat \
-D sonar.login=admin \
-D sonar.password=aditya \
-D sonar.projectKey=sonarqube-test \
-D sonar.exclusions=vendor/**,resources/**,**/*.java \
-D sonar.host.url=http://localhost:9000/"
}
}
}
```

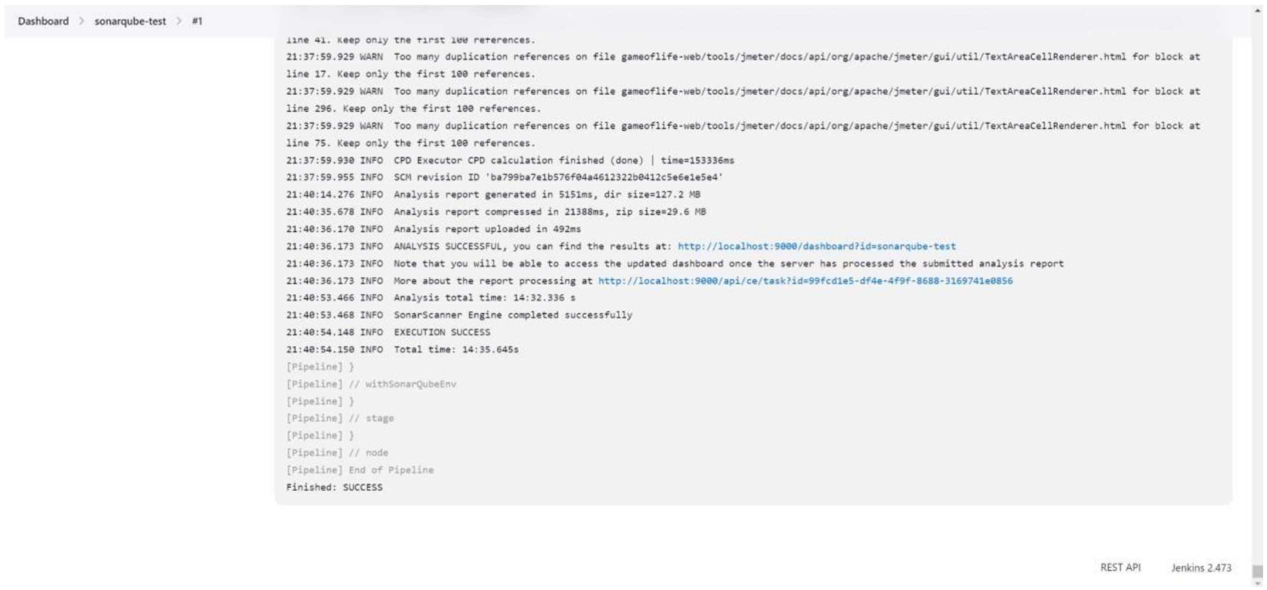
Use Groovy Sandbox [✓]

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

8. Run The Build.



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

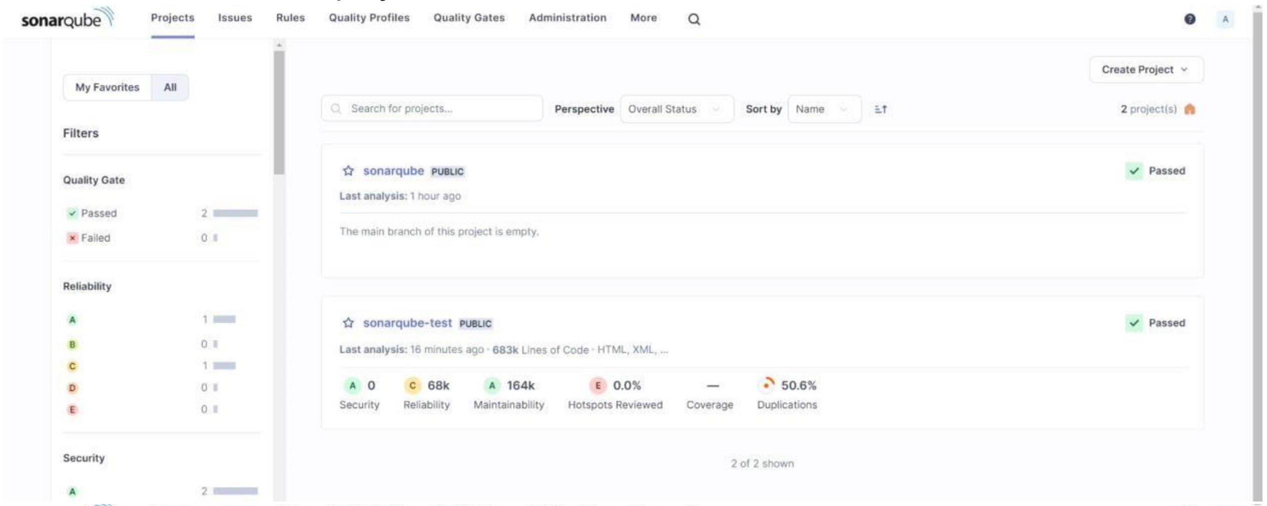


Dashboard > sonarqube-test > #1

