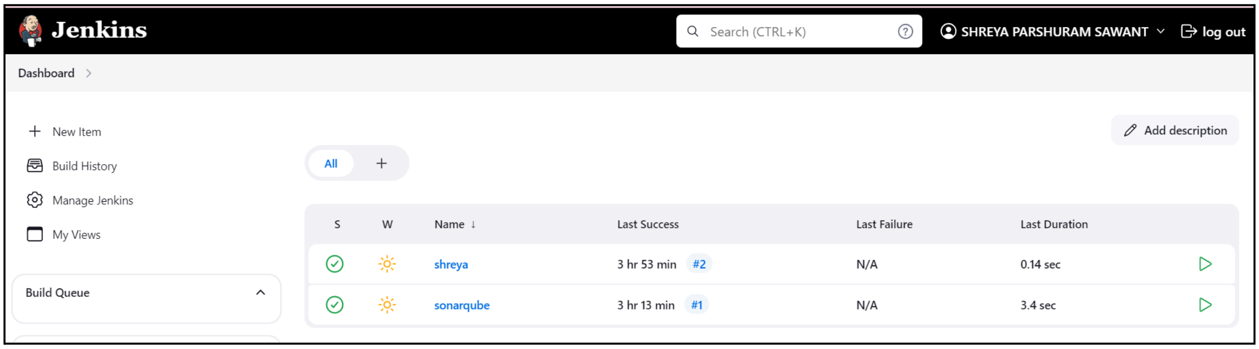
Shreya Sawant
D15A _54

Experiment.8

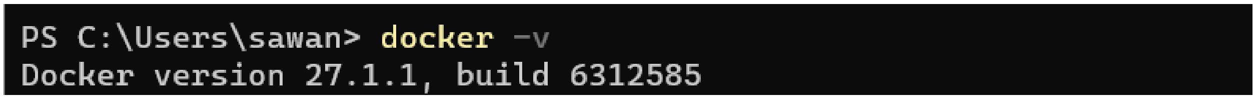
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static. analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web /Java / Python application.

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

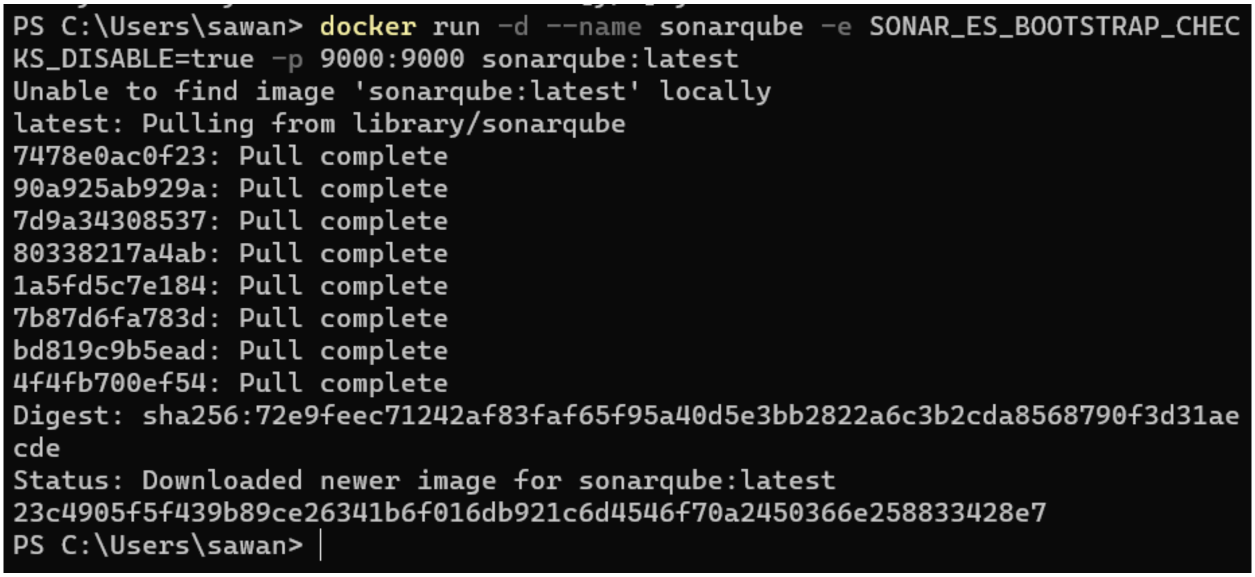


S	W	Name ↓	Last Success	Last Failure	Last Duration
✓	☼	shreya	3 hr 53 min #2	N/A	0.14 sec
✓	☼	sonarqube	3 hr 13 min #1	N/A	3.4 sec

Step.2 Run SonarQube in a Docker container using this command



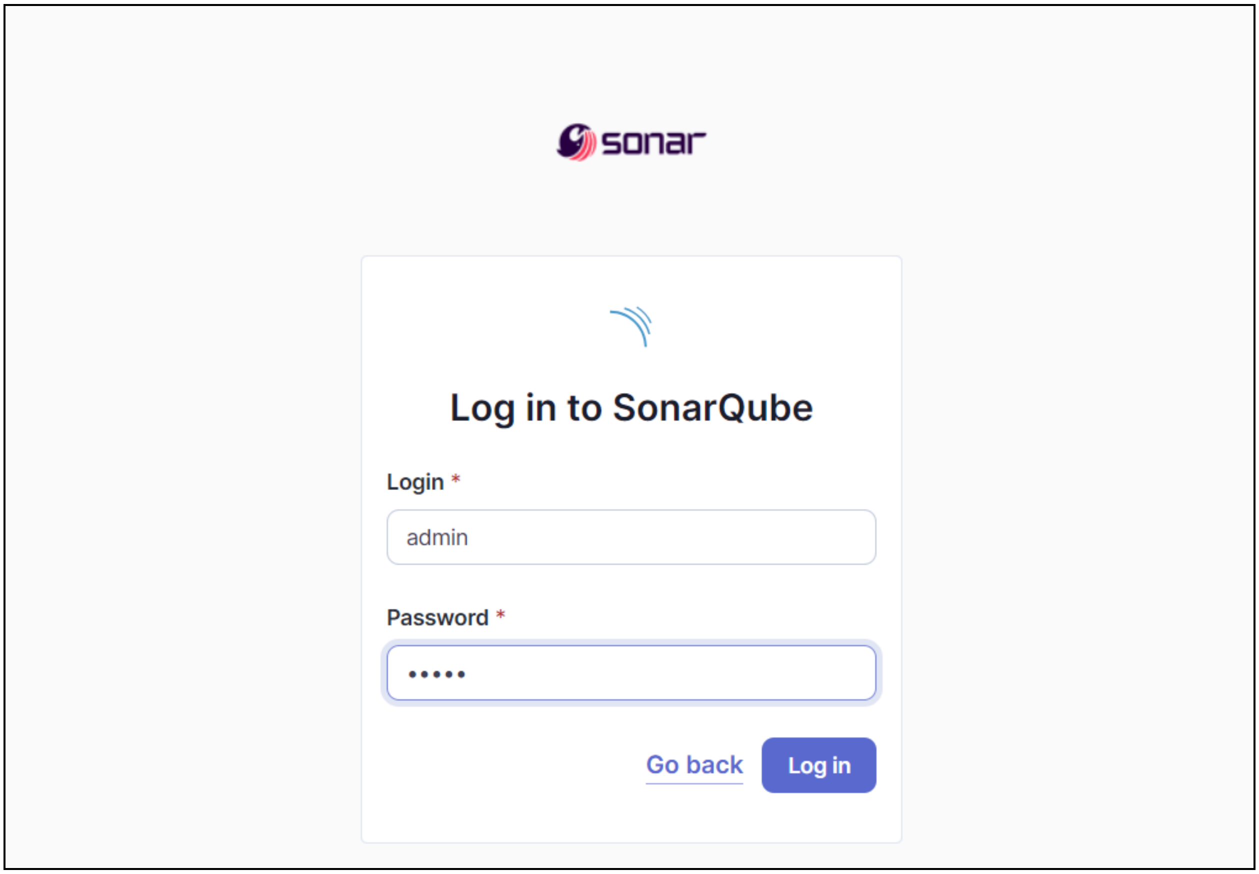
```
PS C:\Users\sawan> docker -v
Docker version 27.1.1, build 6312585
```



```
PS C:\Users\sawan> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHEC
KS_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: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31ae
cde
Status: Downloaded newer image for sonarqube:latest
23c4905f5f439b89ce26341b6f016db921c6d4546f70a2450366e258833428e7
PS C:\Users\sawan> |
```

