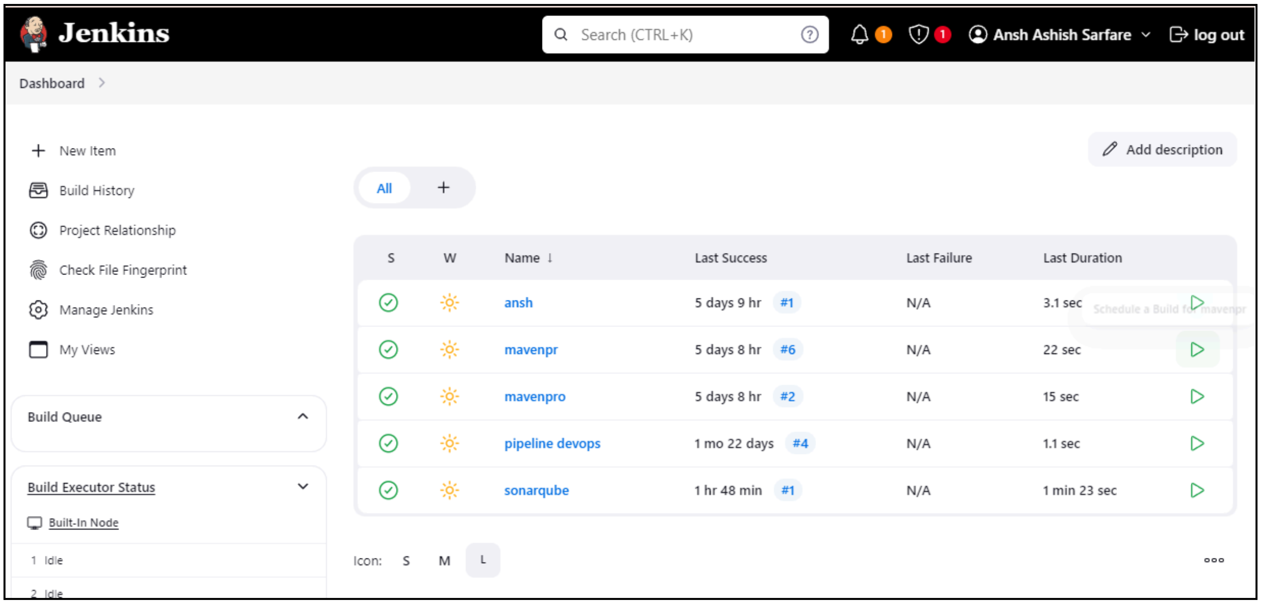
ADVANCE DEVOPS EXP-8

ANSH SARFARE **D15A/50**

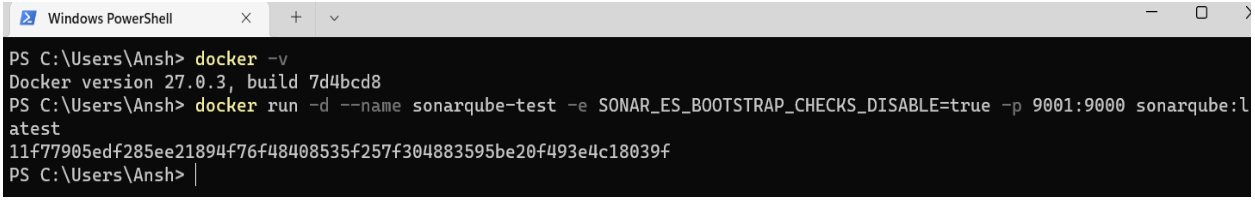
Aim: To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.

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



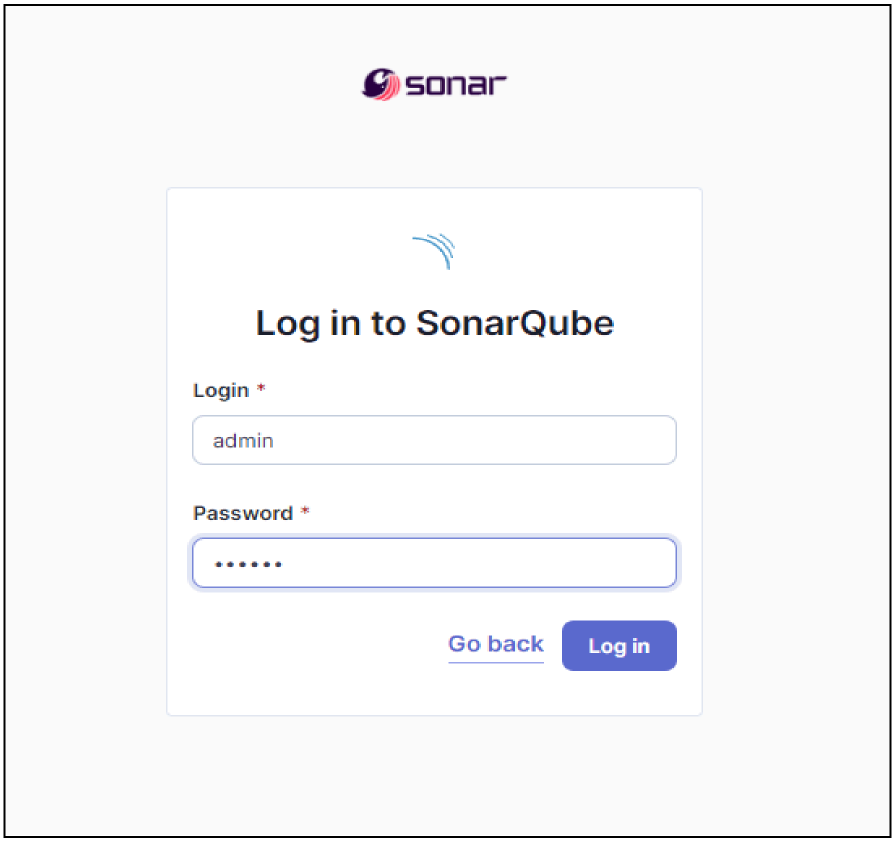
S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☀	ansh	5 days 9 hr #1	N/A	3.1 sec
✓	☀	mavenpr	5 days 8 hr #6	N/A	22 sec
✓	☀	mavenpro	5 days 8 hr #2	N/A	15 sec
✓	☀	pipeline devops	1 mo 22 days #4	N/A	1.1 sec
✓	☀	sonarqube	1 hr 48 min #1	N/A	1 min 23 sec

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 9001:9000 sonarqube:latest



```
PS C:\Users\Ansh> docker -v
Docker version 27.0.3, build 7d4bcd8
PS C:\Users\Ansh> docker run -d --name sonarqube-test -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9001:9000 sonarqube:l
atest
11f77905edf285ee21894f76f48408535f257f304883595be20f493e4c18039f
PS C:\Users\Ansh> |
```

Step-3: Once the container is up and running, you can check the status of SonarQube at localhost port 9001. The login id is “admin” and the password is also “ansh16”.



