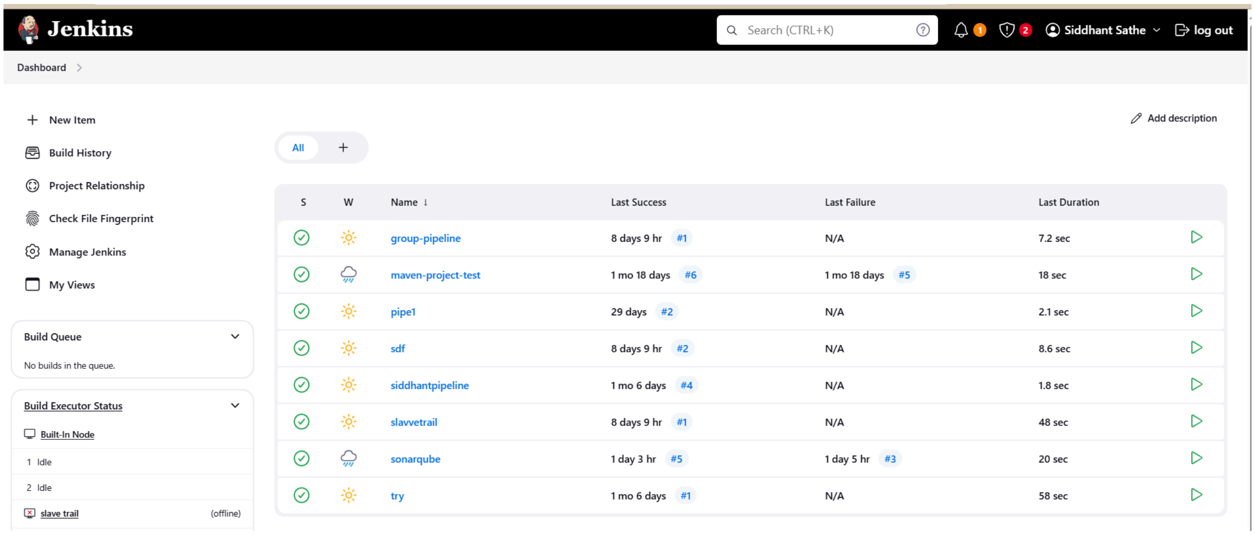
Siddhant Sathe **D15A/51**

Experiment 8

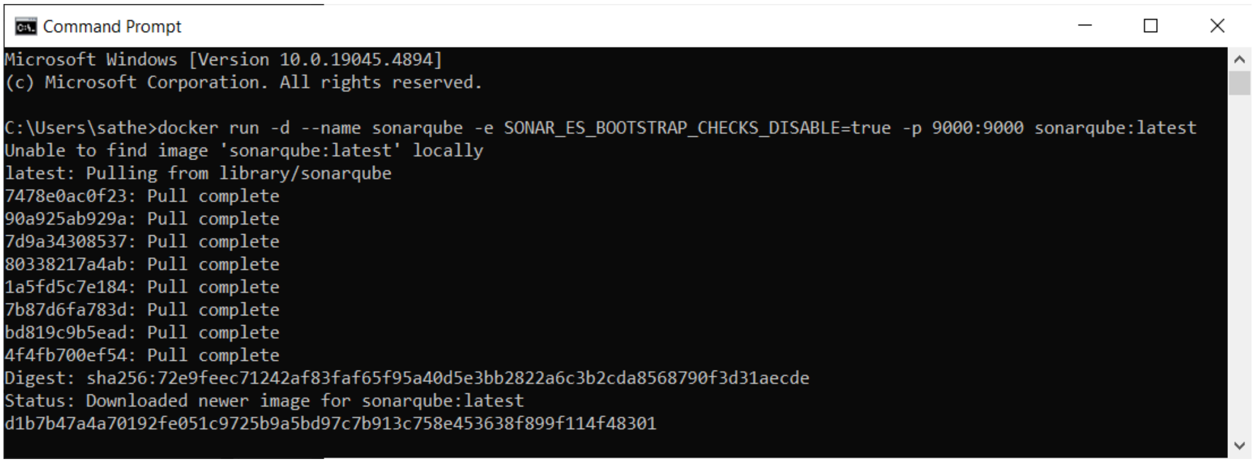
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

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



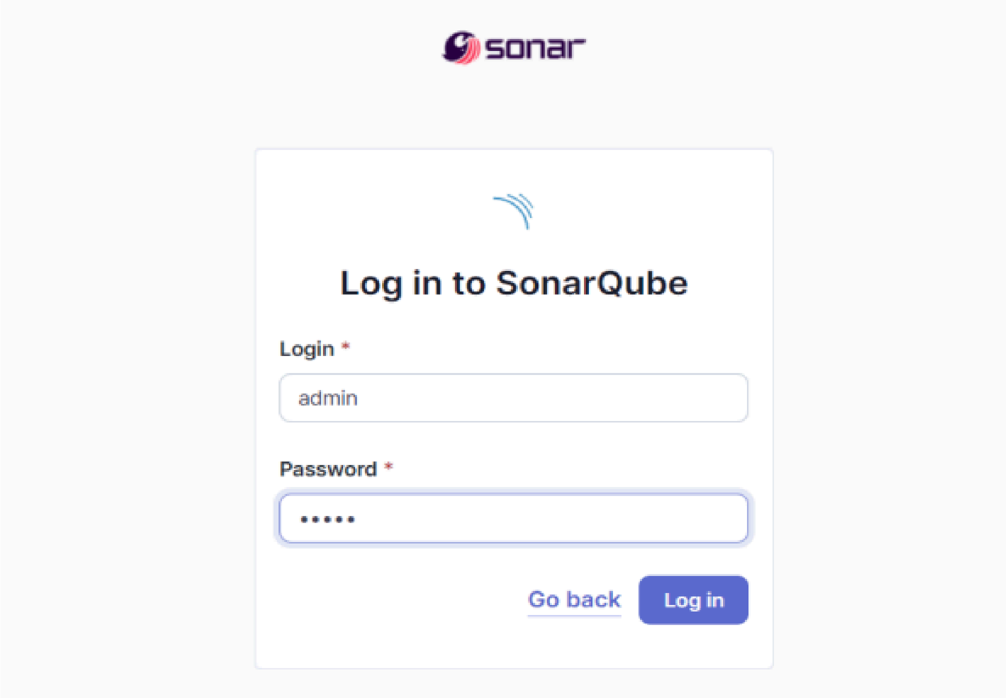
S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☀	group-pipeline	8 days 9 hr #1	N/A	7.2 sec
✓	☁	maven-project-test	1 mo 18 days #6	1 mo 18 days #5	18 sec
✓	☀	pipe1	29 days #2	N/A	2.1 sec
✓	☀	sdf	8 days 9 hr #2	N/A	8.6 sec
✓	☀	siddhantpipeline	1 mo 6 days #4	N/A	1.8 sec
✓	☀	slavvetrail	8 days 9 hr #1	N/A	48 sec
✓	☁	sonarqube	1 day 3 hr #5	1 day 5 hr #3	20 sec
✓	☀	try	1 mo 6 days #1	N/A	58 sec

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



```
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sathe>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
d1b7b47a4a70192fe051c9725b9a5bd97c7b913c758e453638f899f114f48301
```

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



Log in to SonarQube

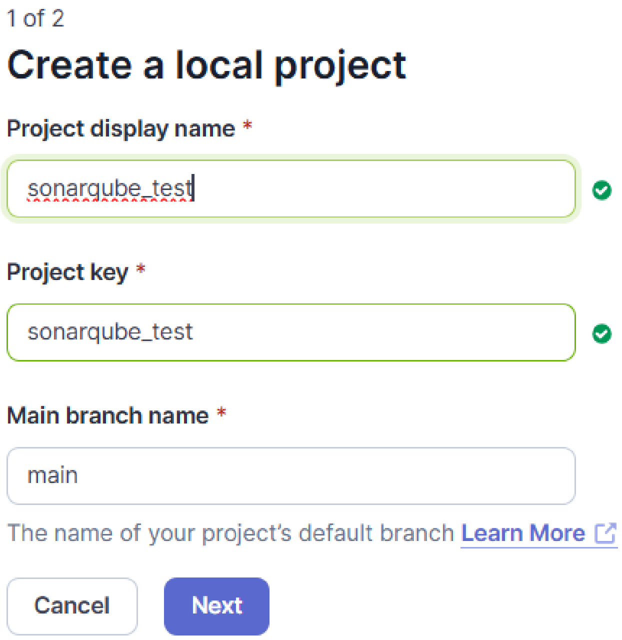
Login *

admin

Password *

•••••

Step-4: Create a local project in SonarQube with the name sonarqube-pipeline.