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

Shreya Sawant
D15A _54



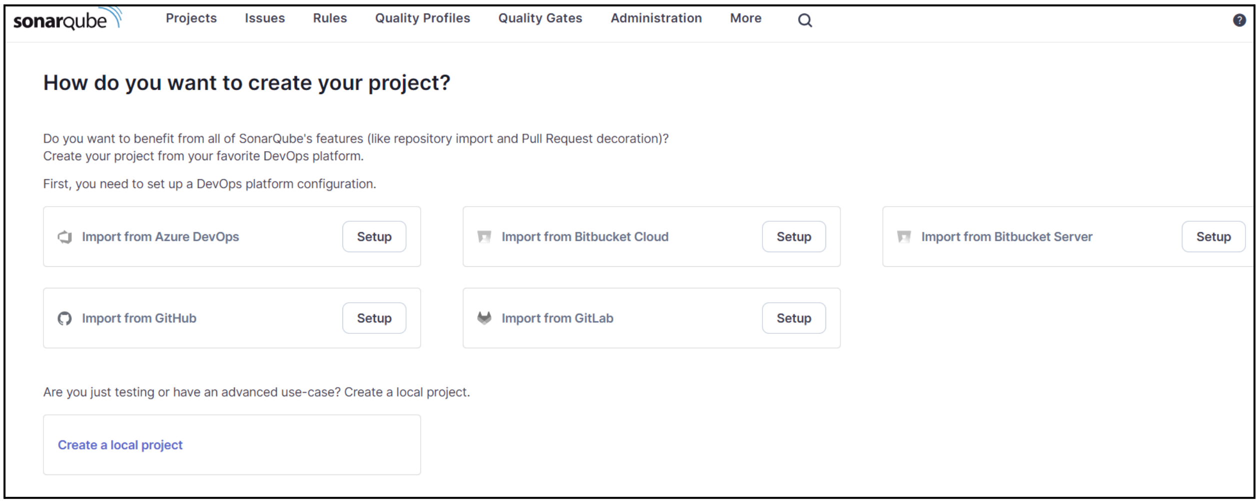
Log in to SonarQube

Login *

admin

Password *

•••••



How do you want to create your project?

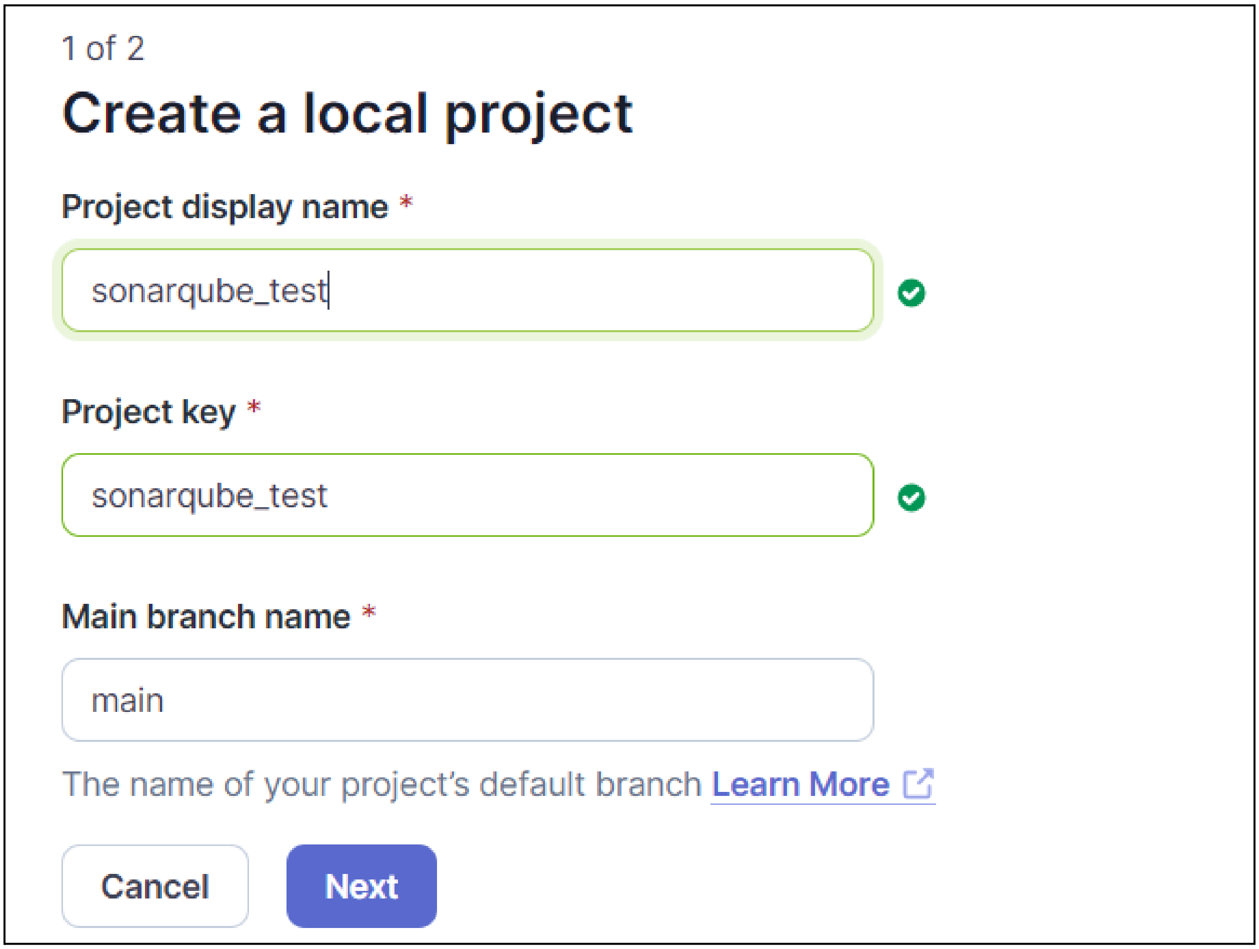
Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)?
Create your project from your favorite DevOps platform.

First, you need to set up a DevOps platform configuration.

Are you just testing or have an advanced use-case? Create a local project.