Log in to SonarQube

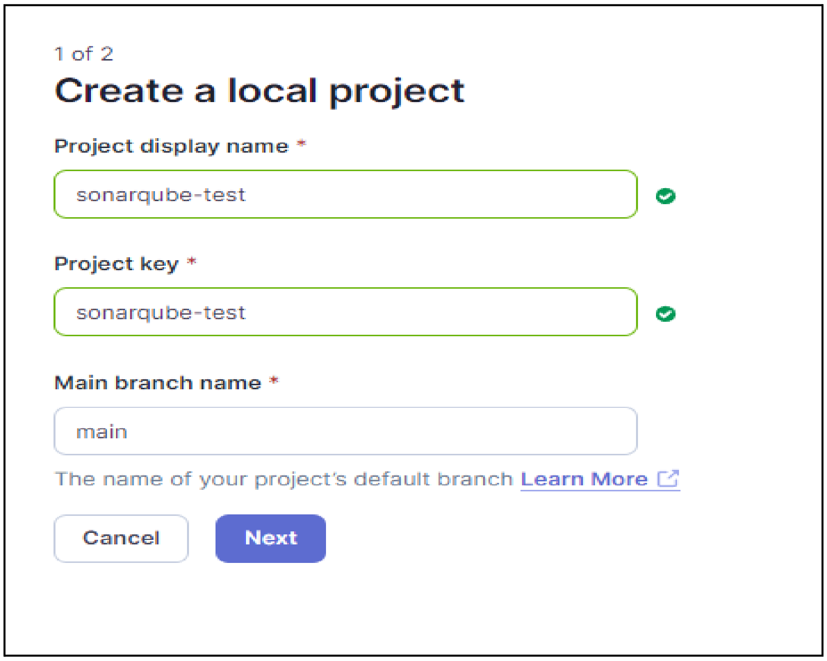
Login *

admin

Password *

••••••

Step-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 *

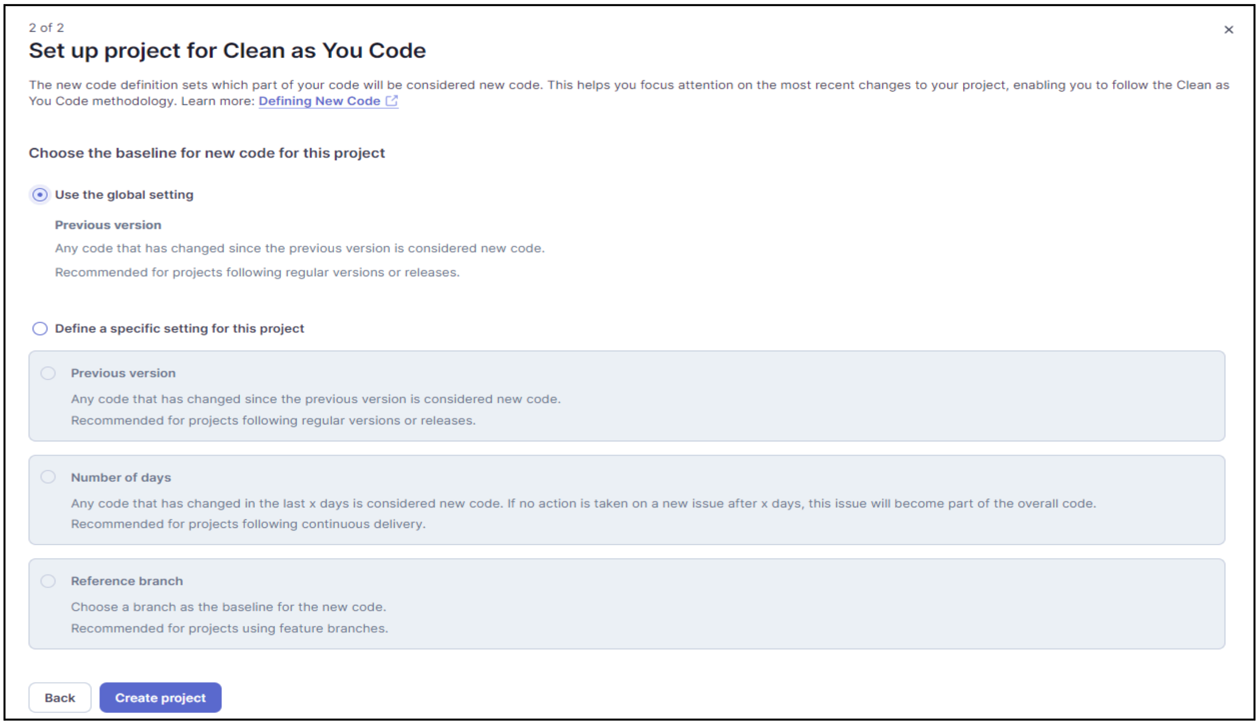
sonarqube-test ✓

Main branch name *

main

The name of your project's default branch Learn More

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



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.

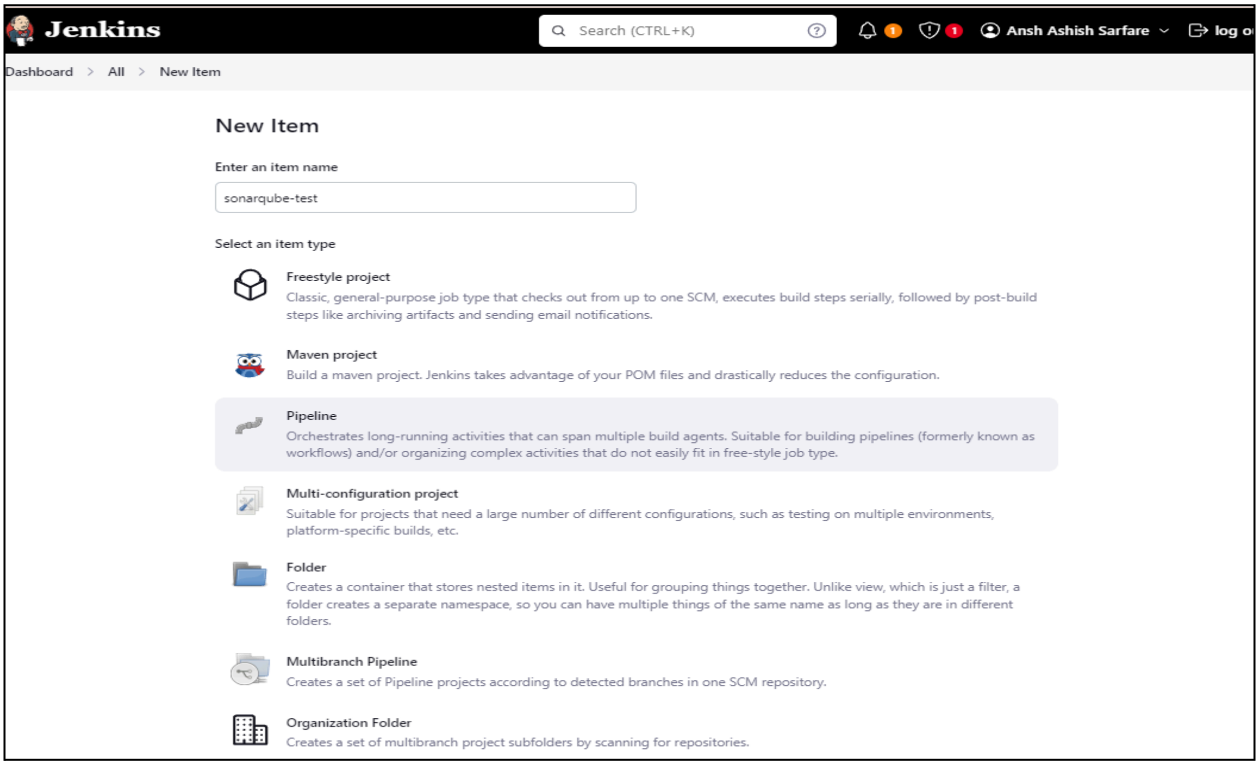
Recommended for projects following continuous delivery.

○ Reference branch

Choose a branch as the baseline for the new code.

Recommended for projects using feature branches.

Step-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 folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