```
line 41. Keep only the first 100 references.
21:37:59.929 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.
21:37:59.929 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.
21:37:59.929 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.
21:37:59.930 INFO  CPD Executor CPD calculation finished (done) | time=153336ms
21:37:59.955 INFO  SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
21:40:14.276 INFO  Analysis report generated in 5151ms, dir size=127.2 MB
21:40:35.678 INFO  Analysis report compressed in 21388ms, zip size=29.6 MB
21:40:36.170 INFO  Analysis report uploaded in 492ms
21:40:36.173 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube-test
21:40:36.173 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
21:40:36.173 INFO  More about the report processing at http://localhost:9000/api/ce/task?id=99fcd1e5-df4e-4f9f-8688-3169741e0856
21:40:53.466 INFO  Analysis total time: 14:32.336 s
21:40:53.468 INFO  SonarScanner Engine completed successfully
21:40:54.148 INFO  EXECUTION SUCCESS
21:40:54.150 INFO  Total time: 14:35.645s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

REST API Jenkins 2.473

10. After that, check the project in SonarQube.



Perspective Overall Status Sort by Name 2 project(s)

Filters

Quality Gate
- Passed 2
- Failed 0

Reliability
- A 1
- B 0
- C 1
- D 0
- E 0

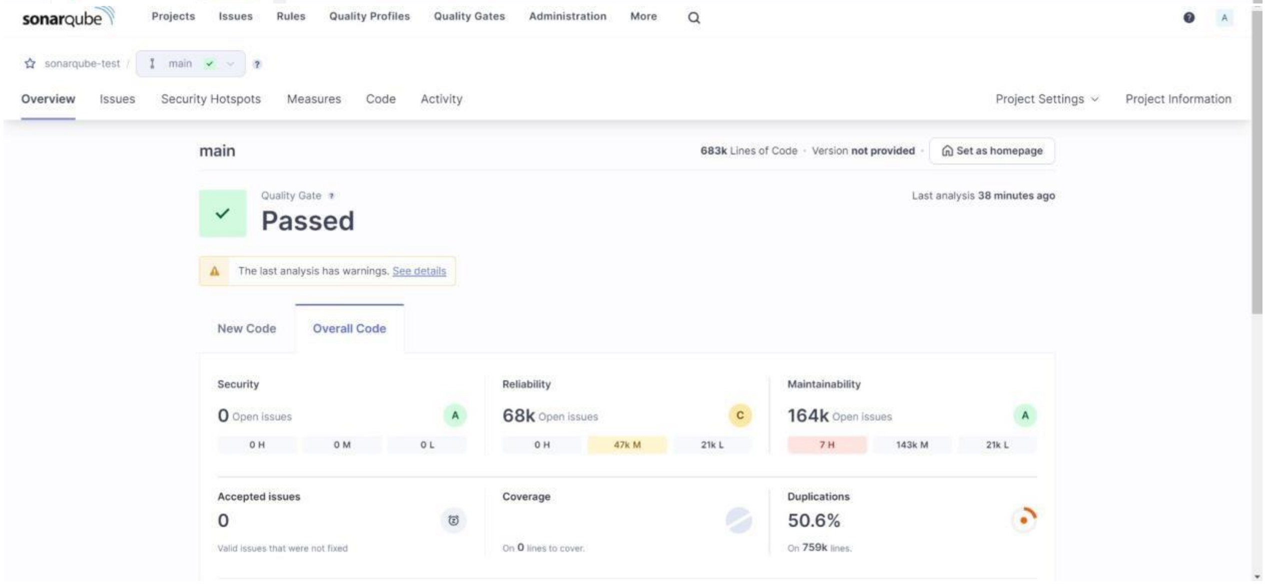
Security
- A 2

sonarqube PUBLIC — Passed
Last analysis: 1 hour ago
The main branch of this project is empty.

sonarqube-test PUBLIC — Passed
Last analysis: 16 minutes ago · 683k Lines of Code · HTML, XML, ...