Shreya Sawant
D15A _54

Step.4 Create a manual project in SonarQube with the name sonarqube-test



1 of 2

Create a local project

Project display name *

sonarqube_test ✓

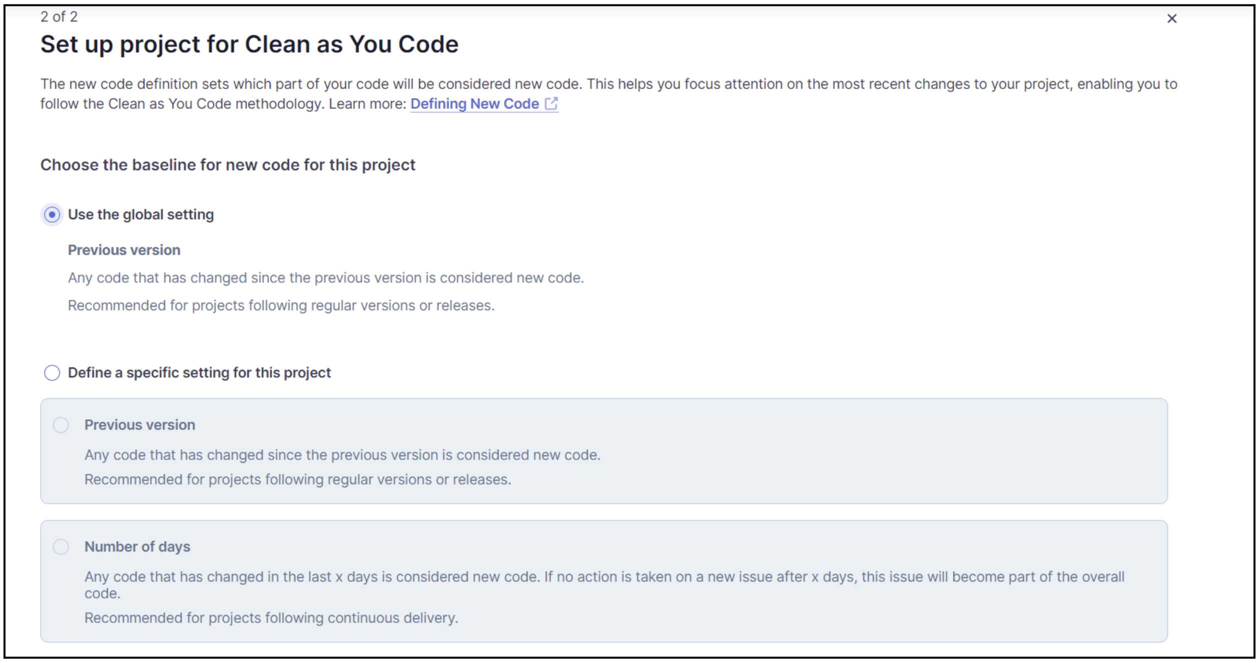
Project key *

sonarqube_test ✓

Main branch name *

main

The name of your project's default branch Learn More



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.

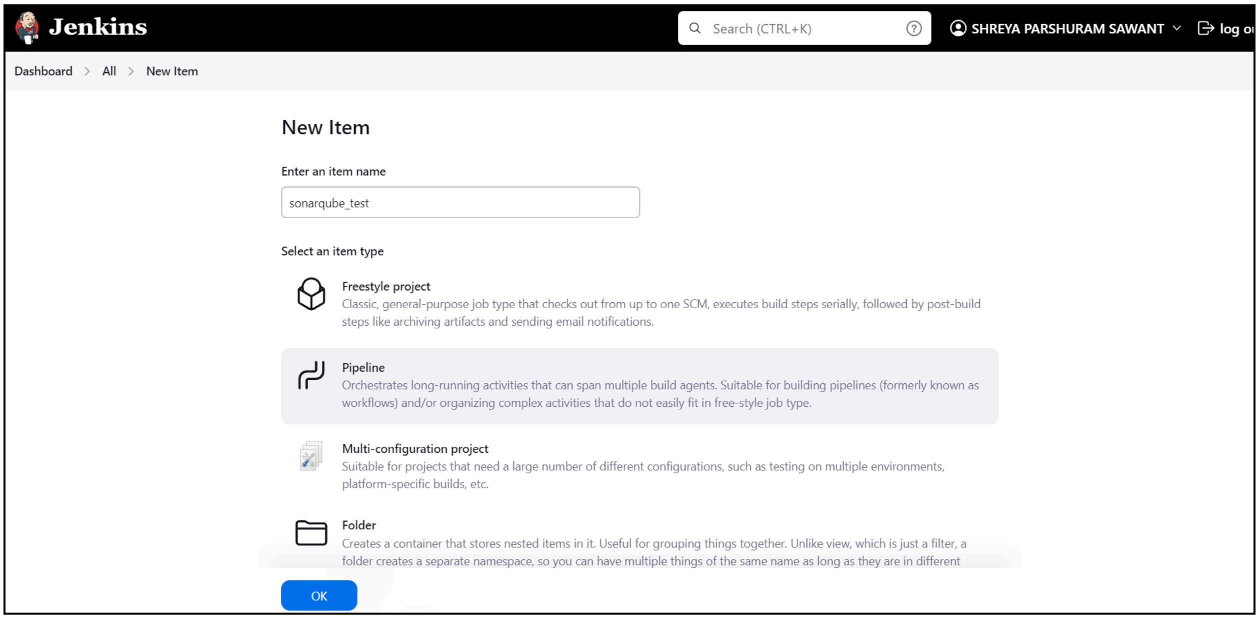
○ Number of days

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.

Shreya Sawant
D15A _54

Step.5 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.

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.

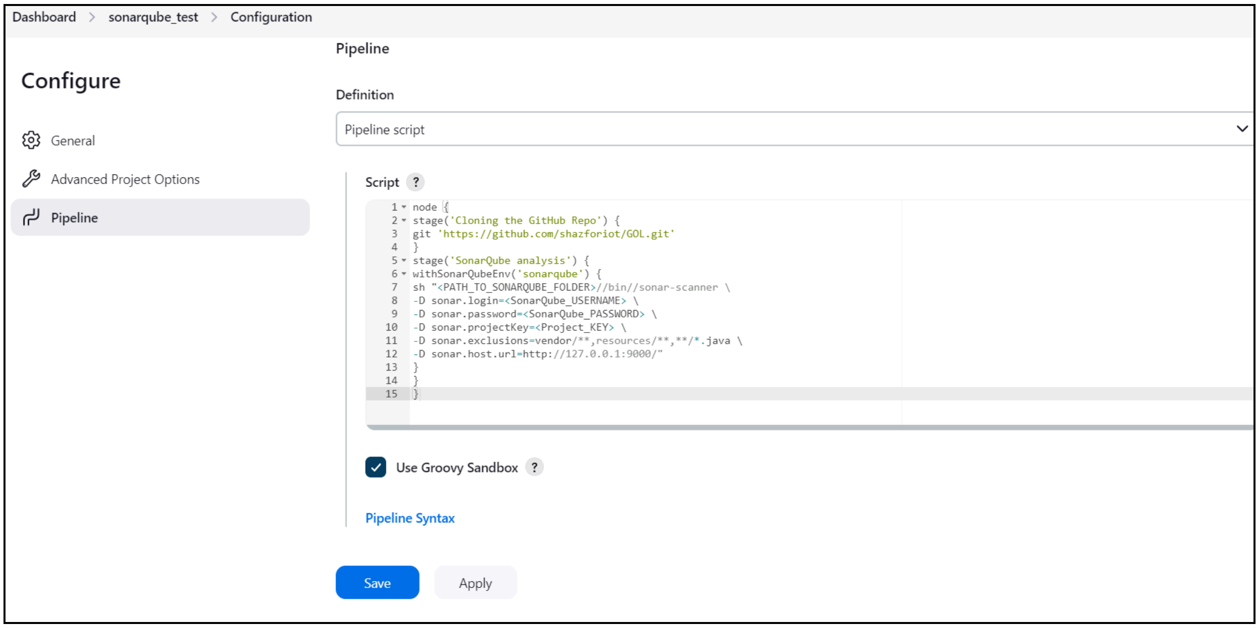
Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.