Multibranch Pipeline

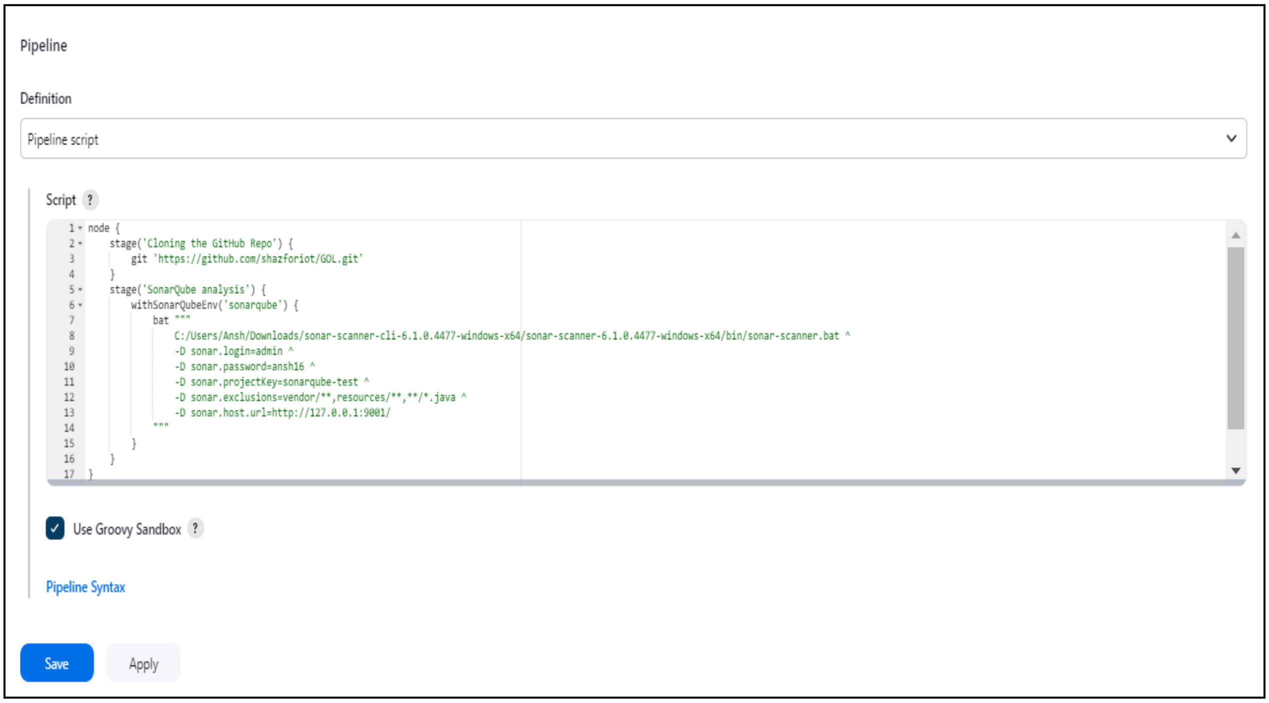
Creates a set of Pipeline projects according to detected branches in one SCM repository.

Organization Folder

Creates a set of multibranch project subfolders by scanning for repositories.

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

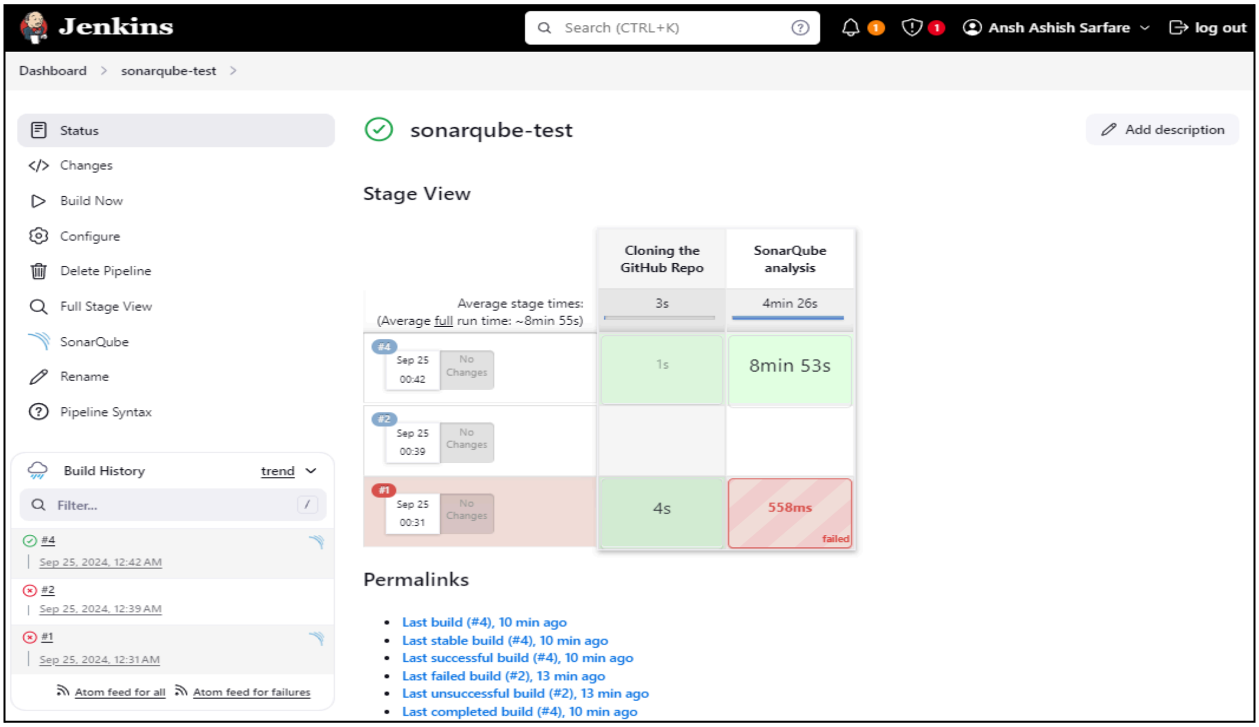
```
node {
    stage('Cloning the GitHub Repo')
   {
    git 'https://github.com/shazforiot/GOL.git'
}
stage('SonarQube analysis') {
withSonarQubeEnv('sonarqube') {
bat
"C:\\Users\\Ansh\\Downloads\\sonar-scanner-cli-6.1.0.4477-windows-x64\\sonar-scanner-6.1.0.4477-windows-x64\\bin\\sonar-scanner.bat \
-D sonar.login=admin \
-D sonar.password=ansh16 \
-D sonar.projectKey=sonarqube-test \
-D sonar.exclusions=vendor/**,resources/**,**/*.java \
-D sonar.host.url=http://localhost:9001/"
}
}
}
```



```
node {
    stage('Cloning the GitHub Repo') {
        git 'https://github.com/shazforiot/GOL.git'
    }
    stage('SonarQube analysis') {
        withSonarQubeEnv('sonarqube') {
            bat """
                C:/Users/Ansh/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=ansh16 ^
                -D sonar.projectKey=sonarqube-test ^
                -D sonar.exclusions=vendor/**,resources/**,**/*.java ^
                -D sonar.host.url=http://127.0.0.1:9001/
            """
        }
    }
}
```

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-test

Stage View

	Cloning the GitHub Repo	SonarQube analysis
Average stage times: (Average full run time: ~8min 55s)	3s	4min 26s
#4 Sep 25 00:42 No Changes	1s	8min 53s
#2 Sep 25 00:39 No Changes		
#1 Sep 25 00:31 No Changes	4s	558ms failed

Build History trend

Filter...