A 0	C 68k	A 164k	E 0.0%	—	50.6%
Security	Reliability	Maintainability	Hotspots Reviewed	Coverage	Duplications

2 of 2 shown



main 683k Lines of Code · Version not provided

Quality Gate
Passed

Last analysis 38 minutes ago

The last analysis has warnings. See details

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)

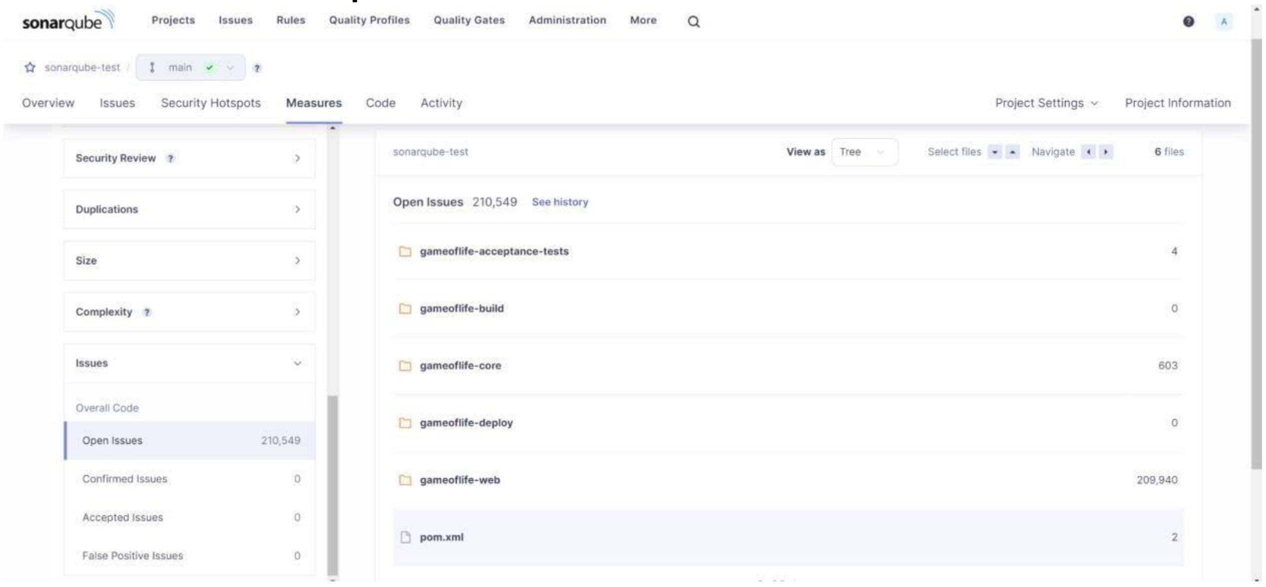
Accepted issues: 0 — Valid issues that were not fixed

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 Open Issues**


sonarqube
Projects Issues Rules Quality Profiles Quality Gates Administration More
sonarqube-test / main
Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information
Security Review
Duplications
Size
Complexity
Issues
View as Tree Select files Navigate