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

Under Pipeline Script, enter the following -

```
node {
stage('Cloning the GitHub Repo') {
git 'https://github.com/shazforiot/GOL.git'
}
stage('SonarQube analysis') {
withSonarQubeEnv('sonarqube') {
sh "<PATH_TO_SONARQUBE_FOLDER>//bin//sonar-scanner \
-D sonar.login=<SonarQube_USERNAME> \
-D sonar.password=<SonarQube_PASSWORD> \
-D sonar.projectKey=<Project_KEY> \
-D sonar.exclusions=vendor/**,resources/**,**/*.java \
-D sonar.host.url=http://127.0.0.1:9000/"
}
}
}
```

Shreya Sawant
D15A _54



Pipeline

Definition

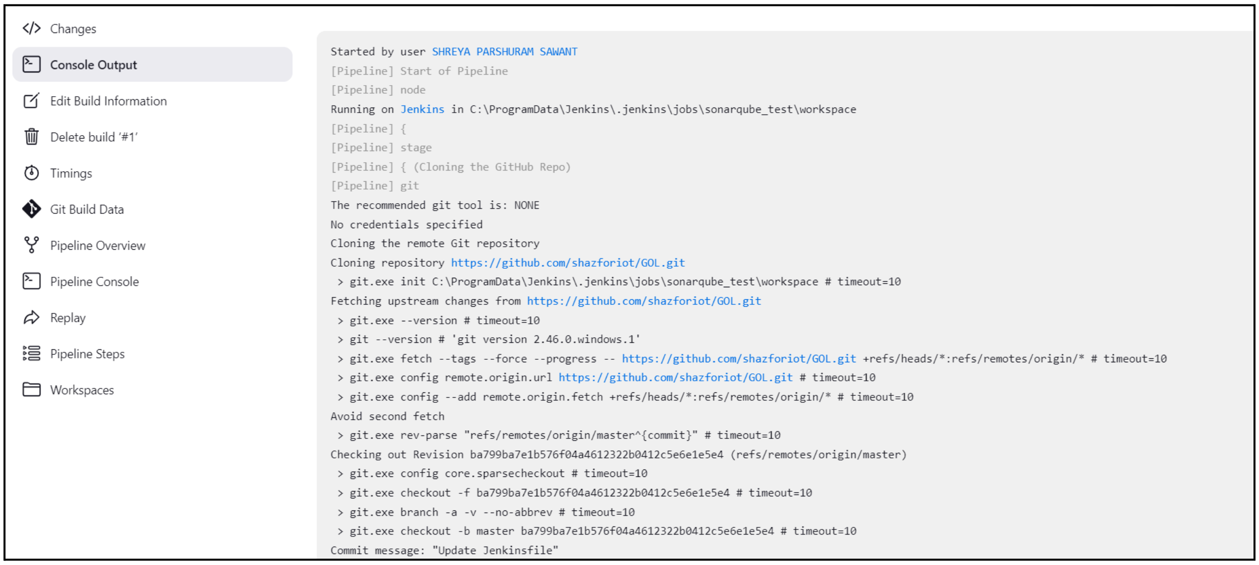
Pipeline script

Script ?

```
node {
stage('Cloning the GitHub Repo') {
git 'https://github.com/shazforiot/GOL.git'
}
stage('SonarQube analysis') {
withSonarQubeEnv('sonarqube') {
sh "<PATH_TO_SONARQUBE_FOLDER>//bin//sonar-scanner \
-D sonar.login=<SonarQube_USERNAME> \
-D sonar.password=<SonarQube_PASSWORD> \
-D sonar.projectKey=<Project_KEY> \
-D sonar.exclusions=vendor/**,resources/**,**/*.java \
-D sonar.host.url=http://127.0.0.1:9000/"
}
}
}
```

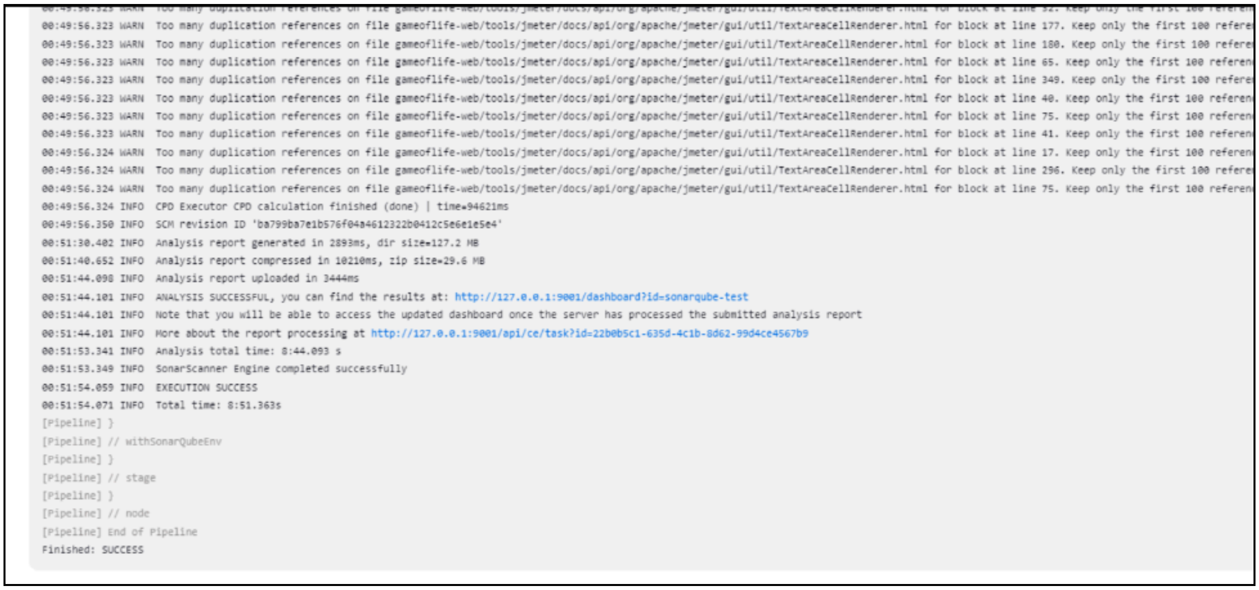
☑ Use Groovy Sandbox ?

Step.6 Run The Build.



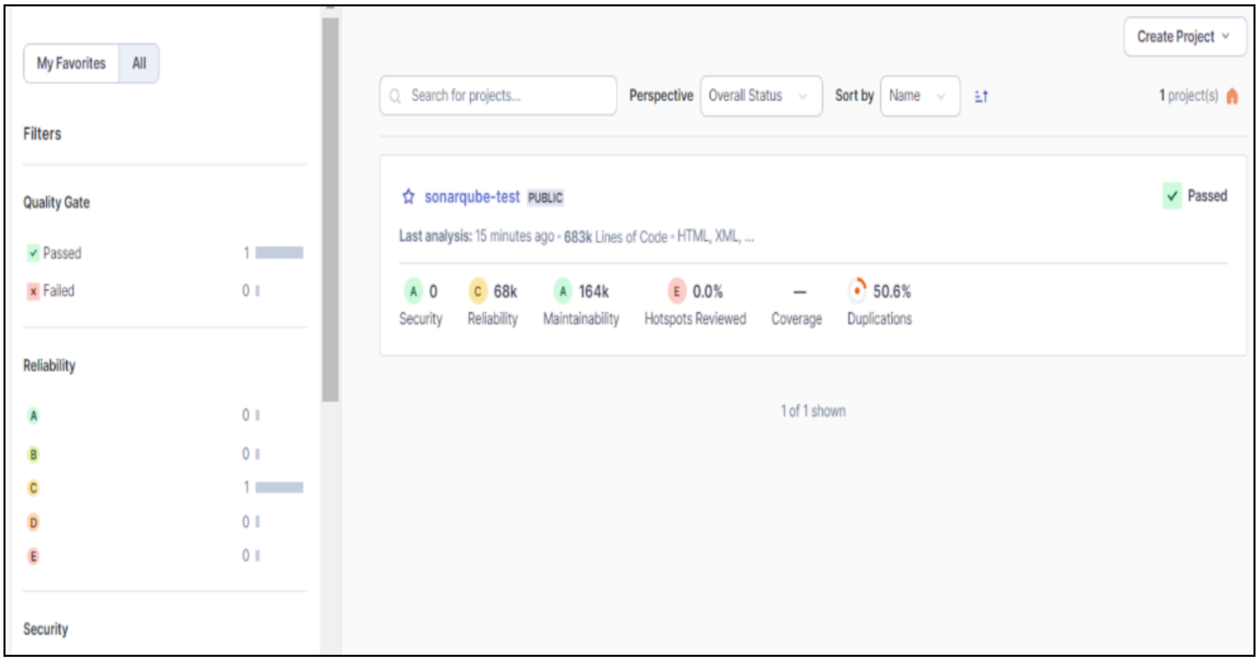
```
Started by user SHREYA PARSHURAM SAWANT
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in C:\ProgramData\Jenkins\.jenkins\jobs\sonarqube_test\workspace
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Cloning the GitHub Repo)
[Pipeline] git
The recommended git tool is: NONE
No credentials specified
Cloning the remote Git repository
Cloning repository https://github.com/shazforiot/GOL.git
 > git.exe init C:\ProgramData\Jenkins\.jenkins\jobs\sonarqube_test\workspace # timeout=10
Fetching upstream changes from https://github.com/shazforiot/GOL.git
 > git.exe --version # timeout=10
 > git --version # 'git version 2.46.0.windows.1'
 > git.exe fetch --tags --force --progress -- https://github.com/shazforiot/GOL.git +refs/heads/*:refs/remotes/origin/* # timeout=10
 > git.exe config remote.origin.url https://github.com/shazforiot/GOL.git # timeout=10
 > git.exe config --add remote.origin.fetch +refs/heads/*:refs/remotes/origin/* # timeout=10
Avoid second fetch
 > git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 (refs/remotes/origin/master)
 > git.exe config core.sparsecheckout # timeout=10
 > git.exe checkout -f ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
 > git.exe branch -a -v --no-abbrev # timeout=10
 > git.exe checkout -b master ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
Commit message: "Update Jenkinsfile"
```