1 of 2

Create a local project

Project display name *

sonarqube_test

Project key *

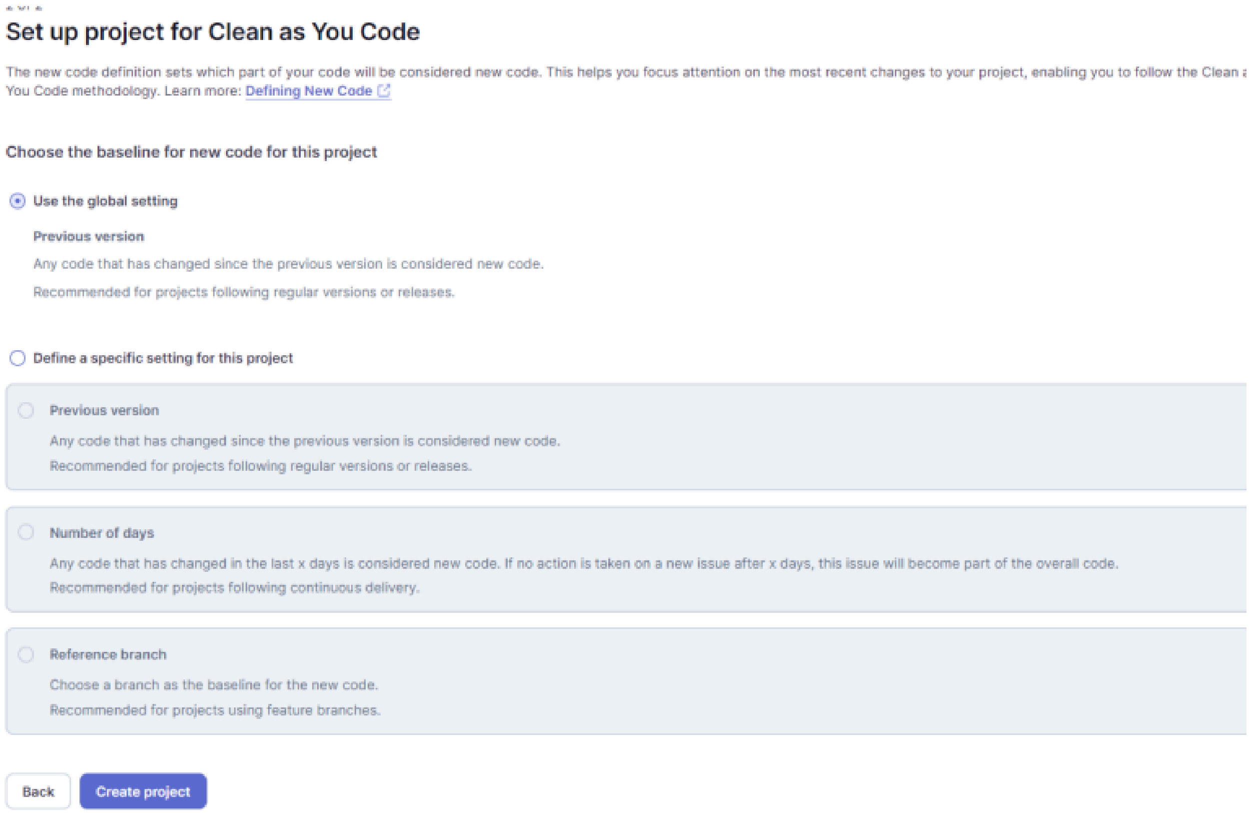
sonarqube_test

Main branch name *

main

The name of your project's default branch Learn More

Step-5: Setup the project and come back to Jenkins Dashboard.



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
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.

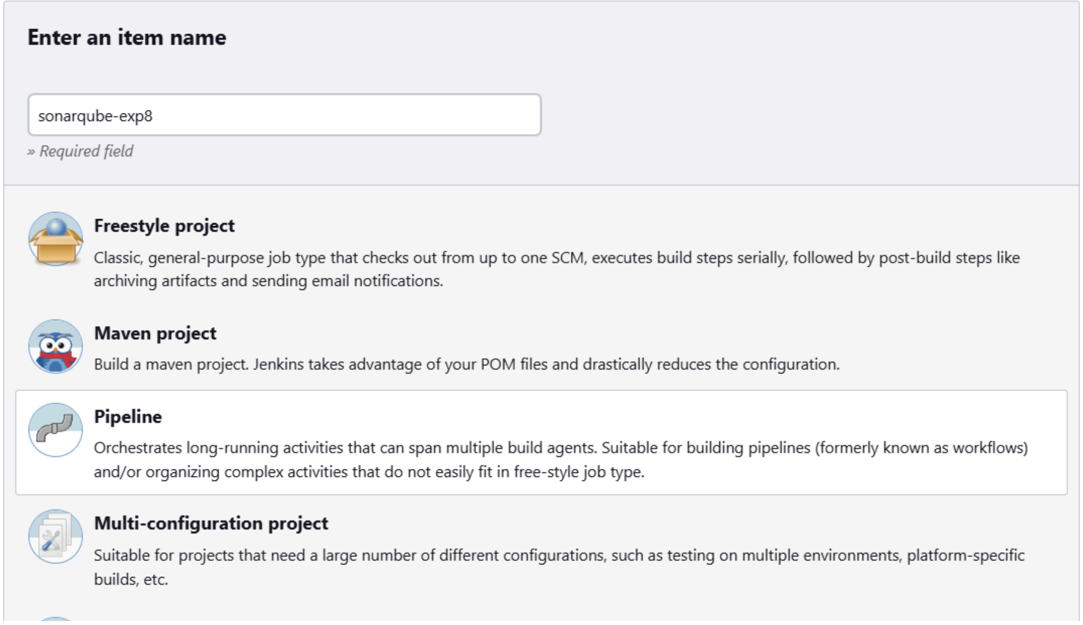
○ Reference branch

Choose a branch as the baseline for the new code.

Recommended for projects using feature branches.

Back | Create project

Step-6: Create a New Item in Jenkins, choose Pipeline.



Enter an item name

sonarqube-exp8

» *Required field*

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

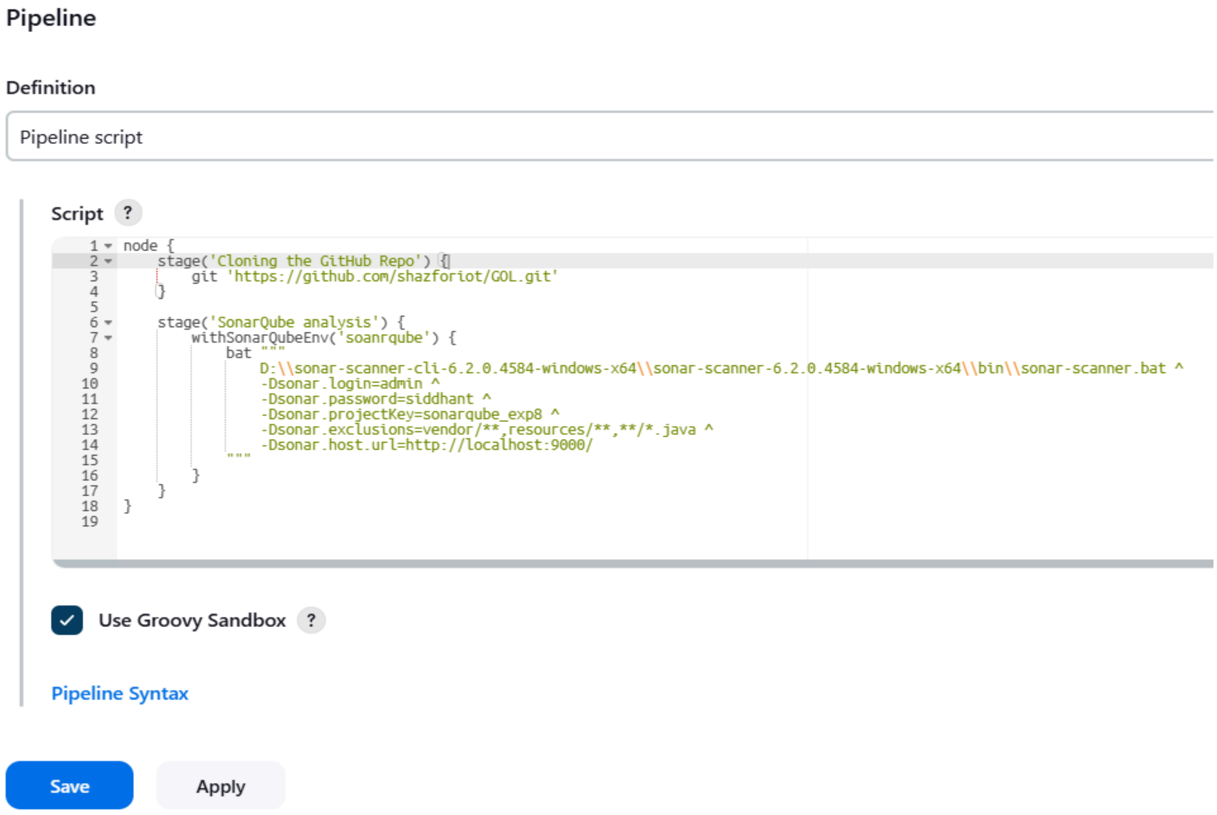
Orchestrates long-running activities that can span multiple build agents. Suitable for building pipelines (formerly known as workflows) and/or organizing complex activities that do not easily fit in free-style job type.