sonarqube-test — 6 files

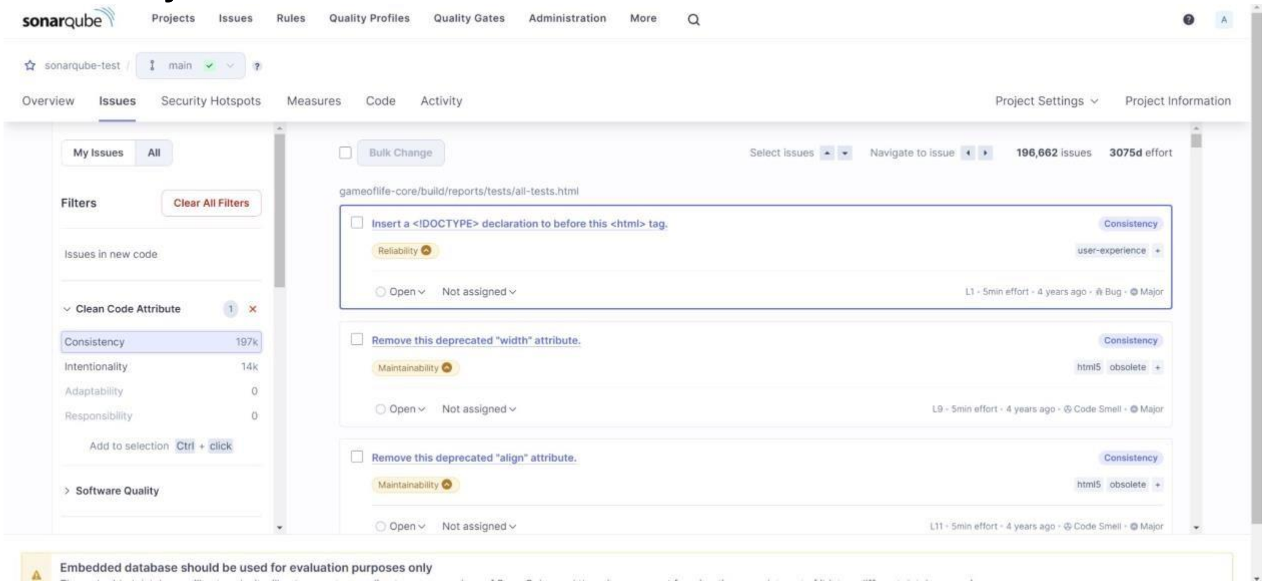
Open Issues 210,549 See history

gameoflife-acceptance-tests	4
gameoflife-build	0
gameoflife-core	603
gameoflife-deploy	0
gameoflife-web	209,940
pom.xml	2

Overall Code

Open Issues	210,549
Confirmed Issues	0
Accepted Issues	0
False Positive Issues	0

Consistency


sonarqube
Projects Issues Rules Quality Profiles Quality Gates Administration More
sonarqube-test / main
Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information
My Issues All
Filters Clear All Filters
Issues in new code
Bulk Change Select issues Navigate to issue
Add to selection Ctrl + click
Software Quality

Clean Code Attribute 1

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

196,662 issues 3075d effort

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

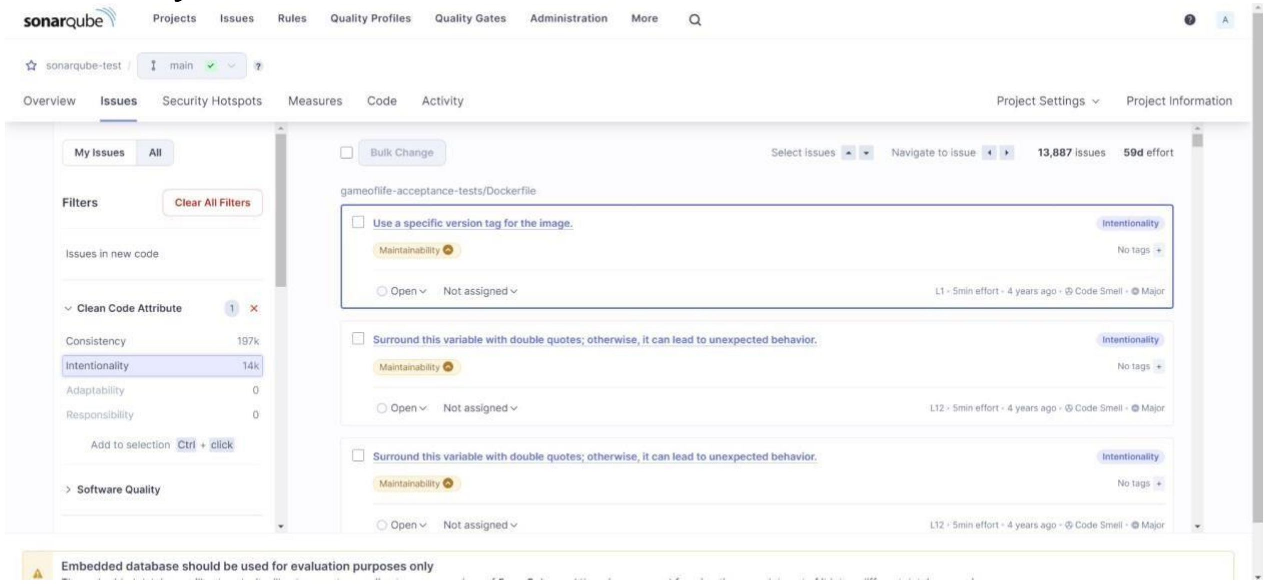
Insert a <!DOCTYPE> declaration to before this <html> tag. Consistency
Reliability user-experience
Open · Not assigned · L1 · 5min effort · 4 years ago · Bug · Major