Shreya Sawant
D15A _54



```
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 32. 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 177. Keep only the first 100 refere
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 refere
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 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 349. Keep only the first 100 refere
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 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 75. 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 41. 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 17. 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 296. Keep only the first 100 refere
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 referen
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.7 After that, check the project in SonarQube.



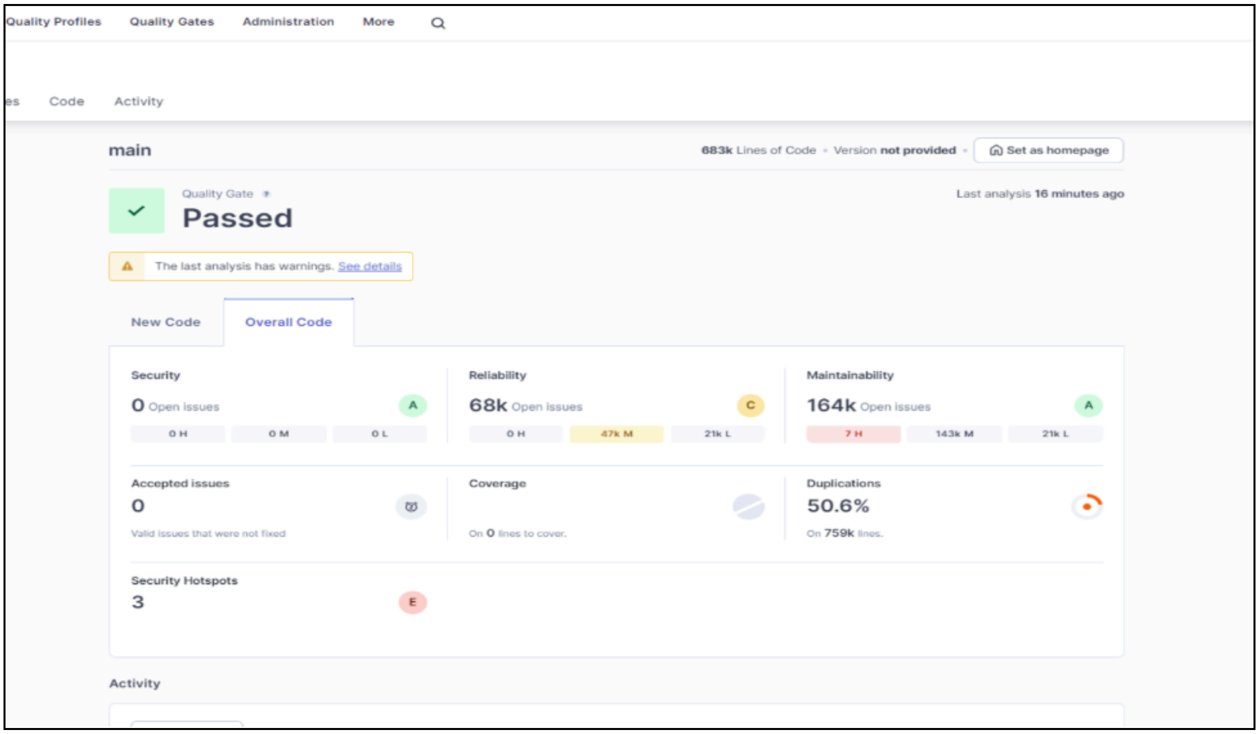
☆ sonarqube-test PUBLIC ✓ Passed

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

Shreya Sawant
D15A _54



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

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

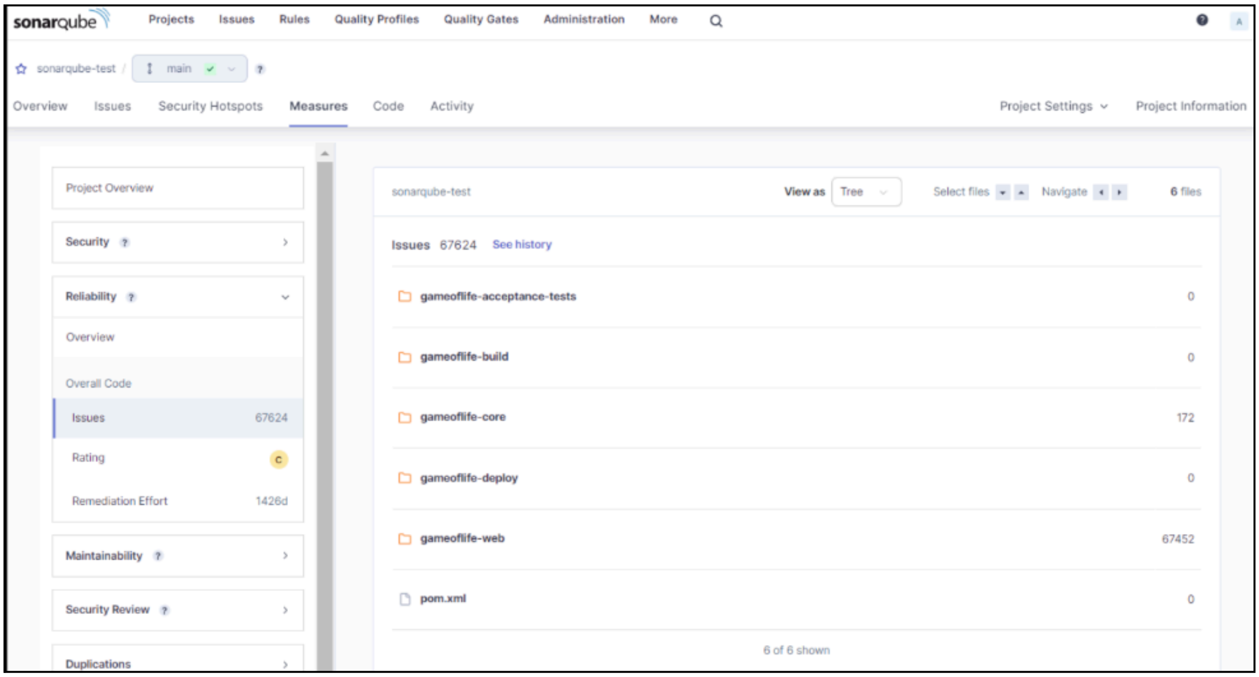
Accepted issues
0
Valid issues that were not fixed

Coverage
On 0 lines to cover.

Duplications
50.6%
On 759k lines.

Security Hotspots
3 E

Activity



Issues 67624
Rating C
Remediation Effort 1426d

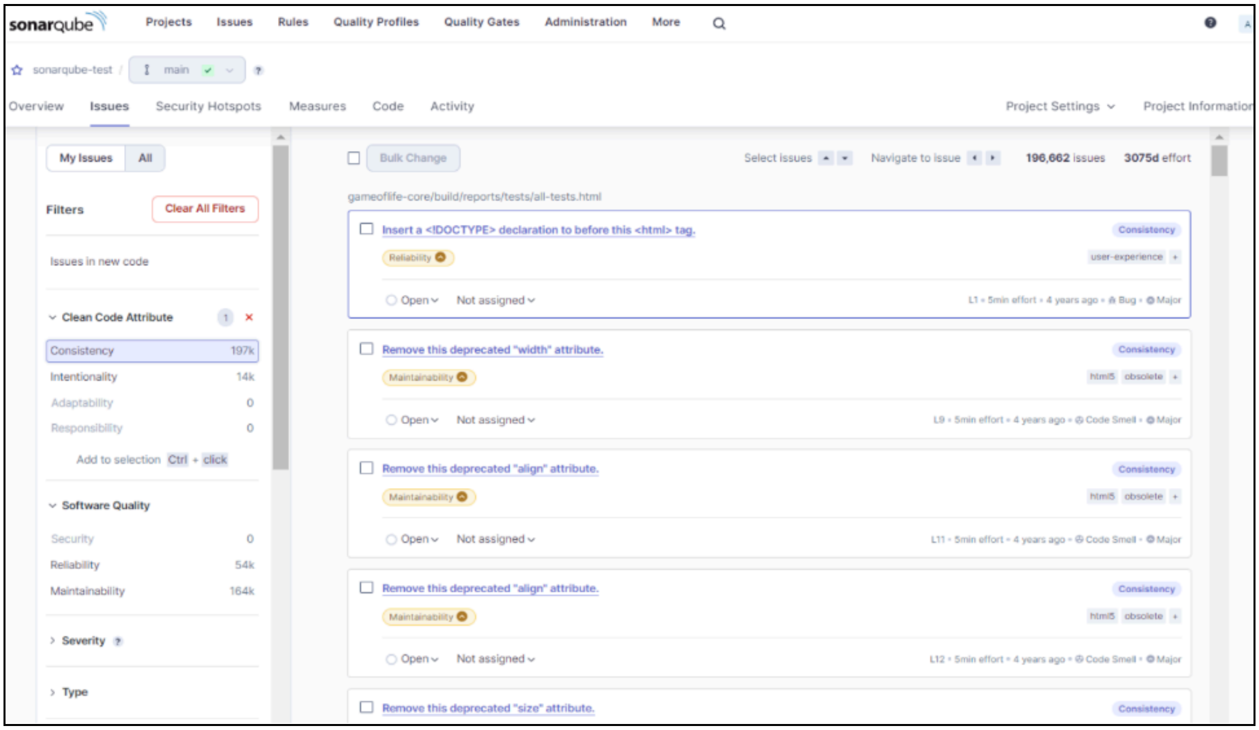
sonarqube-test   View as Tree   Select files   Navigate   6 files