Multi-configuration project

Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

Step-7: Under Pipeline Script, enter the following -

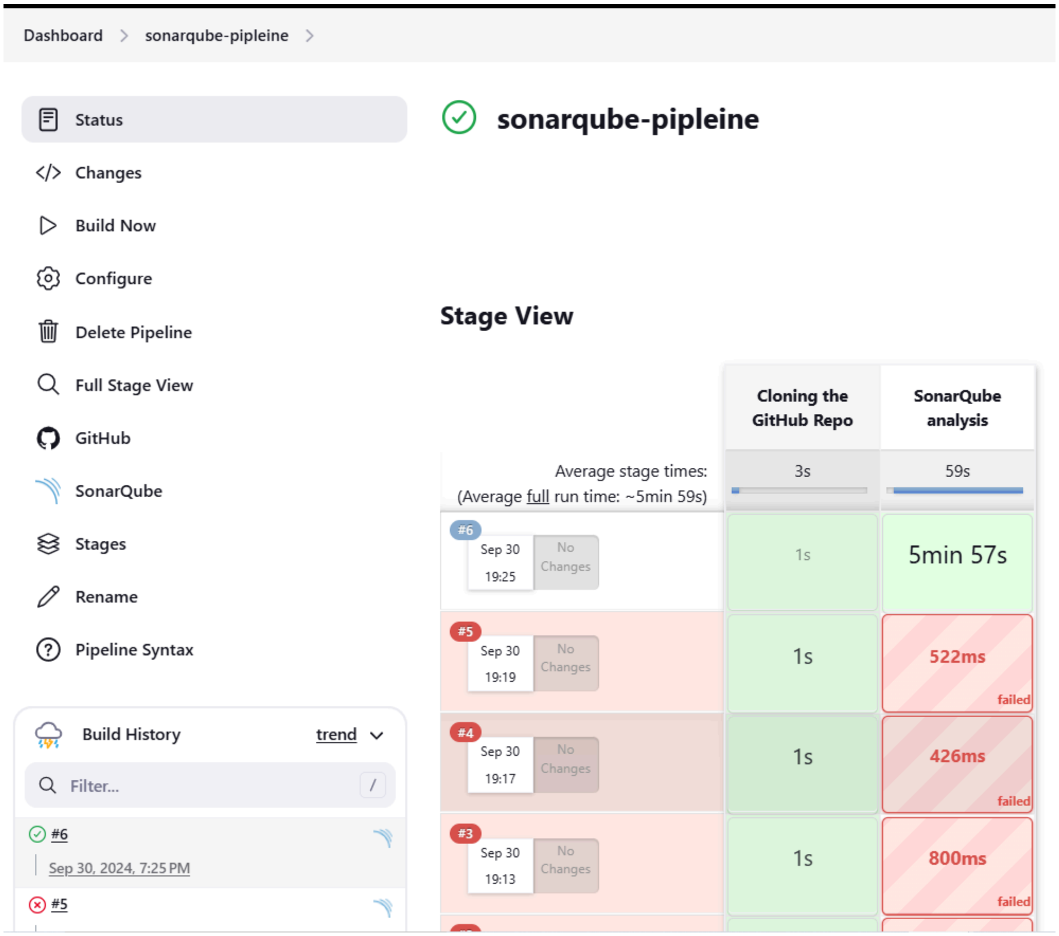
```
node {
    stage('Cloning the GitHub Repo') {
        git 'https://github.com/shazforiot/GOL.git'
    }

    stage('SonarQube analysis') {
        withSonarQubeEnv('soanrqube') {
            bat """
D:\\sonar-scanner-cli-6.2.0.4584-windows-x64\\sonar-scanner-6.2.0.4584-windows-x64\\bin\\sonar-scanner.bat ^
                -Dsonar.login=admin ^
                -Dsonar.password=siddhant ^
                -Dsonar.projectKey=sonarqube_exp8 ^
                -Dsonar.exclusions=vendor/**,resources/**,**/*.java ^
                -Dsonar.host.url=http://localhost:9000/
            """
        }
    }
}
```



```
node {
    stage('Cloning the GitHub Repo') {
        git 'https://github.com/shazforiot/GOL.git'
    }

    stage('SonarQube analysis') {
        withSonarQubeEnv('soanrqube') {
            bat """
                D:\\sonar-scanner-cli-6.2.0.4584-windows-x64\\sonar-scanner-6.2.0.4584-windows-x64\\bin\\sonar-scanner.bat ^
                -Dsonar.login=admin ^
                -Dsonar.password=siddhant ^
                -Dsonar.projectKey=sonarqube_exp8 ^
                -Dsonar.exclusions=vendor/**,resources/**,**/*.java ^
                -Dsonar.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.

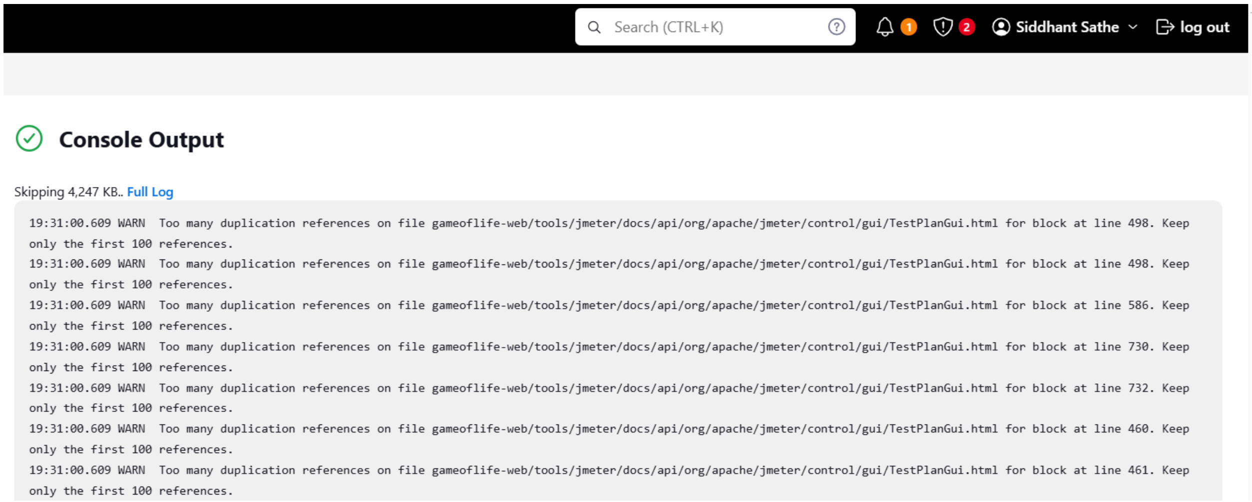
Step-8: Run The Build and check the console output:



sonarqube-pipleine

Stage View

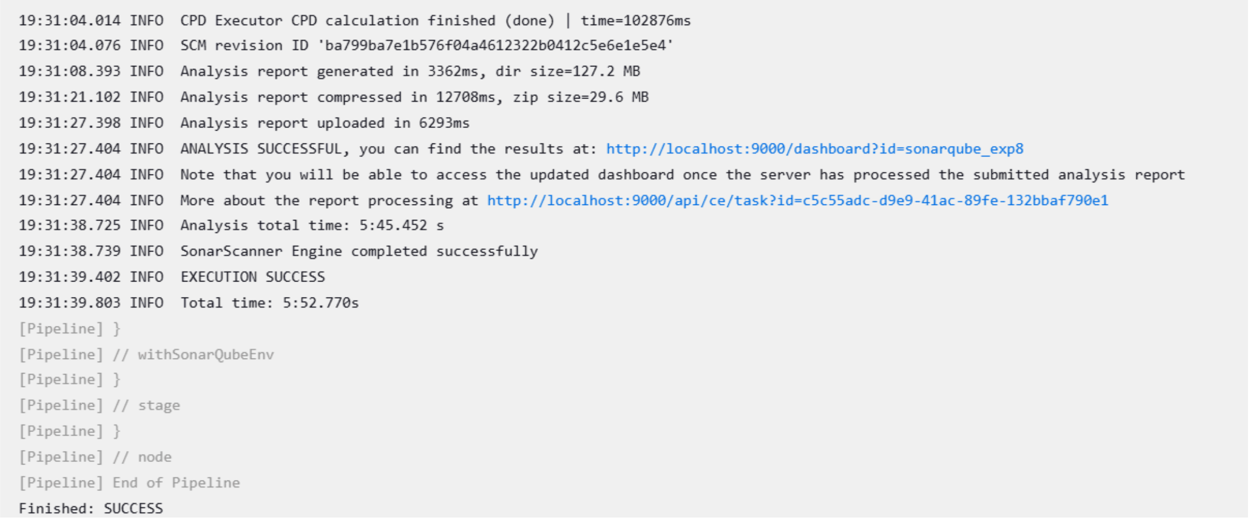
	Cloning the GitHub Repo	SonarQube analysis
Average stage times: (Average full run time: ~5min 59s)	3s	59s
#6 Sep 30 19:25 No Changes	1s	5min 57s
#5 Sep 30 19:19 No Changes	1s	522ms failed
#4 Sep 30 19:17 No Changes	1s	426ms failed
#3 Sep 30 19:13 No Changes	1s	800ms failed



Console Output

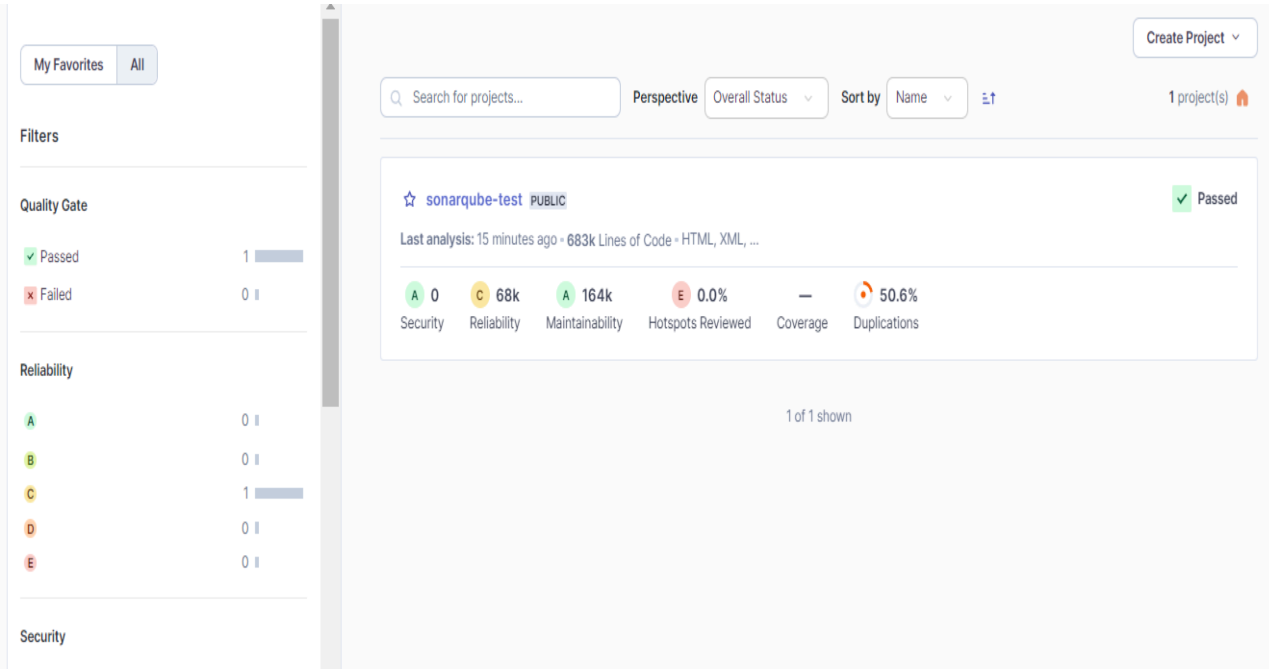
Skipping 4,247 KB.. Full Log