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

Embedded database should be used for evaluation purposes only

Intentionality



13,887 issues 59d effort

Issues in new code

Clean Code Attribute 1

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection Ctrl + click

Software Quality

gameoflife-acceptance-tests/Dockerfile

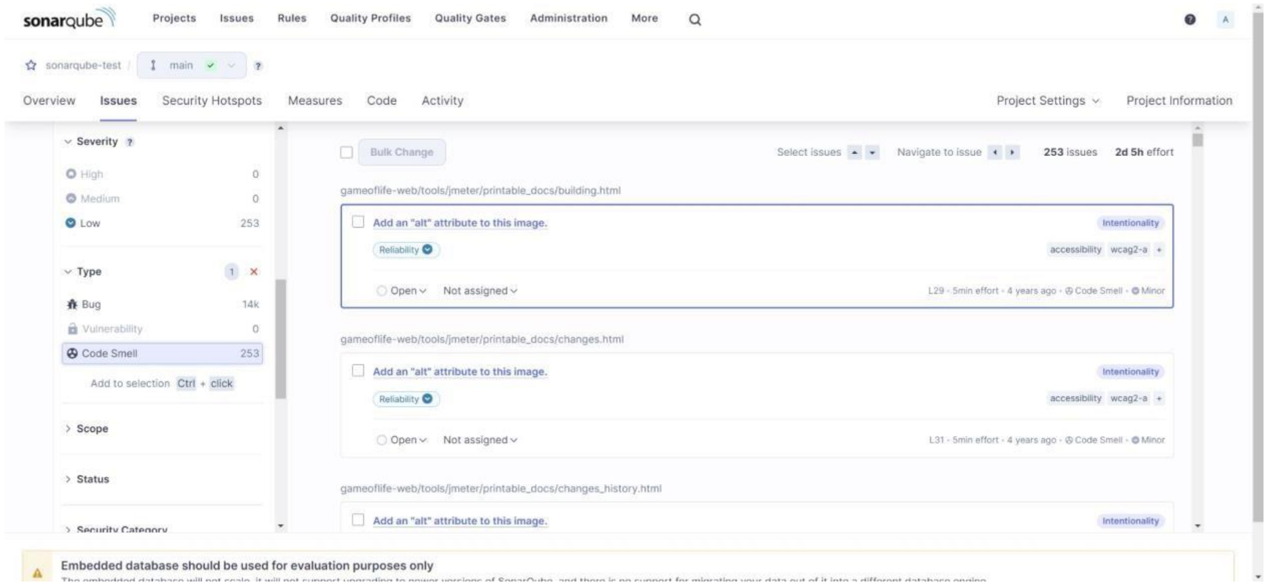
Use a specific version tag for the image. Intentionality
Maintainability No tags
Open Not assigned L1 · 5min effort · 4 years ago · Code Smell · Major

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

Embedded database should be used for evaluation purposes only

Code Smells



253 issues 2d 5h effort

Severity

High	0
Medium	0
Low	253

Type 1

Bug	14k
Vulnerability	0
Code Smell	253

Add to selection Ctrl + click

Scope

Status

Security Category

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

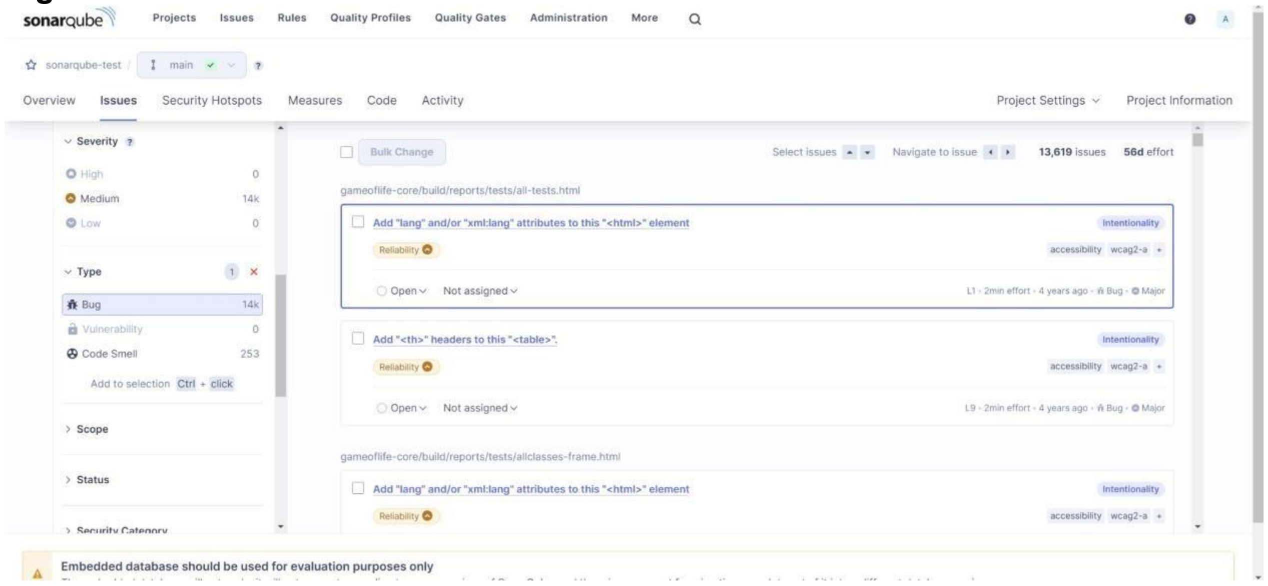
Add an "alt" attribute to this image. Intentionality
Reliability accessibility wcag2-a
Open Not assigned L31 · 5min effort · 4 years ago · Code Smell · Minor