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

Shreya Sawant
D15A _54



196,662 issues 3075d effort

Filters — Clear All Filters

Issues in new code

Clean Code Attribute 1

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Software Quality

Security	0
Reliability	54k
Maintainability	164k

Severity

Type

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

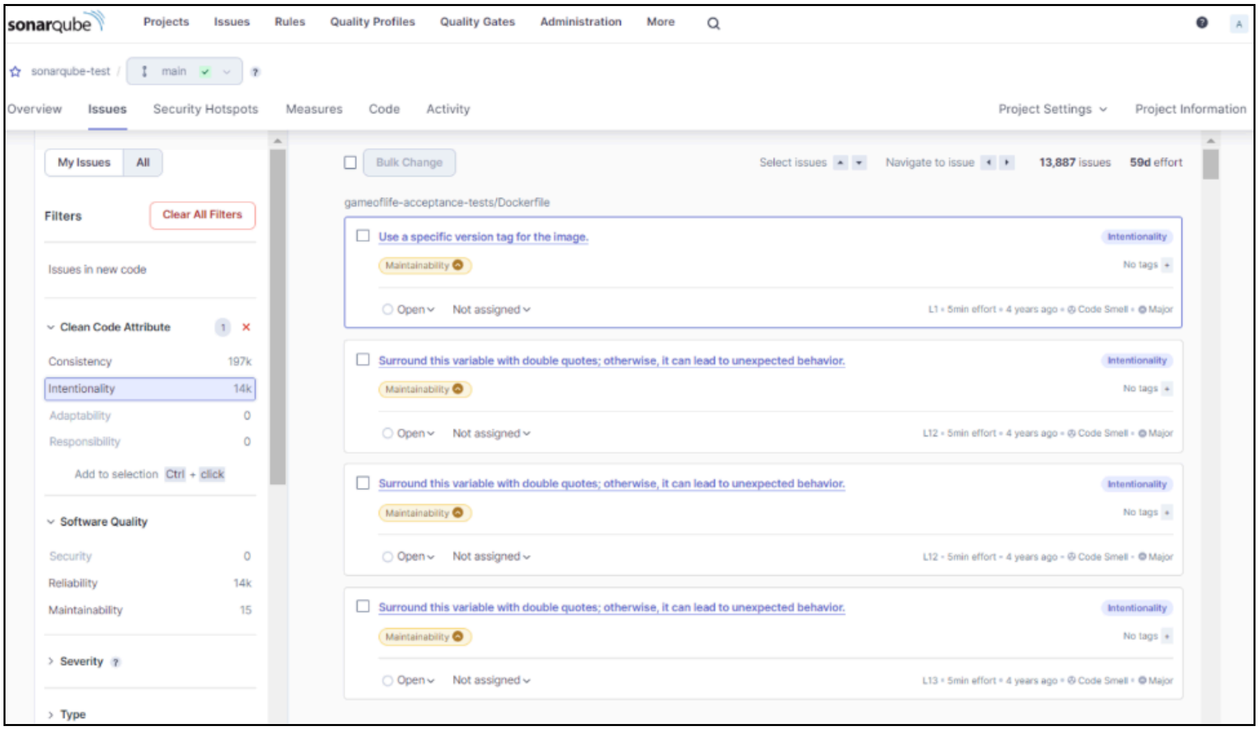
□ Insert a <!DOCTYPE> declaration to before this <html> tag. — Consistency
Reliability — user-experience +
○ Open — Not assigned — L1 • 5min effort • 4 years ago • Bug • Major

□ 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



13,887 issues 59d effort

Filters — Clear All Filters

Issues in new code

Clean Code Attribute 1

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Software Quality

Security	0
Reliability	14k
Maintainability	15

Severity

Type

gameoflife-acceptance-tests/Dockerfile

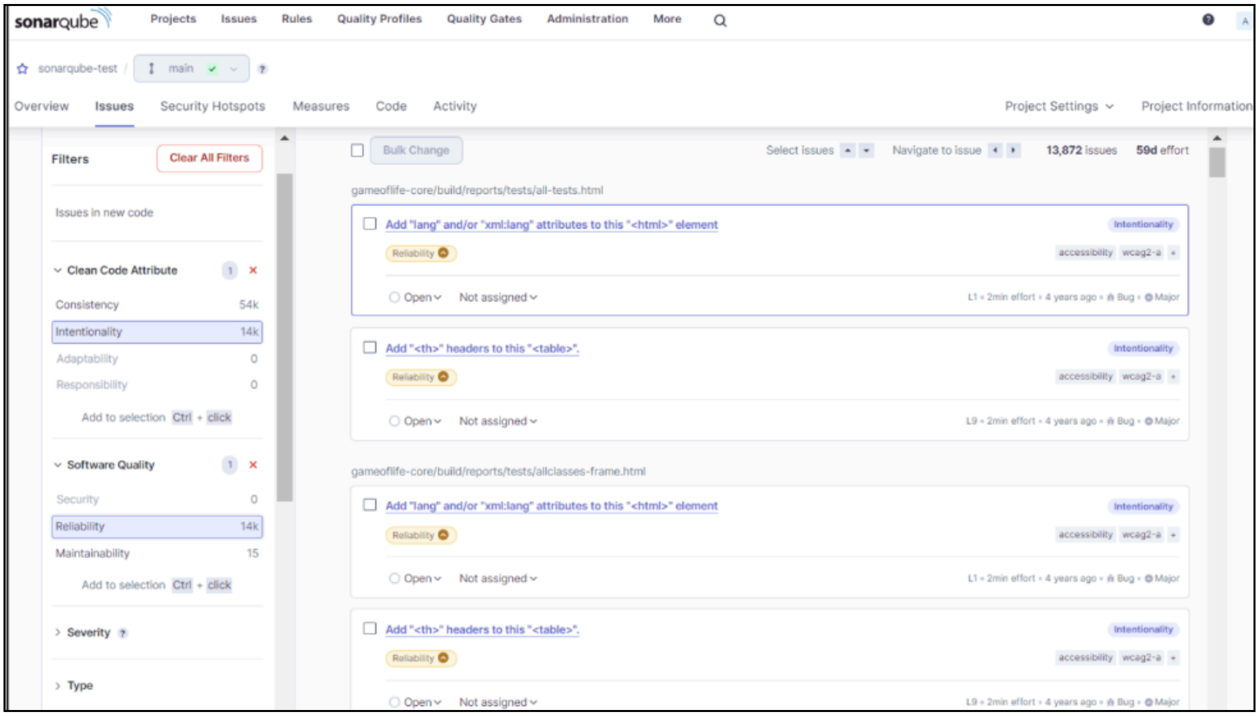
□ Use a specific version tag for the image. — Intentionality
Maintainability — No tags +
○ Open — Not assigned — L1 • 5min effort • 4 years ago • Code Smell • Major

□ 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

Shreya Sawant
D15A _54



sonarqube · Projects · Issues · Rules · Quality Profiles · Quality Gates · Administration · More

sonarqube-test / main

Overview · **Issues** · Security Hotspots · Measures · Code · Activity · Project Settings · Project Information

Filters · Clear All Filters