```
19:31:00.609 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/TestPlanGui.html for block at line 498. Keep
only the first 100 references.
19:31:00.609 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/TestPlanGui.html for block at line 498. Keep
only the first 100 references.
19:31:00.609 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/TestPlanGui.html for block at line 586. Keep
only the first 100 references.
19:31:00.609 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/TestPlanGui.html for block at line 730. Keep
only the first 100 references.
19:31:00.609 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/TestPlanGui.html for block at line 732. Keep
only the first 100 references.
19:31:00.609 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/TestPlanGui.html for block at line 460. Keep
only the first 100 references.
19:31:00.609 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/TestPlanGui.html for block at line 461. Keep
only the first 100 references.
```



```
19:31:04.014 INFO  CPD Executor CPD calculation finished (done) | time=102876ms
19:31:04.076 INFO  SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
19:31:08.393 INFO  Analysis report generated in 3362ms, dir size=127.2 MB
19:31:21.102 INFO  Analysis report compressed in 12708ms, zip size=29.6 MB
19:31:27.398 INFO  Analysis report uploaded in 6293ms
19:31:27.404 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube_exp8
19:31:27.404 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
19:31:27.404 INFO  More about the report processing at http://localhost:9000/api/ce/task?id=c5c55adc-d9e9-41ac-89fe-132bbaf790e1
19:31:38.725 INFO  Analysis total time: 5:45.452 s
19:31:38.739 INFO  SonarScanner Engine completed successfully
19:31:39.402 INFO  EXECUTION SUCCESS
19:31:39.803 INFO  Total time: 5:52.770s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

Step-9: After that, check the project in SonarQube.

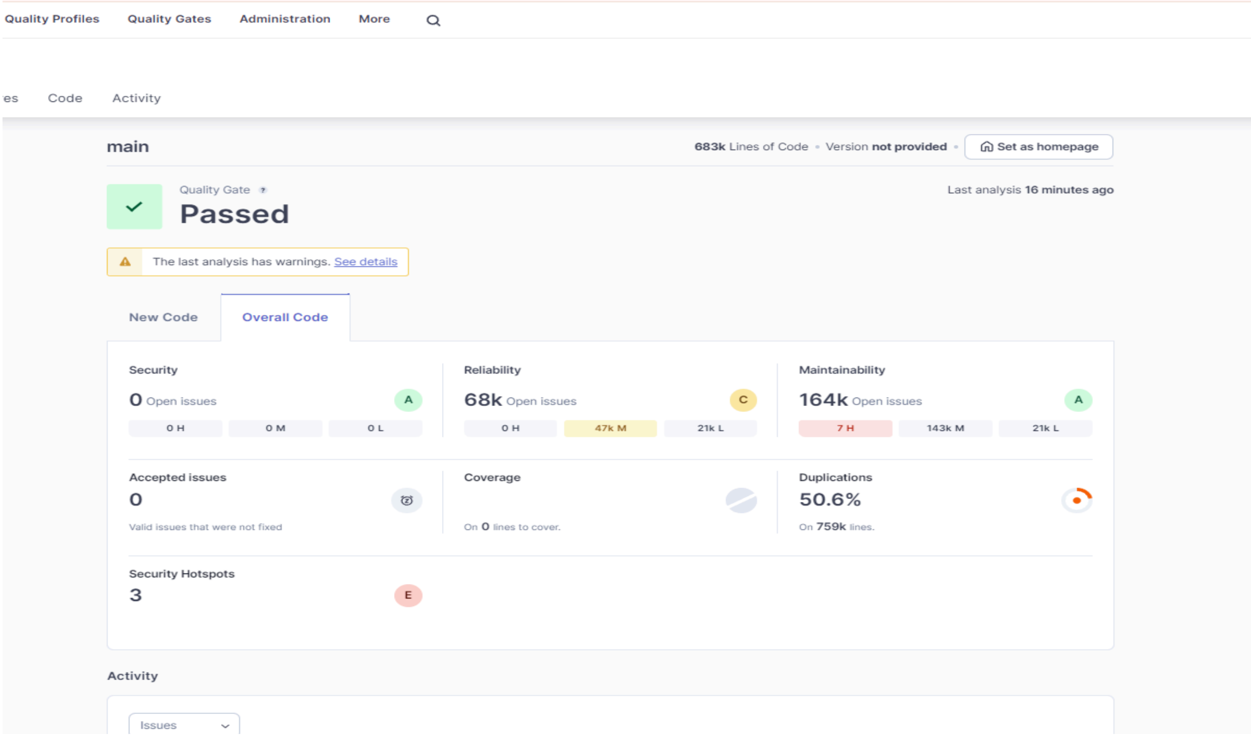


sonarqube-test PUBLIC ✓ Passed

Last analysis: 15 minutes ago • 683k Lines of Code • HTML, XML, ...