#4 Sep 25, 2024, 12:42 AM

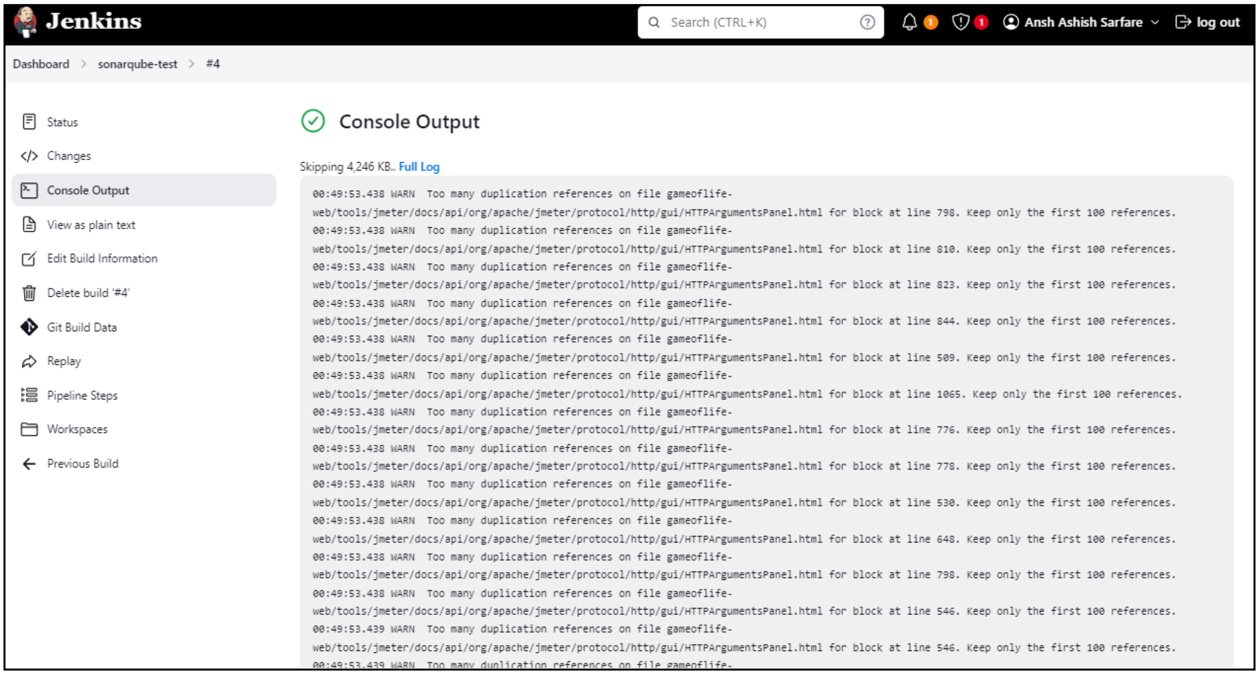
#2 Sep 25, 2024, 12:39 AM

#1 Sep 25, 2024, 12:31 AM

Atom feed for all Atom feed for failures

Permalinks

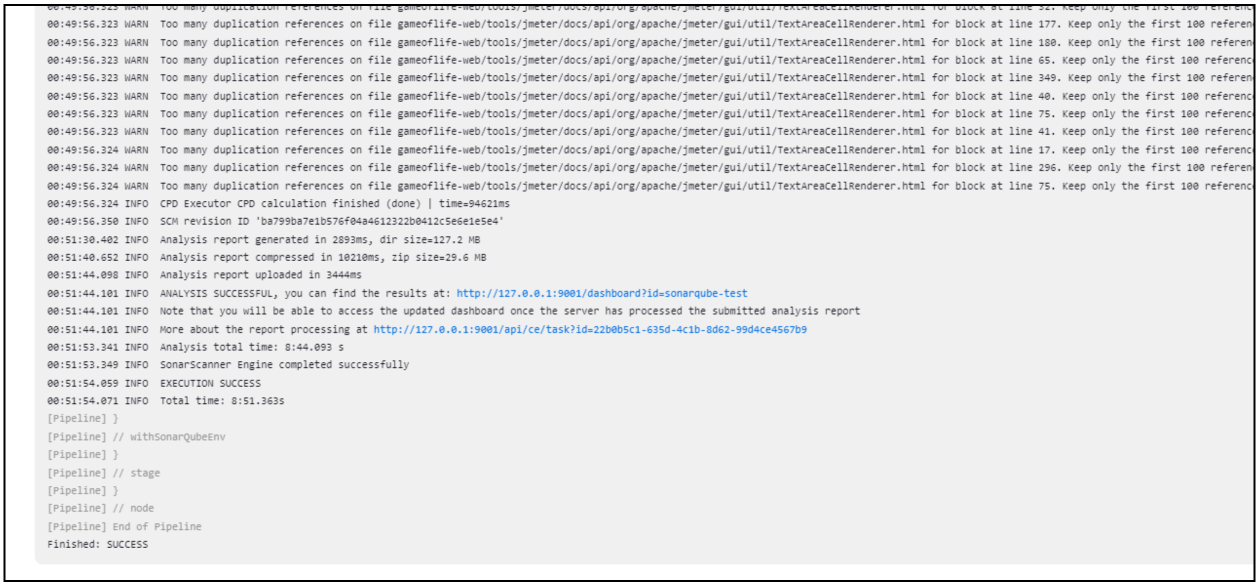
- Last build (#4), 10 min ago
- Last stable build (#4), 10 min ago
- Last successful build (#4), 10 min ago
- Last failed build (#2), 13 min ago
- Last unsuccessful build (#2), 13 min ago
- Last completed build (#4), 10 min ago