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
Bulk Change
Select issues Navigate to issue

13,619 issues 56d effort

Severity: High 0, Medium 14k, Low 0

Type: Bug 14k, Vulnerability 0, Code Smell 253

Add to selection Ctrl + click

Scope

Status

Security Category

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

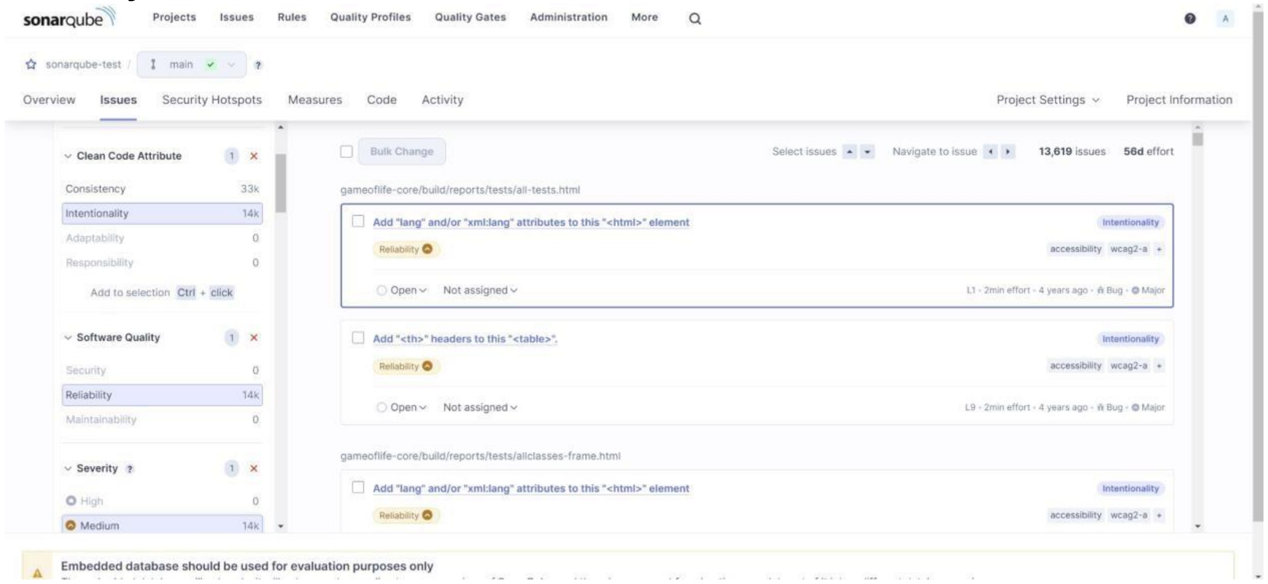
Add "<th>" headers to this "<table>".
Intentionality
Reliability
accessibility wcag2-a
Open
Not assigned
L9 · 2min effort · 4 years ago · Bug · Major

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



sonarqube
Projects Issues Rules Quality Profiles Quality Gates Administration More
sonarqube-test / main
Overview Issues Security Hotspots Measures Code Activity Project Settings Project Information
Bulk Change
Select issues Navigate to issue

13,619 issues 56d effort

Clean Code Attribute: Consistency 33k, Intentionality 14k, Adaptability 0, Responsibility 0