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

1 of 1 shown



main

683k Lines of Code · Version not provided

Quality Gate
Passed

Last analysis 16 minutes ago

The last analysis has warnings. See details

Security	Reliability	Maintainability
0 Open issues A	68k Open issues C	164k Open issues A
0 H · 0 M · 0 L	0 H · 47k M · 21k L	7 H · 143k M · 21k L

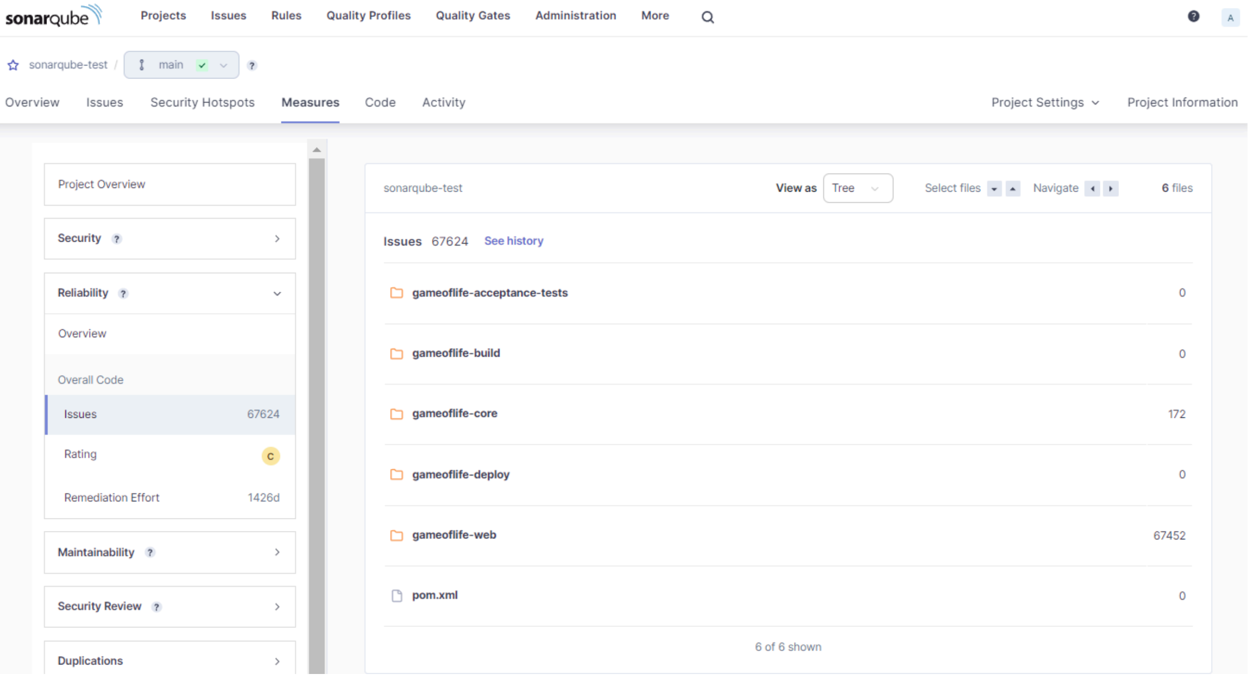
Accepted issues	Coverage	Duplications
0		50.6%
Valid issues that were not fixed	On 0 lines to cover.	On 759k lines.

Security Hotspots
3 E

Activity

Step-10: Under different tabs, check all different issues with the code.
Code Problems

Code issues:



Reliability	
Issues	67624
Rating	C
Remediation Effort	1426d

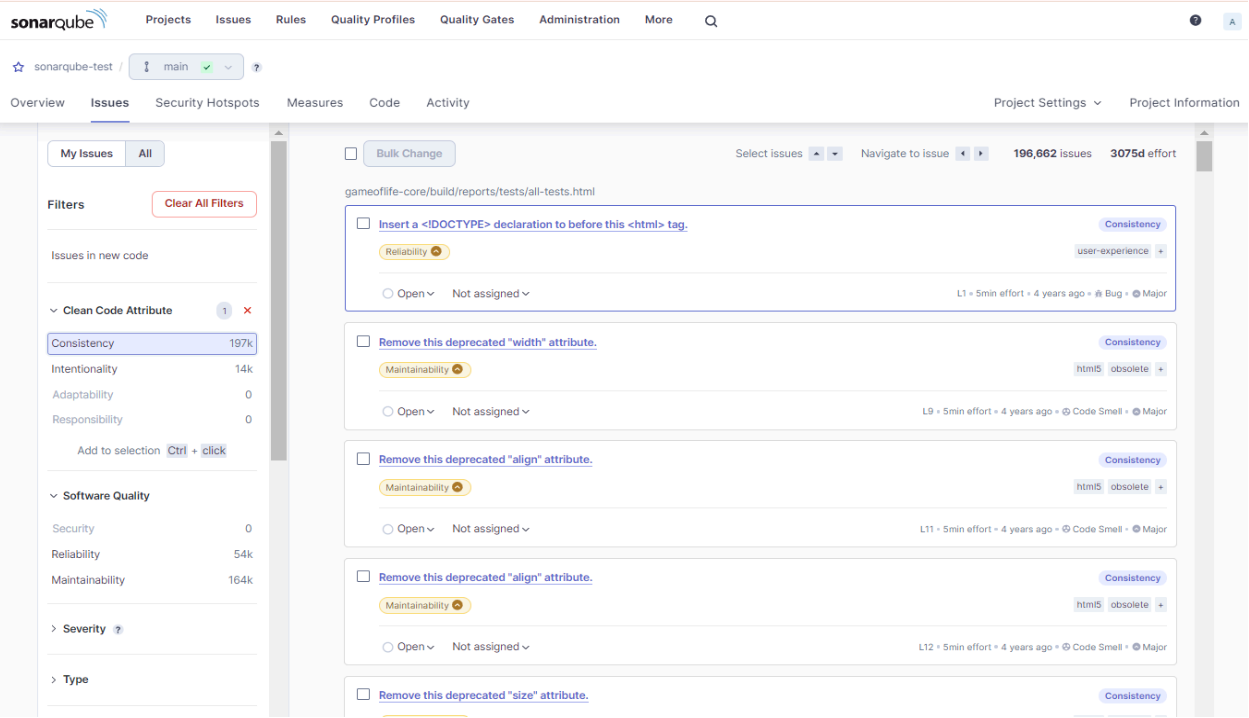
sonarqube-test · 6 files

Issues 67624 See history

gameoflife-acceptance-tests	0
gameoflife-build	0
gameoflife-core	172
gameoflife-deploy	0
gameoflife-web	67452
pom.xml	0

6 of 6 shown

Consistency:



196,662 issues 3075d effort

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 ?

Type

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

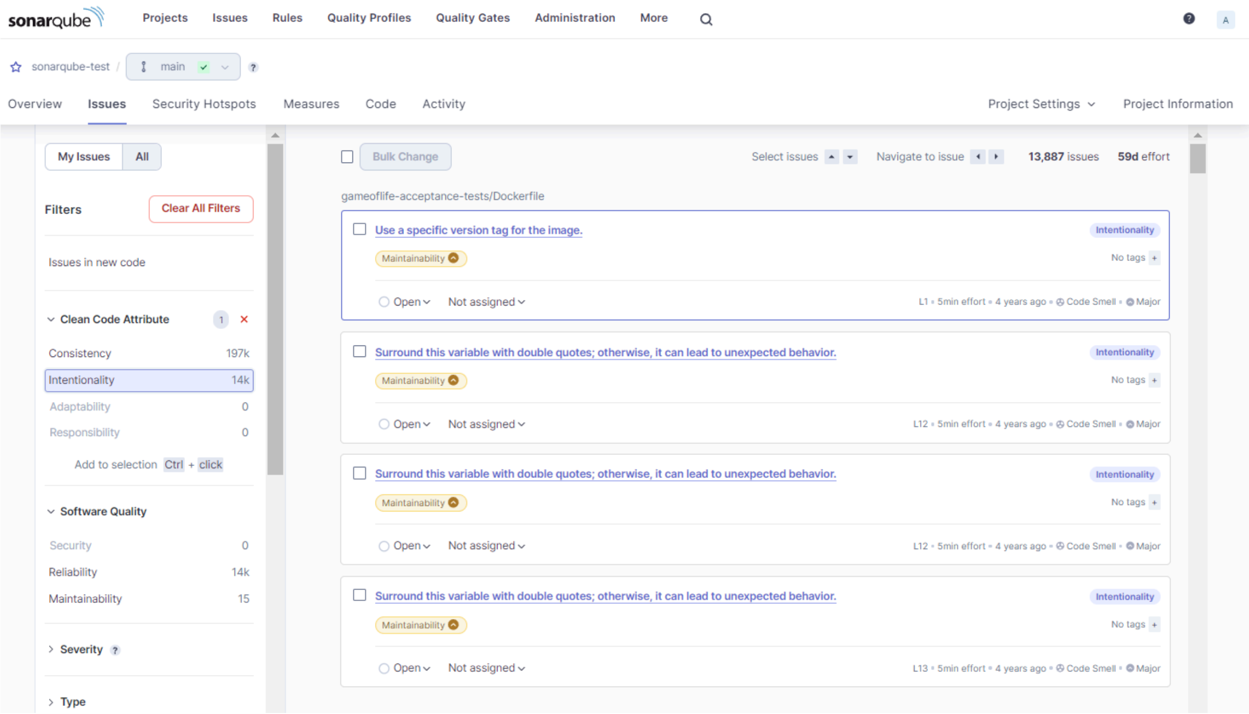
□ Remove this deprecated "width" attribute. — Consistency — Maintainability — html5 obsolete +
○ Open Not assigned — L9 • 5min effort • 4 years ago • Code Smell • Major