Console Output

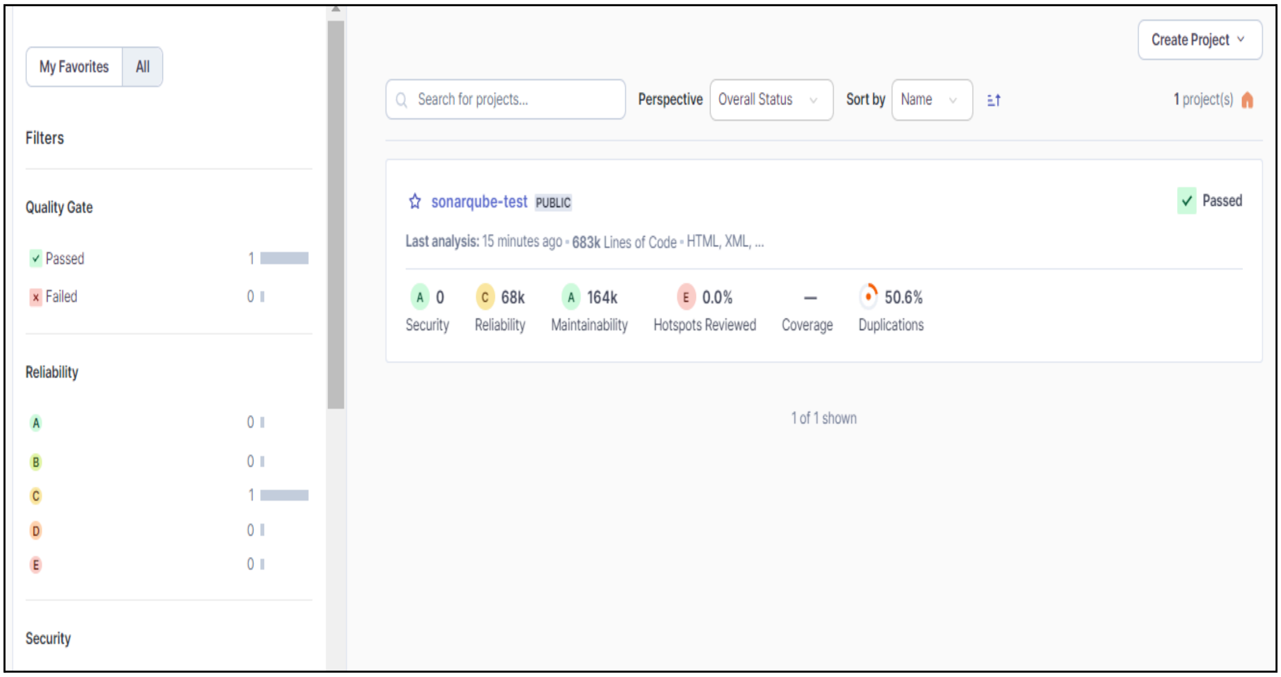
Skipping 4,246 KB.. Full Log

```
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 798. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 810. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 823. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 844. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 509. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 1065. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 776. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 778. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 530. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 648. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 798. Keep only the first 100 references.
00:49:53.438 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 546. Keep only the first 100 references.
00:49:53.439 WARN  Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/gui/HTTPArgumentsPanel.html for block at line 546. Keep only the first 100 references.
00:49:53.439 WARN  Too many duplication references on file gameoflife-
```



```
00:49:56.323 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 52. Keep only the first 100 referenc
00:49:56.323 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 177. Keep only the first 100 referen
00:49:56.323 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 180. Keep only the first 100 referen
00:49:56.323 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 65. Keep only the first 100 referenc
00:49:56.323 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 349. Keep only the first 100 referen
00:49:56.323 WARN  Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/util/TextAreaCellRenderer.html for block at line 40. Keep only the first 100 referenc
00:49:56.323 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 referenc
00:49:56.323 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 referenc