Add to selection Ctrl + click

Software Quality: Security 0, Reliability 14k, Maintainability 0

Severity: High 0, Medium 14k

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

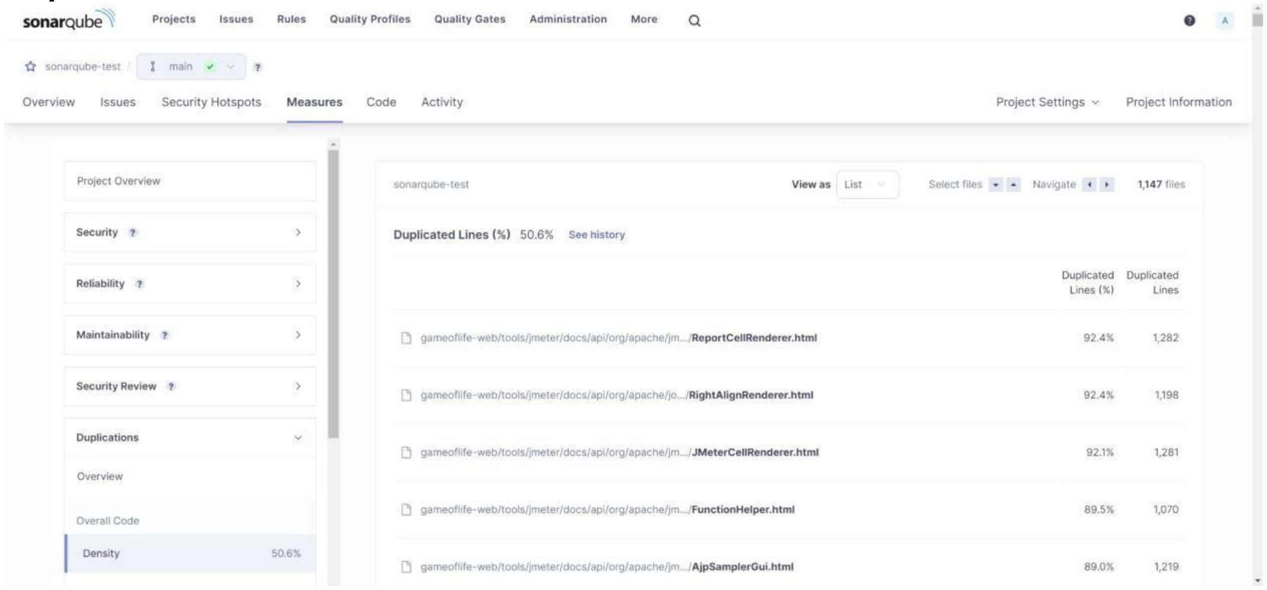
gameoflife-core/build/reports/tests/allclasses-frame.html

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

Name: Muskan chandiramani Class: D15C Roll No: 5

Duplicates



sonarqube
Projects Issues Rules Quality Profiles Quality Gates Administration More
sonarqube-test / main
Overview Issues Security Hotspots Measures Code Activity
Project Settings Project Information
Project Overview
Security
Reliability
Maintainability
Security Review
Duplications
Overview
Overall Code

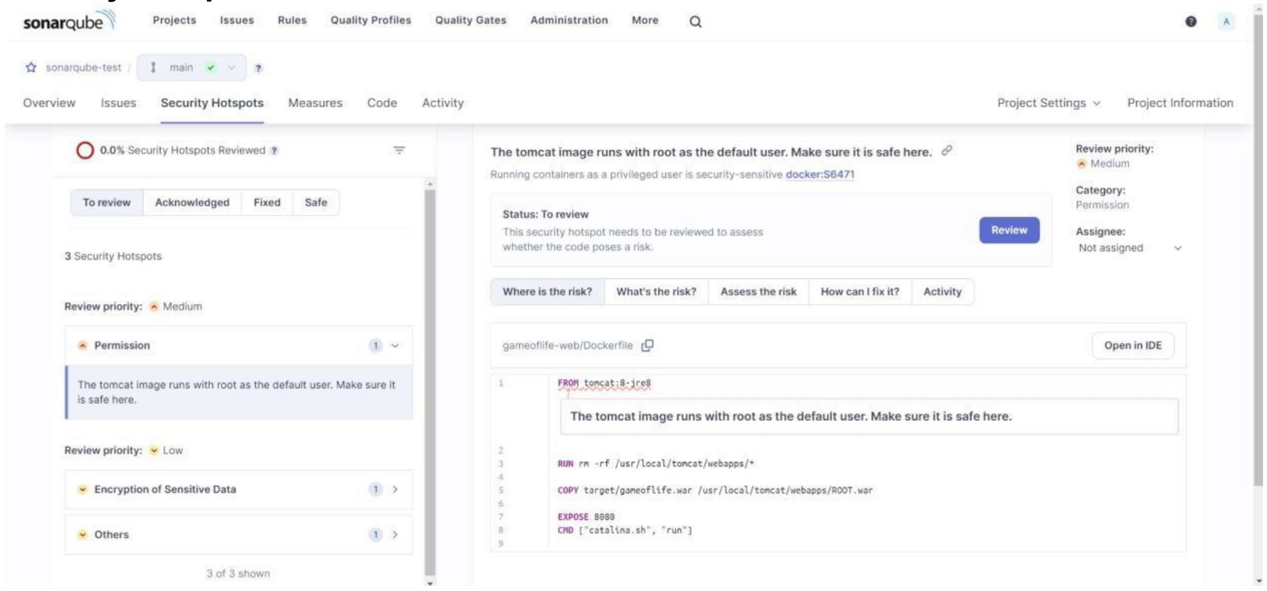
Density 50.6%

sonarqube-test View as List Select files Navigate 1,147 files

Duplicated Lines (%) 50.6% See history

	Duplicated Lines (%)	Duplicated Lines
gameoflife-web/tools/jmeter/docs/api/org/apache/jm.../ReportCellRenderer.html	92.4%	1,282
gameoflife-web/tools/jmeter/docs/api/org/apache/jo.../RightAlignRenderer.html	92.4%	1,198
gameoflife-web/tools/jmeter/docs/api/org/apache/jm.../JMeterCellRenderer.html	92.1%	1,281
gameoflife-web/tools/jmeter/docs/api/org/apache/jm.../FunctionHelper.html	89.5%	1,070
gameoflife-web/tools/jmeter/docs/api/org/apache/jm.../AjpSamplerGui.html	89.0%	1,219