□ 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

Intentionally:



13,887 issues 59d effort

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	14k
Maintainability	15

Severity ?

Type

gameoflife-acceptance-tests/Dockerfile

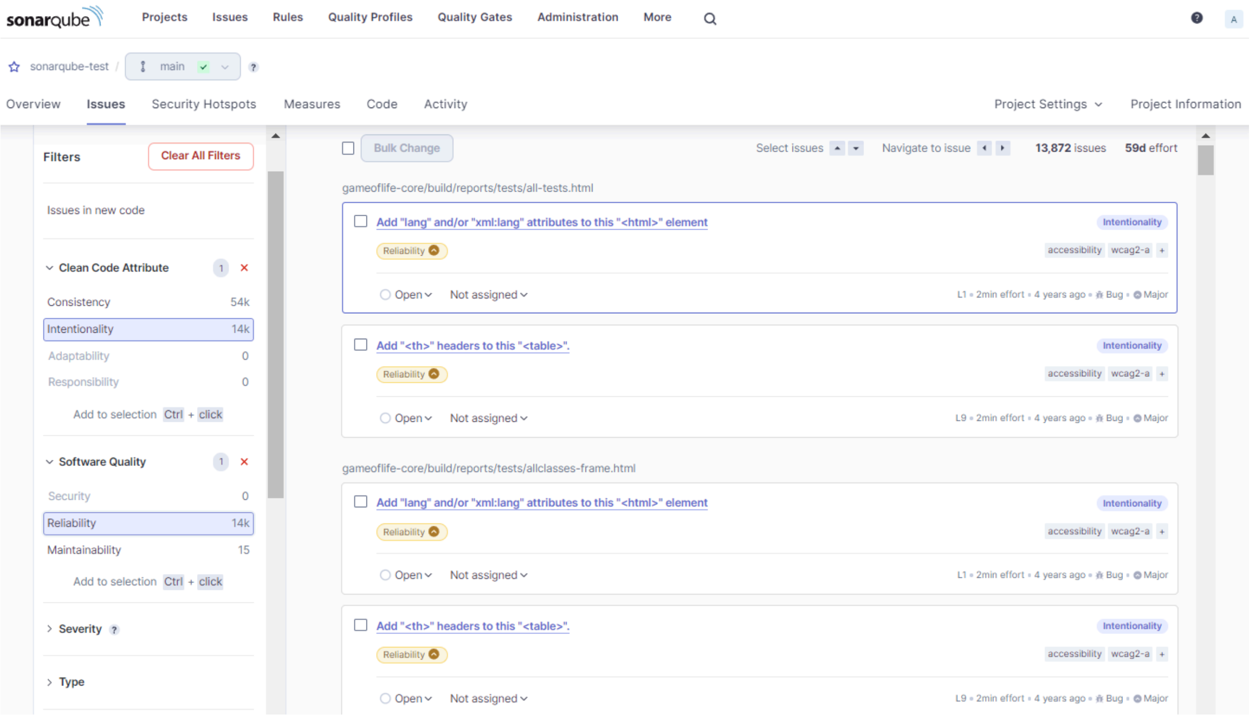
□ Use a specific version tag for the image. — Intentionality — Maintainability — No tags +
○ Open Not assigned — L1 • 5min effort • 4 years ago • Code Smell • Major

□ 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

Reliability:



13,872 issues 59d effort

Issues in new code

Clean Code Attribute 1

Consistency	54k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection Ctrl + click

Software Quality 1

Security	0
Reliability	14k
Maintainability	15

Add to selection Ctrl + click

Severity

Type

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

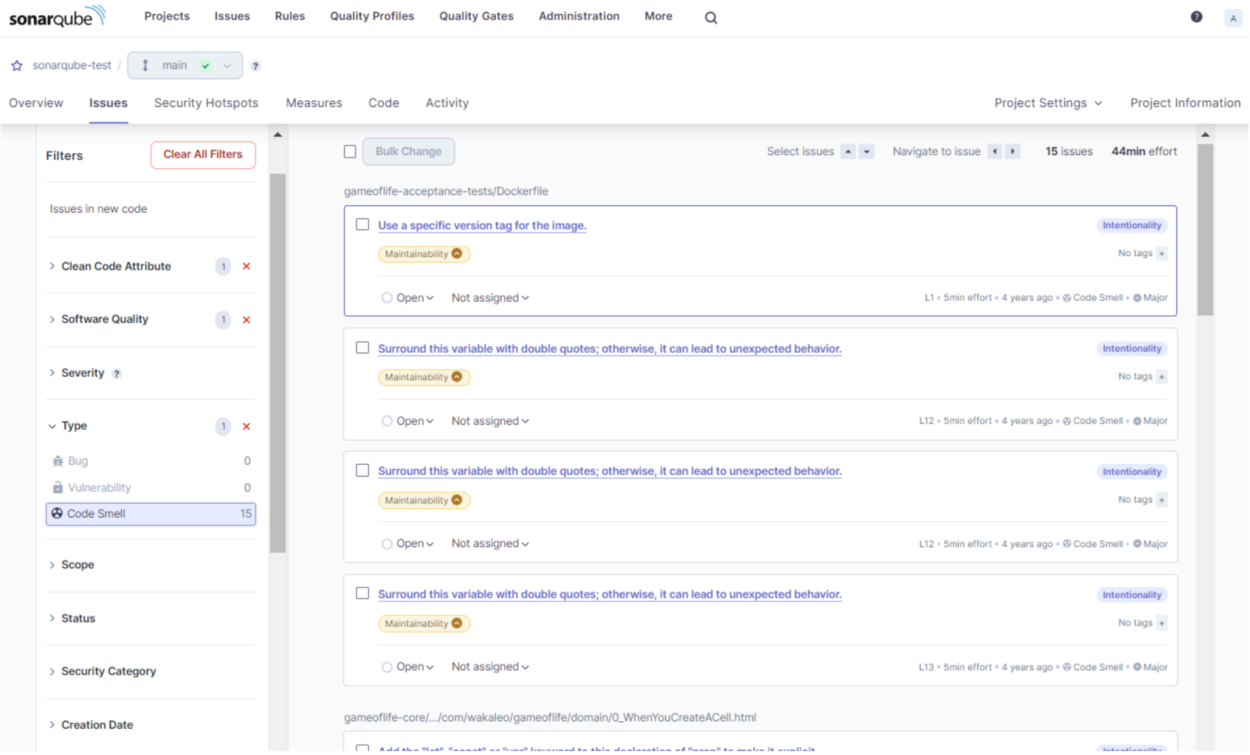
□ Add "<th>" headers to this "<table>". — Intentionality
Reliability — accessibility wcag2-a +
○ Open Not assigned — L9 • 2min effort • 4 years ago • Bug • Major

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

□ Add "lang" and/or "xml:lang" attributes to this "<html>" element
Intentionality
Reliability
accessibility wcag2-a +
○ 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

Code smells:



15 issues 44min effort

Issues in new code

Clean Code Attribute 1

Software Quality 1

Severity

Type 1

Bug	0
Vulnerability	0
Code Smell	15

Scope

Status

Security Category

Creation Date

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

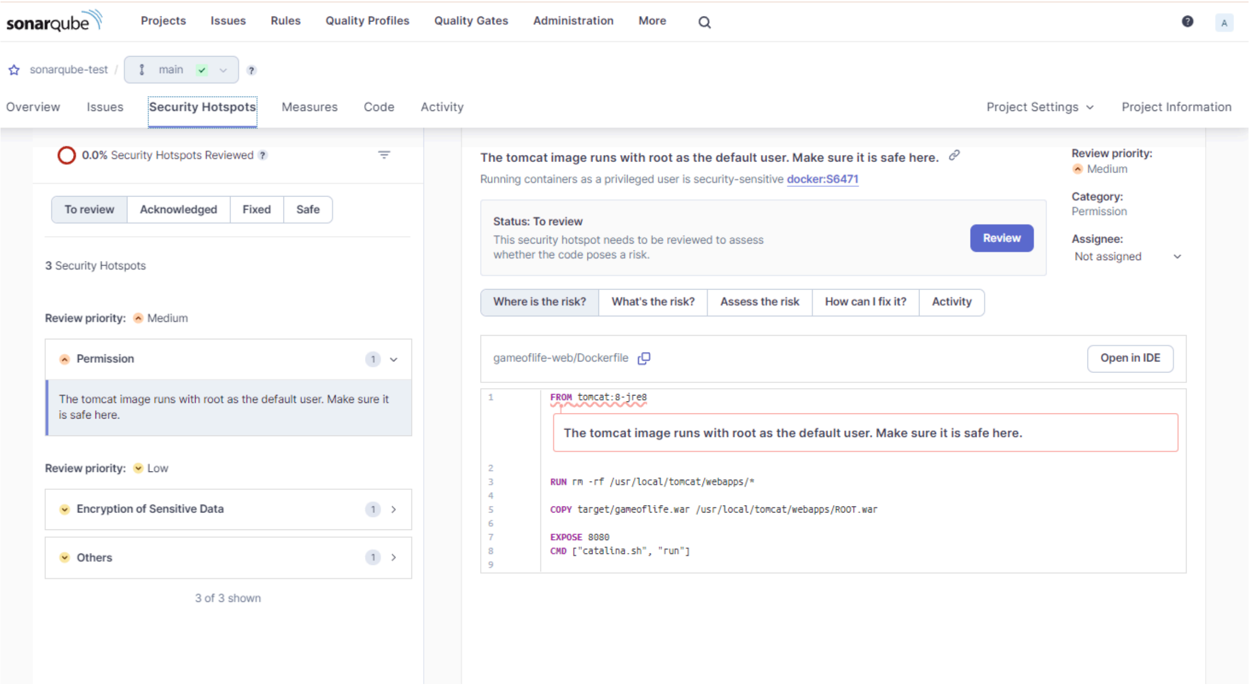
□ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. — Intentionality
Maintainability — No tags +
○ Open Not assigned — L12 • 5min effort • 4 years ago • Code Smell • Major

□ 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/.../com/wakaleo/gameoflife/domain/0_WhenYouCreateACell.html

Security hotspot:



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

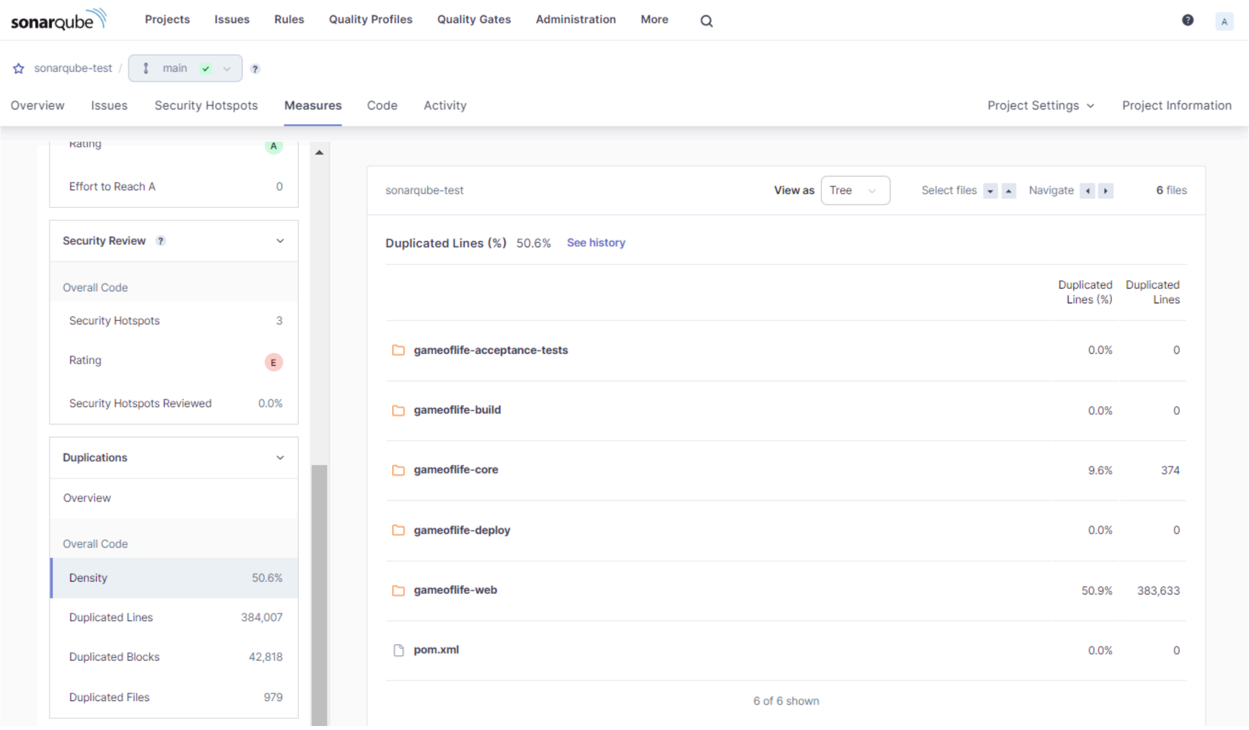
gameoflife-web/Dockerfile

```
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"]

```

Duplicates:



Rating	A
Effort to Reach A	0
Security Review	
Overall Code	
Security Hotspots	3
Rating	E
Security Hotspots Reviewed	0.0%
Duplications	
Overview	
Overall Code	
Density	50.6%
Duplicated Lines	384,007
Duplicated Blocks	42,818
Duplicated Files	979

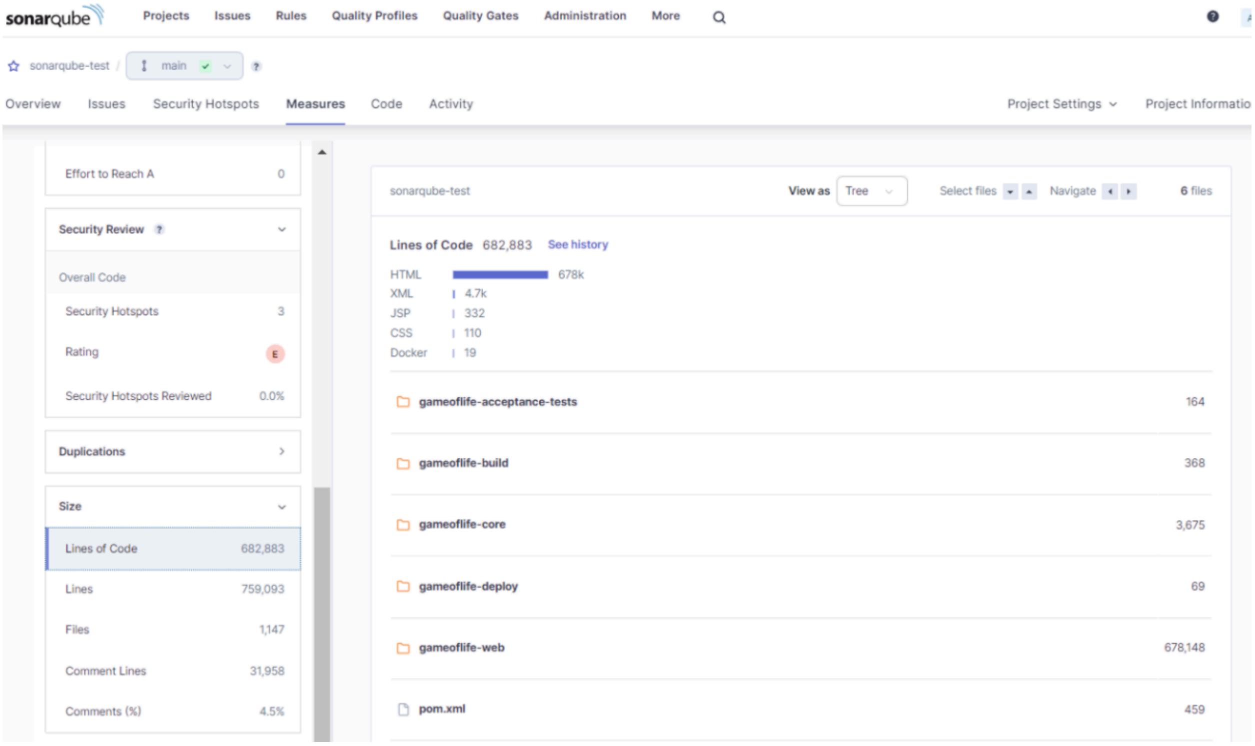
sonarqube-test — 6 files

Duplicated Lines (%) 50.6%

	Duplicated Lines (%)	Duplicated Lines
gameoflife-acceptance-tests	0.0%	0
gameoflife-build	0.0%	0
gameoflife-core	9.6%	374
gameoflife-deploy	0.0%	0
gameoflife-web	50.9%	383,633
pom.xml	0.0%	0