00:49:56.324 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 referenc
00:49:56.324 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 referen
00:49:56.324 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 referenc
00:49:56.324 INFO  CPD Executor CPD calculation finished (done) | time=94621ms
00:49:56.350 INFO  SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
00:51:30.402 INFO  Analysis report generated in 2893ms, dir size=127.2 MB
00:51:40.652 INFO  Analysis report compressed in 10210ms, zip size=29.6 MB
00:51:44.098 INFO  Analysis report uploaded in 3444ms
00:51:44.101 INFO  ANALYSIS SUCCESSFUL, you can find the results at: http://127.0.0.1:9001/dashboard?id=sonarqube-test
00:51:44.101 INFO  Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
00:51:44.101 INFO  More about the report processing at http://127.0.0.1:9001/api/ce/task?id=22b0b5c1-635d-4c1b-8d62-99d4ce4567b9
00:51:53.341 INFO  Analysis total time: 8:44.093 s
00:51:53.349 INFO  SonarScanner Engine completed successfully
00:51:54.059 INFO  EXECUTION SUCCESS
00:51:54.071 INFO  Total time: 8:51.363s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

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



Perspective: Overall Status

Sort by: Name

1 project(s)

Filters

Quality Gate

✓ Passed	1
✗ Failed	0

Reliability

A	0
B	0
C	1
D	0
E	0

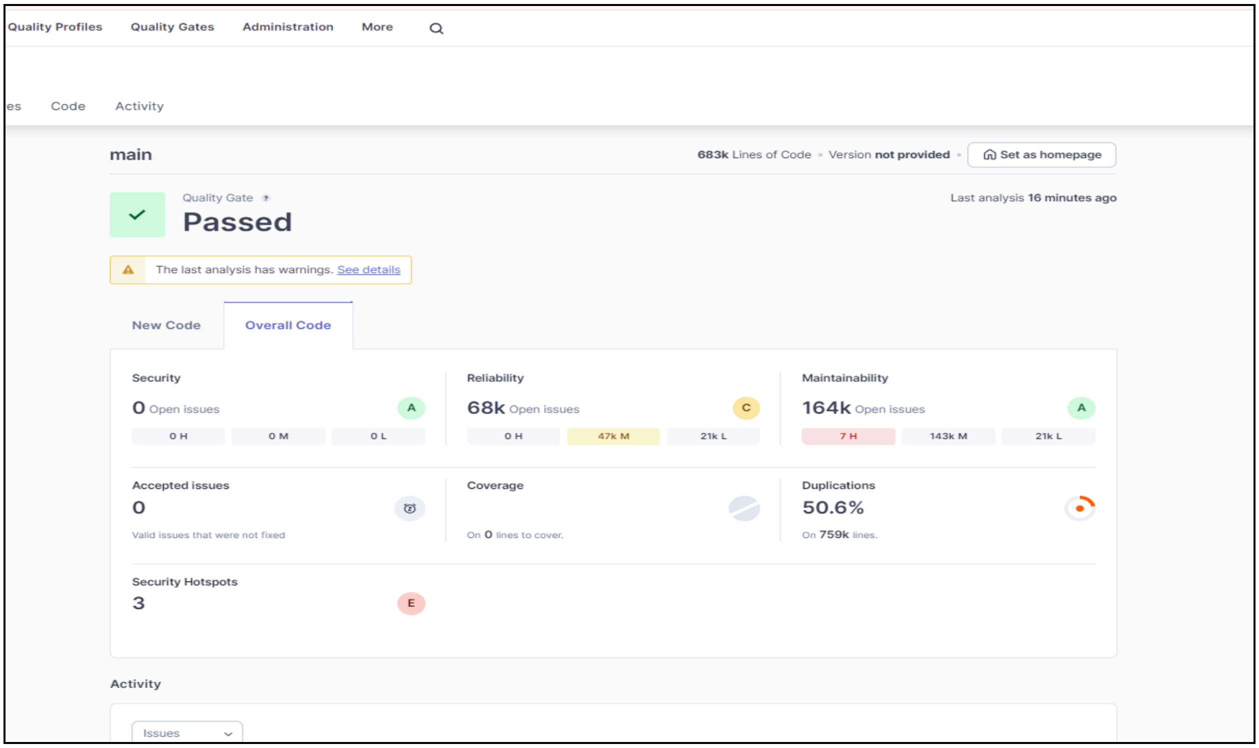
Security

☆ sonarqube-test PUBLIC ✓ Passed

Last analysis: 15 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

1 of 1 shown



main

683k Lines of Code · Version not provided · Set as homepage

Quality Gate

Passed

Last analysis 16 minutes ago

The last analysis has warnings. See details

New Code | Overall Code

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

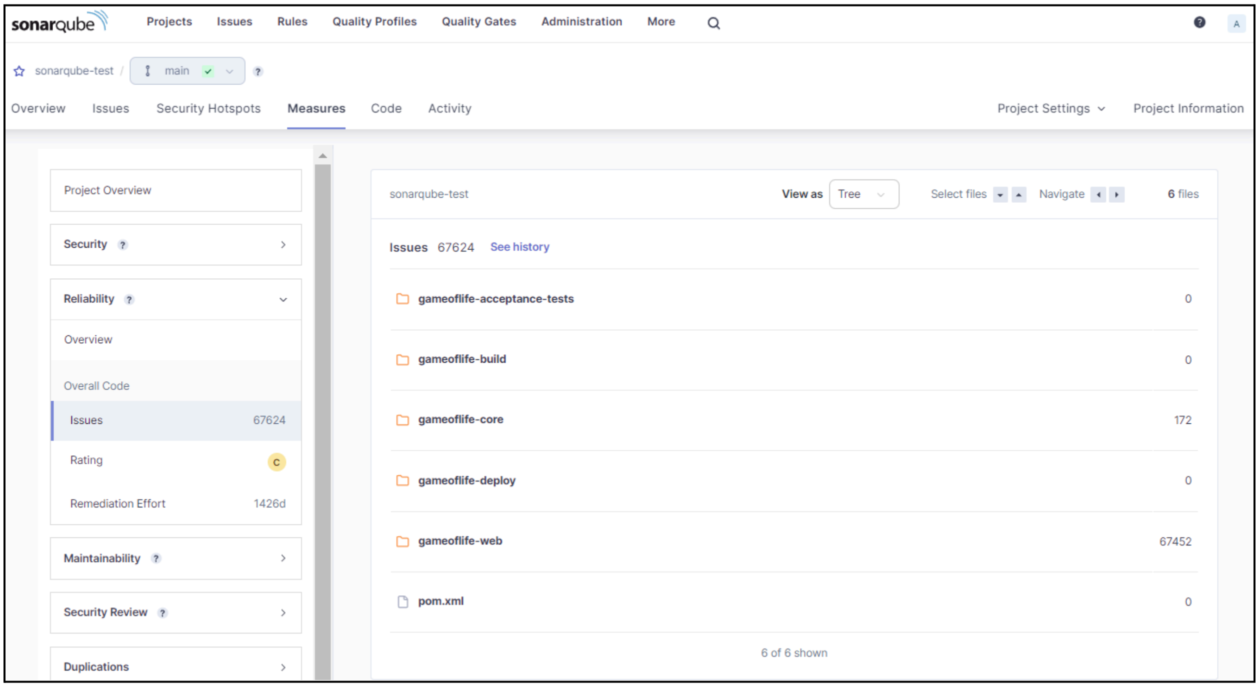
Activity

Issues

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

Code Problems

Code issues:



Project Overview	
Security	
Reliability	
Overview	