Security Hotspot



sonarqube
Projects Issues Rules Quality Profiles Quality Gates Administration More
sonarqube-test / main
Overview Issues Security Hotspots Measures Code Activity
Project Settings Project Information
To review Acknowledged Fixed Safe
Review
Where is the risk? What's the risk? Assess the risk How can I fix it? Activity
Open in IDE

0.0% Security Hotspots Reviewed

3 Security Hotspots

Review priority: Medium

Permission 1

The tomcat image runs with root as the default user. Make sure it is safe here.

Review priority: Low

Encryption of Sensitive Data 1

Others 1

3 of 3 shown

The tomcat image runs with root as the default user. Make sure it is safe here.

Running containers as a privileged user is security-sensitive docker:S6471

Status: To review

This security hotspot needs to be reviewed to assess whether the code poses a risk.

Review priority: Medium

Category: Permission

Assignee: Not assigned

gameoflife-web/Dockerfile

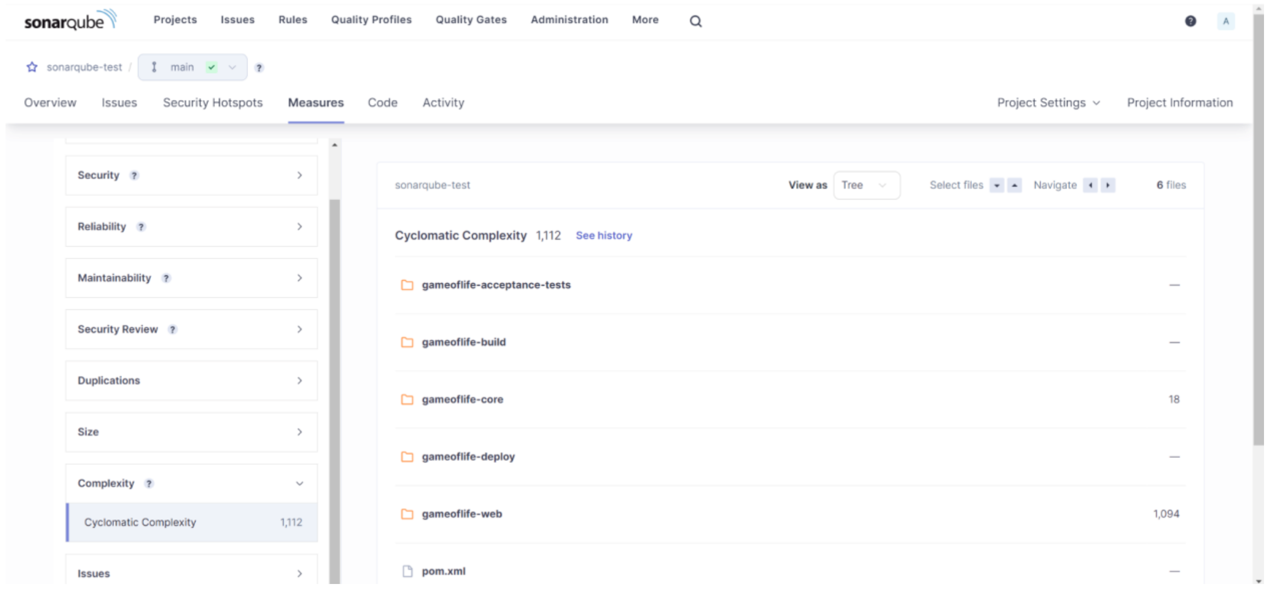
```
FROM tomcat:8-jre8
The tomcat image runs with root as the default user. Make sure it is safe here.

RUN rm -rf /usr/local/tomcat/webapps/*

COPY target/gameoflife.war /usr/local/tomcat/webapps/ROOT.war

EXPOSE 8080
CMD ["catalina.sh", "run"]
```

Cyclomatic Complexity



sonarqube-test

Cyclomatic Complexity 1,112 See history

gameoflife-acceptance-tests	—
gameoflife-build	—
gameoflife-core	18
gameoflife-deploy	—
gameoflife-web	1,094
pom.xml	—

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.