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

□ Bulk Change · Select issues · Navigate to issue · **13,872** issues · **59d** effort

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

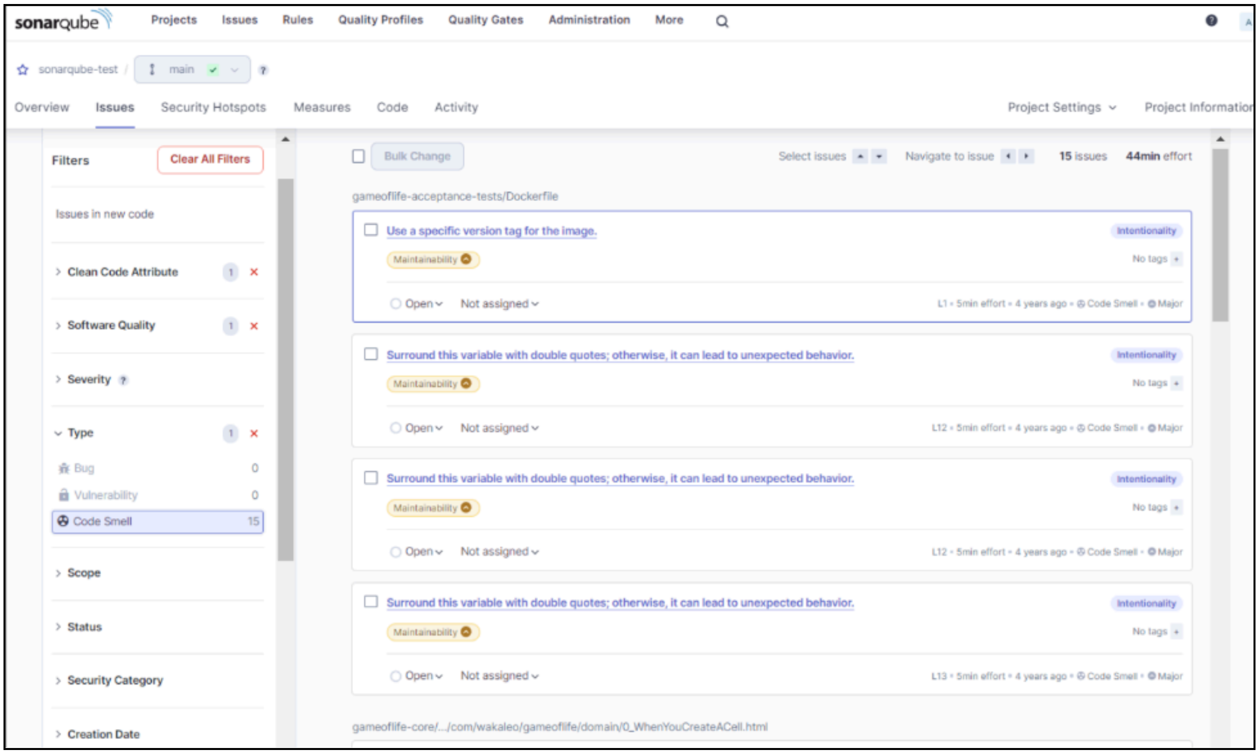
□ Add "lang" and/or "xml:lang" attributes to this "<html>" element · Intentionality
Reliability · accessibility · wcag2-a
○ Open · Not assigned · L1 • 2min effort • 4 years ago • Bug • Major

□ 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

□ 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



sonarqube · Projects · Issues · Rules · Quality Profiles · Quality Gates · Administration · More

sonarqube-test / main

Overview · **Issues** · Security Hotspots · Measures · Code · Activity · Project Settings · Project Information

Filters · Clear All Filters

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

□ Bulk Change · Select issues · Navigate to issue · **15** issues · **44min** 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

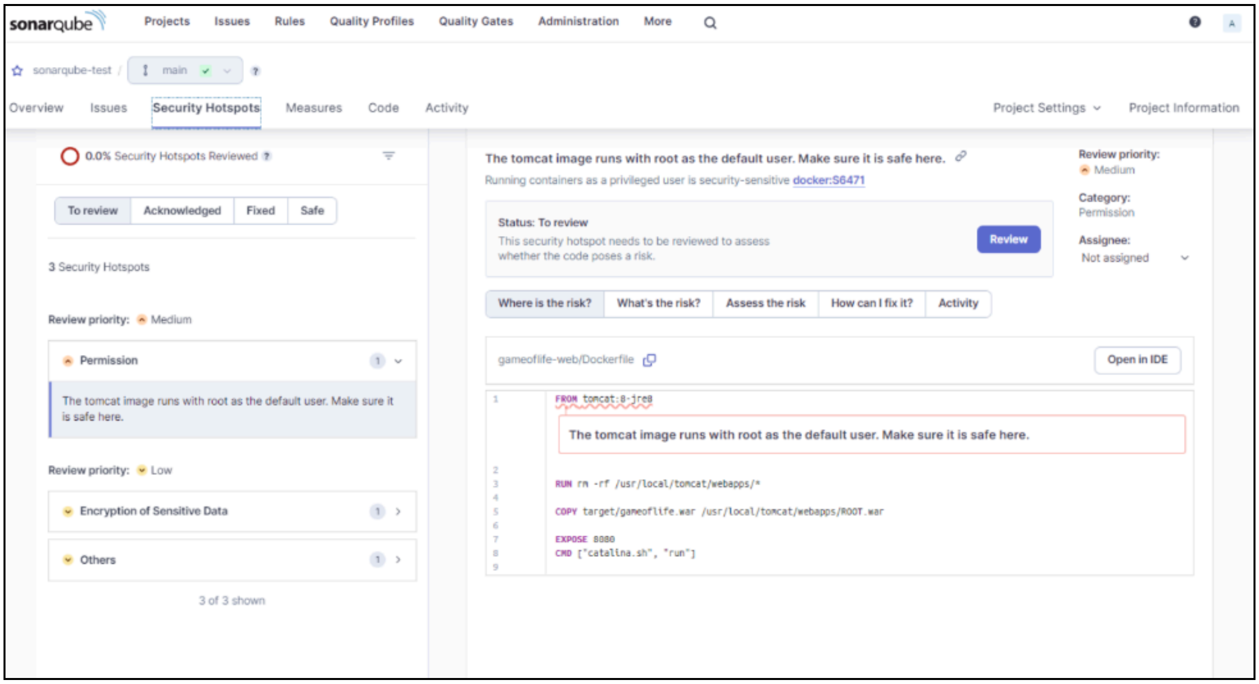
□ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. · Intentionality
Maintainability · No tags
○ Open · Not assigned · L12 • 5min effort • 4 years ago • Code Smell • Major

□ 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

gameoflife-core/.../com/wakaleo/gameoflife/domain/0_WhenYouCreateACell.html

Shreya Sawant
D15A _54



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.

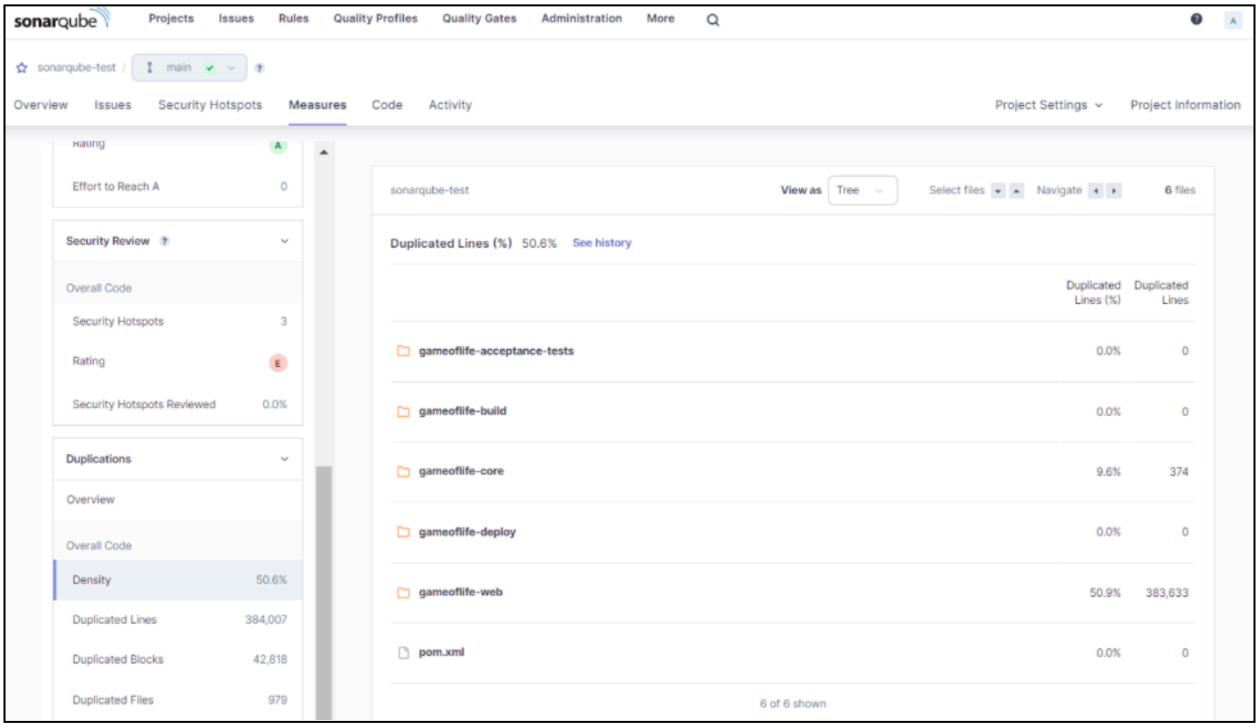
```