Overall Code	
Issues	67624
Rating	C
Remediation Effort	1426d
Maintainability	
Security Review	
Duplications	

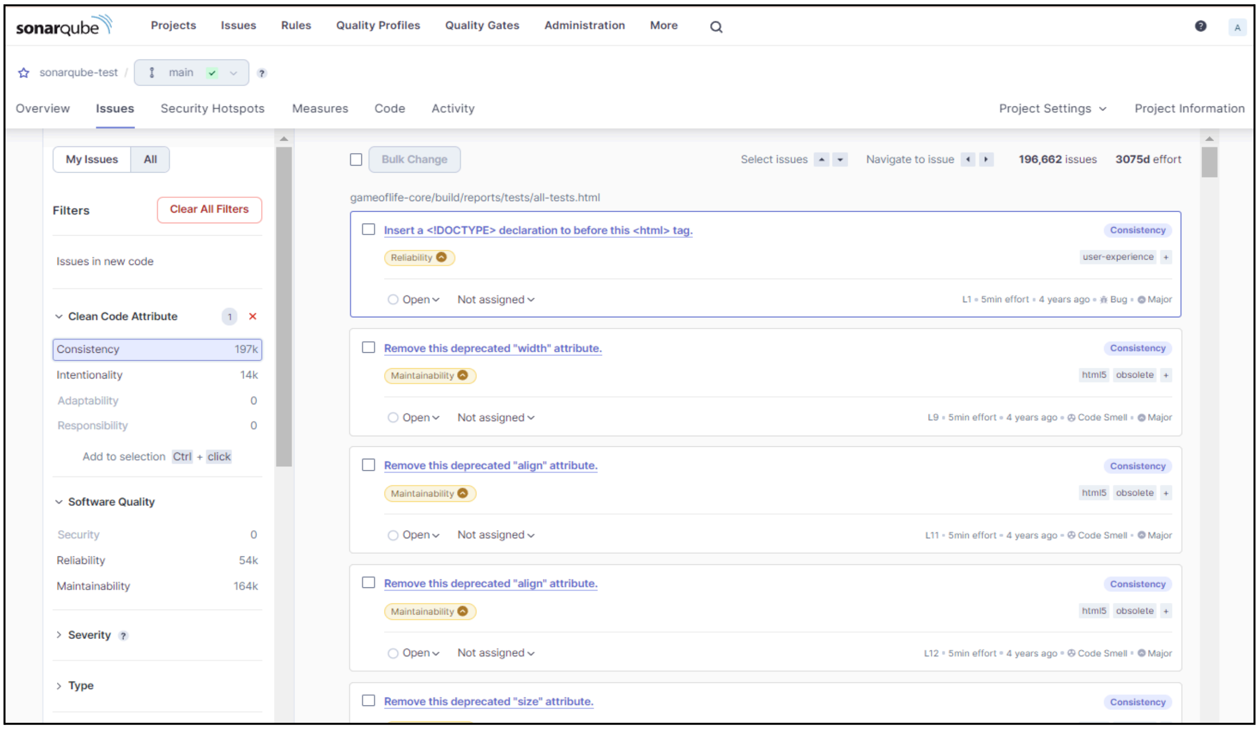
sonarqube-test — View as Tree — Select files — Navigate — 6 files

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:



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

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

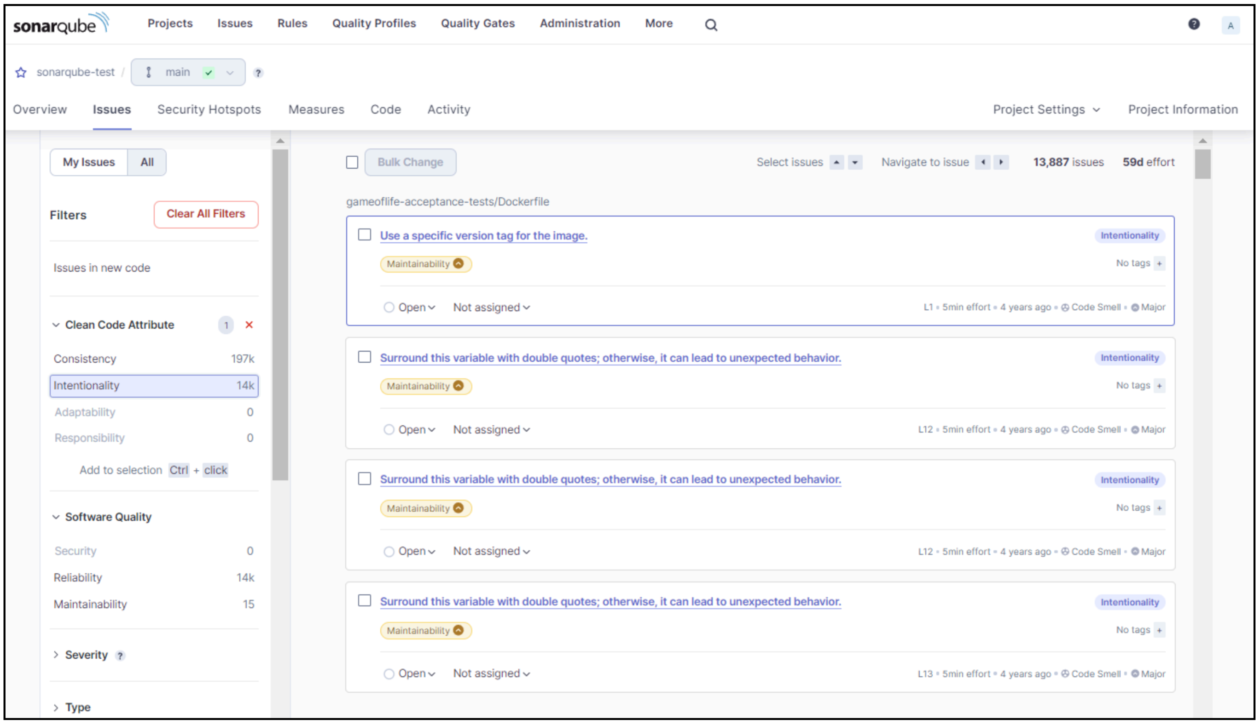
□ Remove this deprecated "width" attribute. — Consistency
Maintainability — html5 obsolete +
○ Open ⌄ Not assigned ⌄ — L9 • 5min effort • 4 years ago • Code Smell • Major

□ Remove this deprecated "align" attribute. — Consistency
Maintainability — html5 obsolete +
○ Open ⌄ Not assigned ⌄ — L11 • 5min effort • 4 years ago • Code Smell • Major

□ 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:



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

13,887 issues **59d** effort

gameoflife-acceptance-tests/Dockerfile

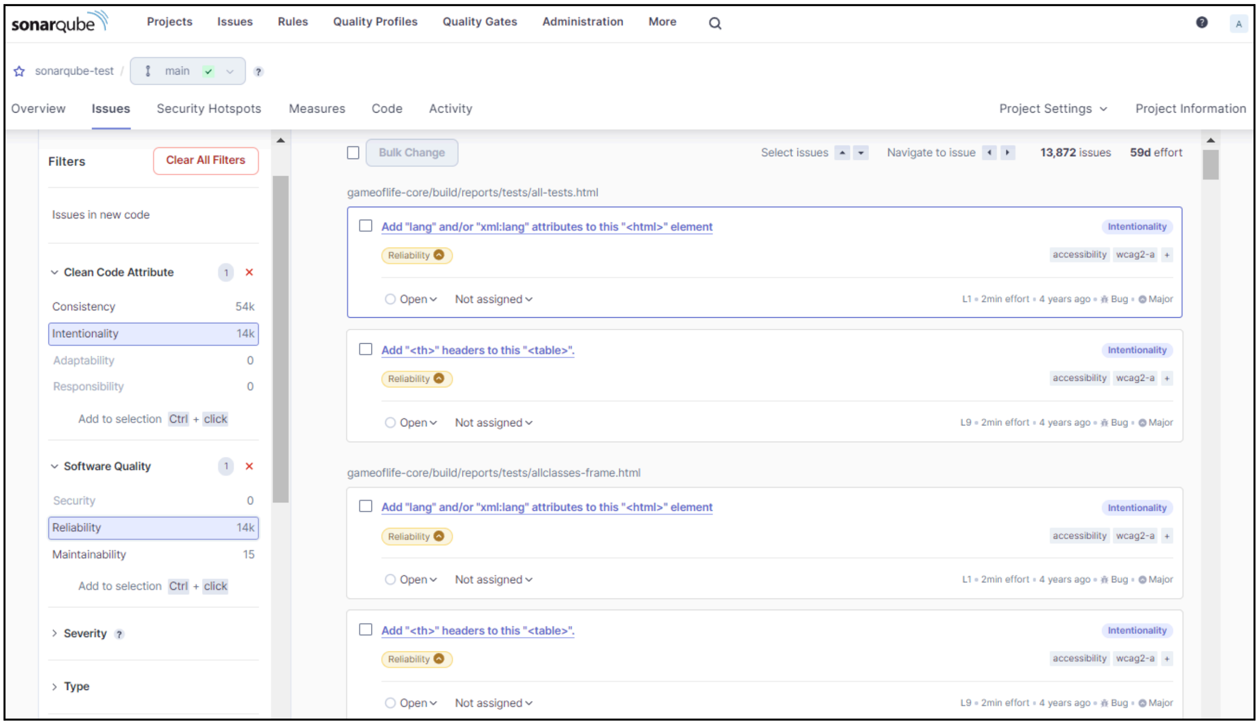
□ Use a specific version tag for the image. — Intentionality
Maintainability — No tags +
○ Open ⌄ Not assigned ⌄ — L1 • 5min effort • 4 years ago • Code Smell • Major

□ 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

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

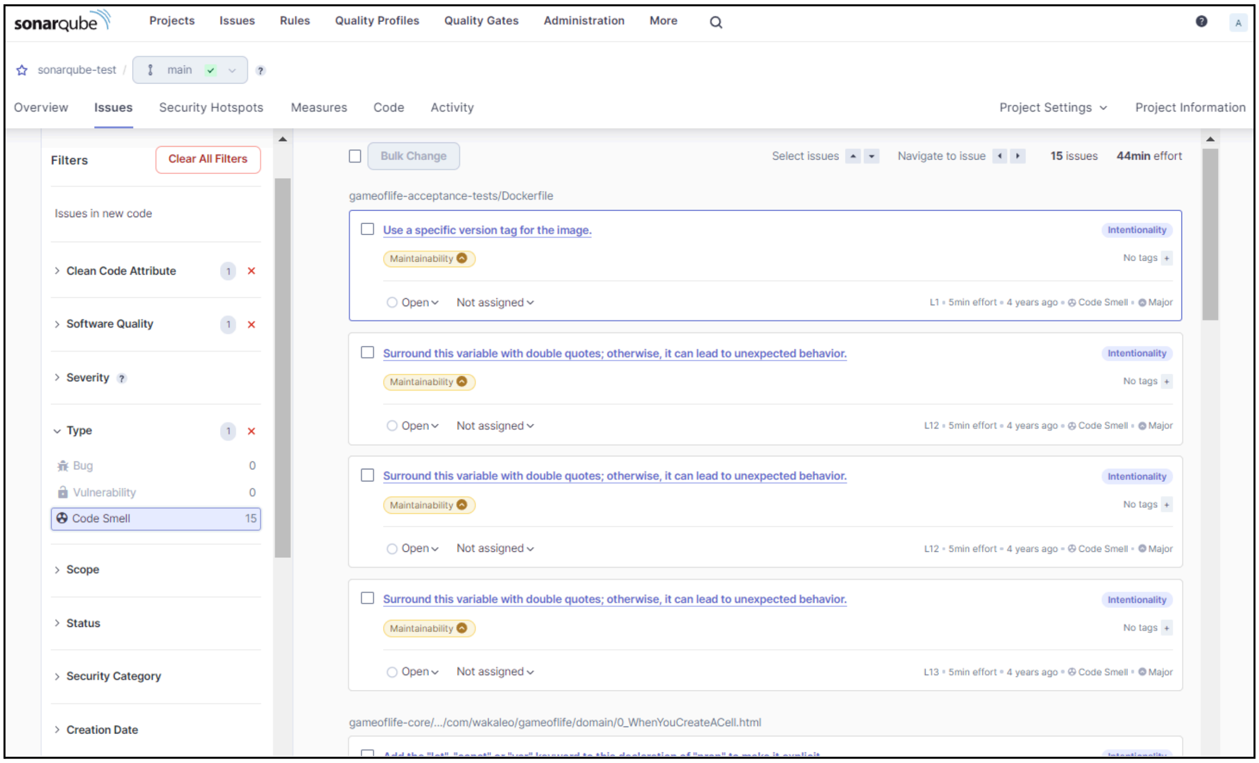
□ Add "<th>" headers to this "<table>". Intentionality
Reliability accessibility wcag2-a +
○ Open Not assigned L9 • 2min effort • 4 years ago • Bug • Major

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

Type 1

Bug	0
Vulnerability	0
Code Smell	15

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

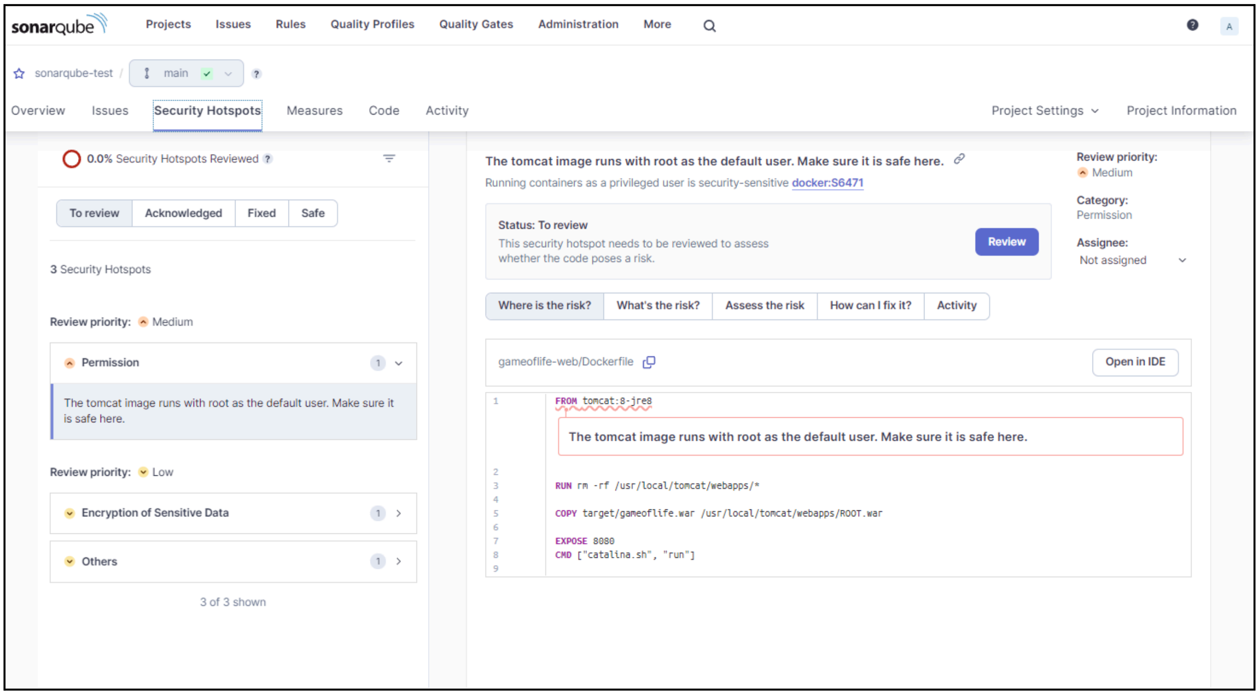
□ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality
Maintainability No tags +
○ Open Not assigned L12 • 5min effort • 4 years ago • Code Smell • Major

□ 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

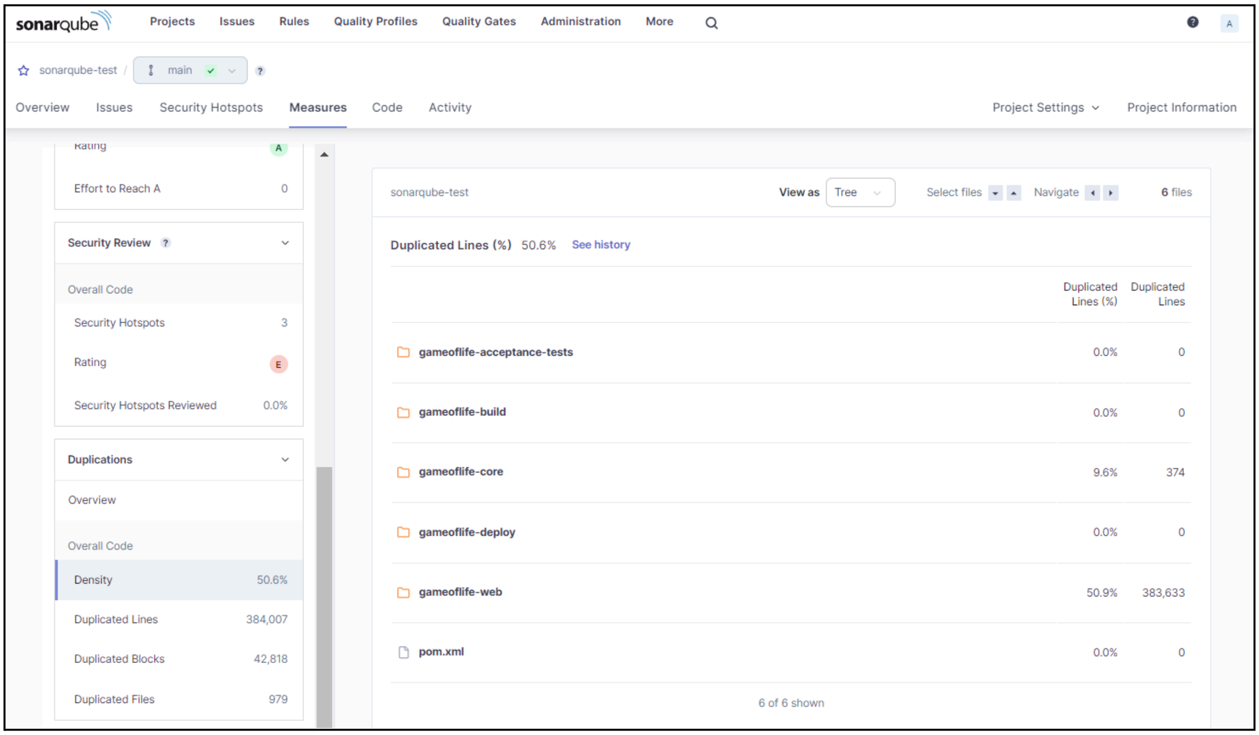
gameoflife-web/Dockerfile