6 of 6 shown

Size:



Effort to Reach A	0
Security Review	
Overall Code	
Security Hotspots	3
Rating	E
Security Hotspots Reviewed	0.0%
Duplications	
Size	
Lines of Code	682,883
Lines	759,093
Files	1,147
Comment Lines	31,958
Comments (%)	4.5%

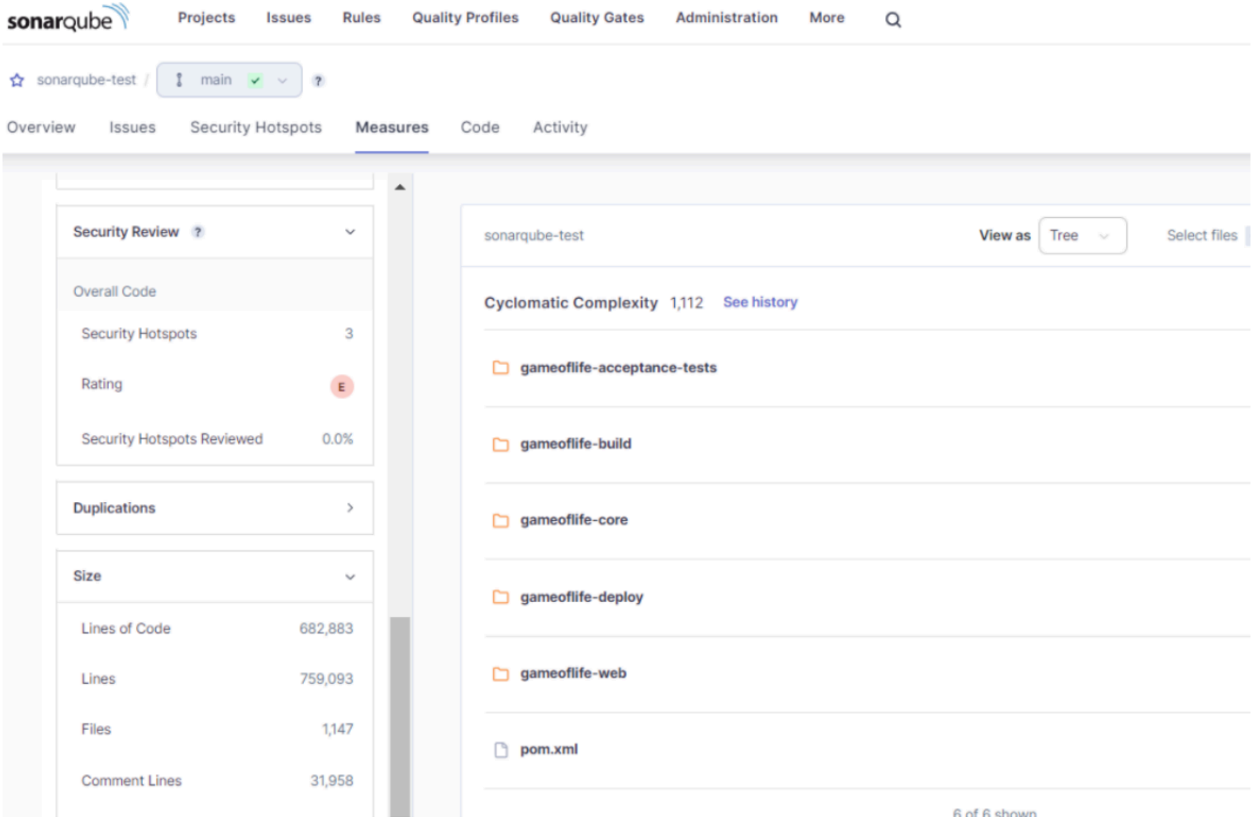
sonarqube-test

Lines of Code 682,883 See history

HTML	678k
XML	4.7k
JSP	332
CSS	110
Docker	19

gameoflife-acceptance-tests	164
gameoflife-build	368
gameoflife-core	3,675
gameoflife-deploy	69
gameoflife-web	678,148
pom.xml	459

Complexity:



Security Review	
Overall Code	
Security Hotspots	3
Rating	E
Security Hotspots Reviewed	0.0%
Duplications	
Size	
Lines of Code	682,883
Lines	759,093
Files	1,147
Comment Lines	31,958

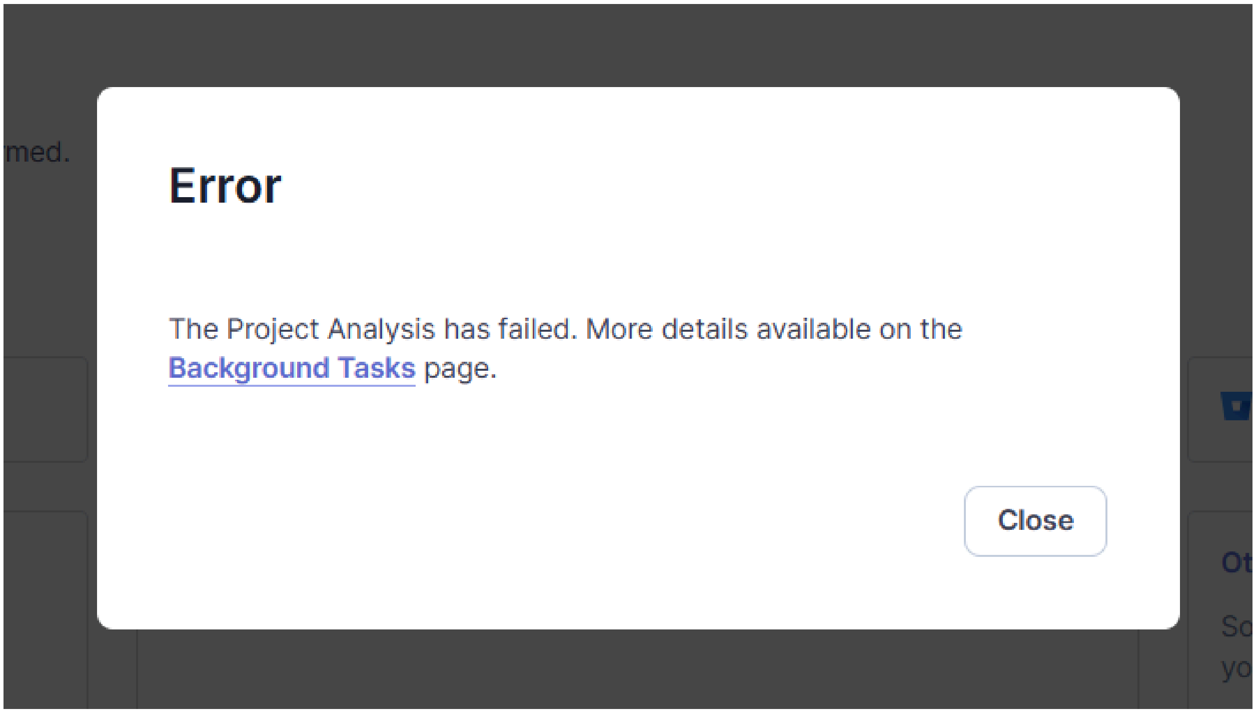
sonarqube-test

Cyclomatic Complexity 1,112 See history

- gameoflife-acceptance-tests
- gameoflife-build
- gameoflife-core
- gameoflife-deploy
- gameoflife-web
- pom.xml

6 of 6 shown

Errors:
Build was not successful because my sonarqube env name was wrong in scripts



Error

The Project Analysis has failed. More details available on the Background Tasks page.