```
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

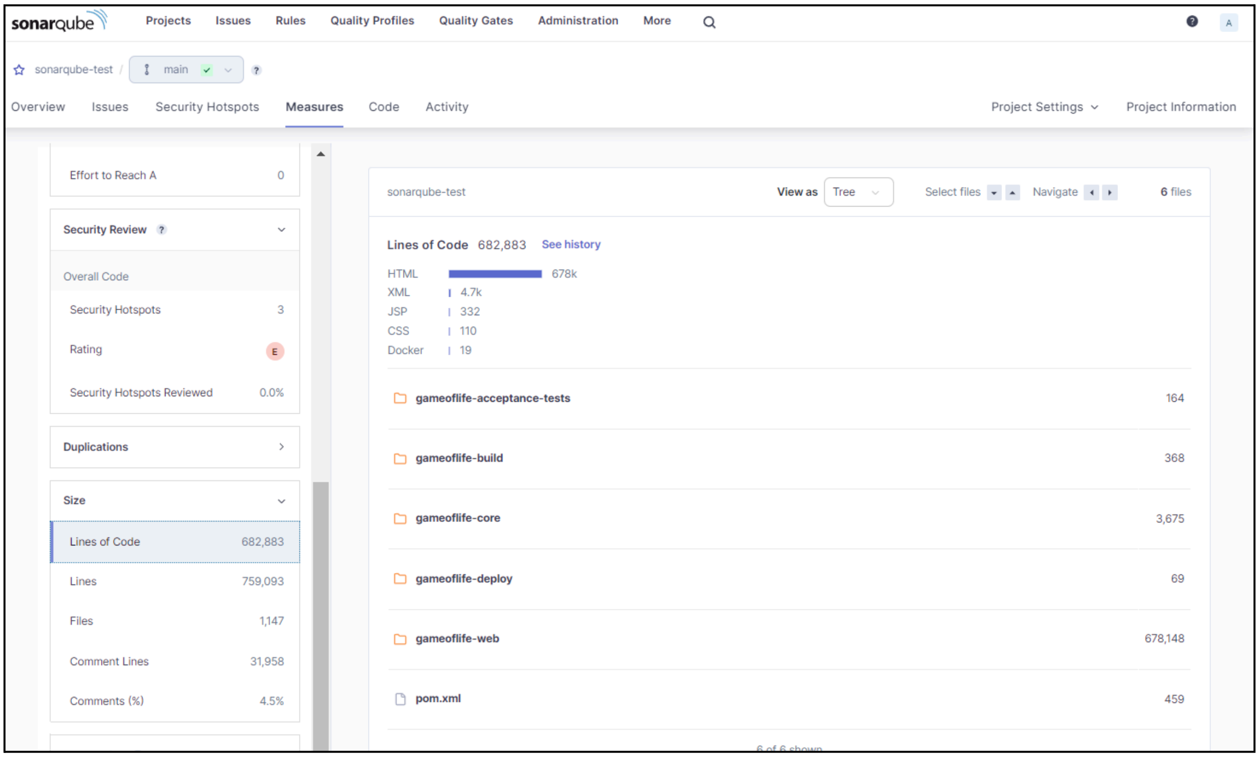
sonarqube-test 6 files

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   View as Tree   Select files   Navigate   **6** files

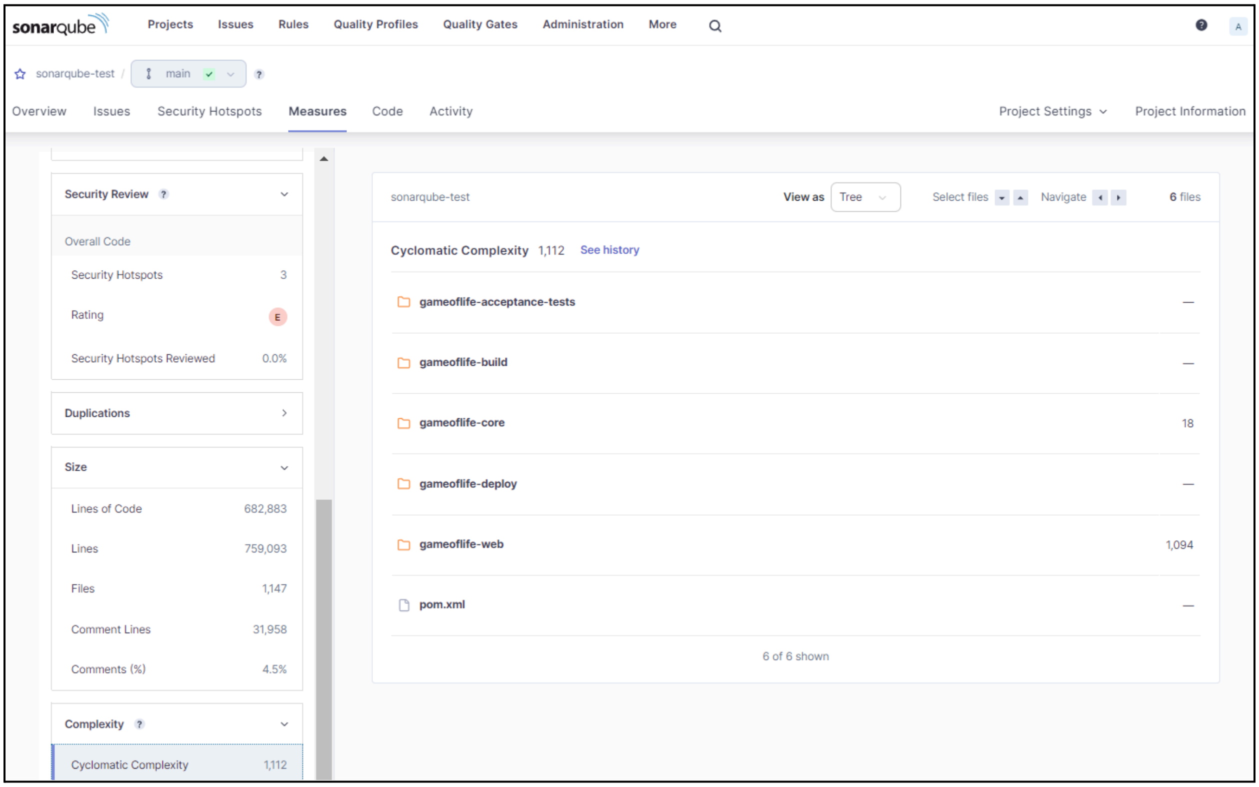
Lines of Code 682,883 See history

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

6 of 6 shown

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
Comments (%)	4.5%
Complexity	
Cyclomatic Complexity	1,112

sonarqube-test   View as Tree   Select files   Navigate   **6** files

Cyclomatic Complexity 1,112 See history

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

6 of 6 shown