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

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

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

```



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

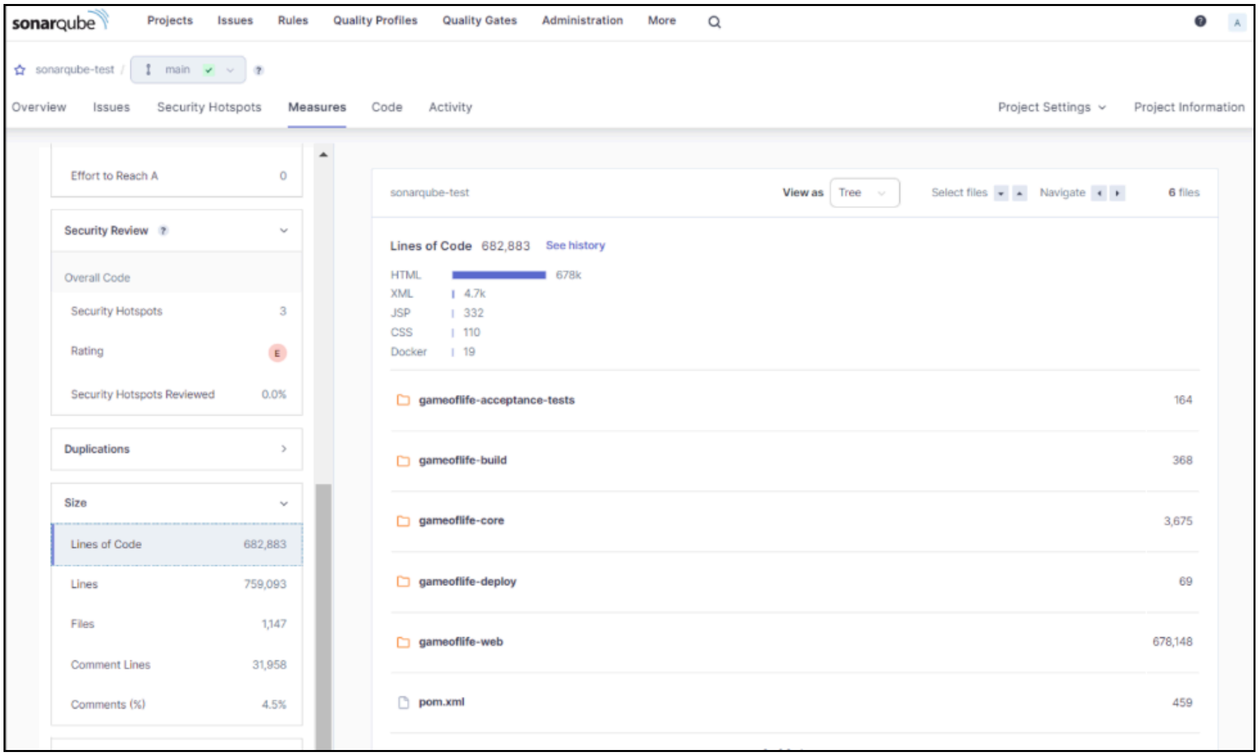
sonarqube-test View as Tree Select files Navigate 6 files

Duplicated Lines (%) 50.6% See history

	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

Shreya Sawant
D15A _54



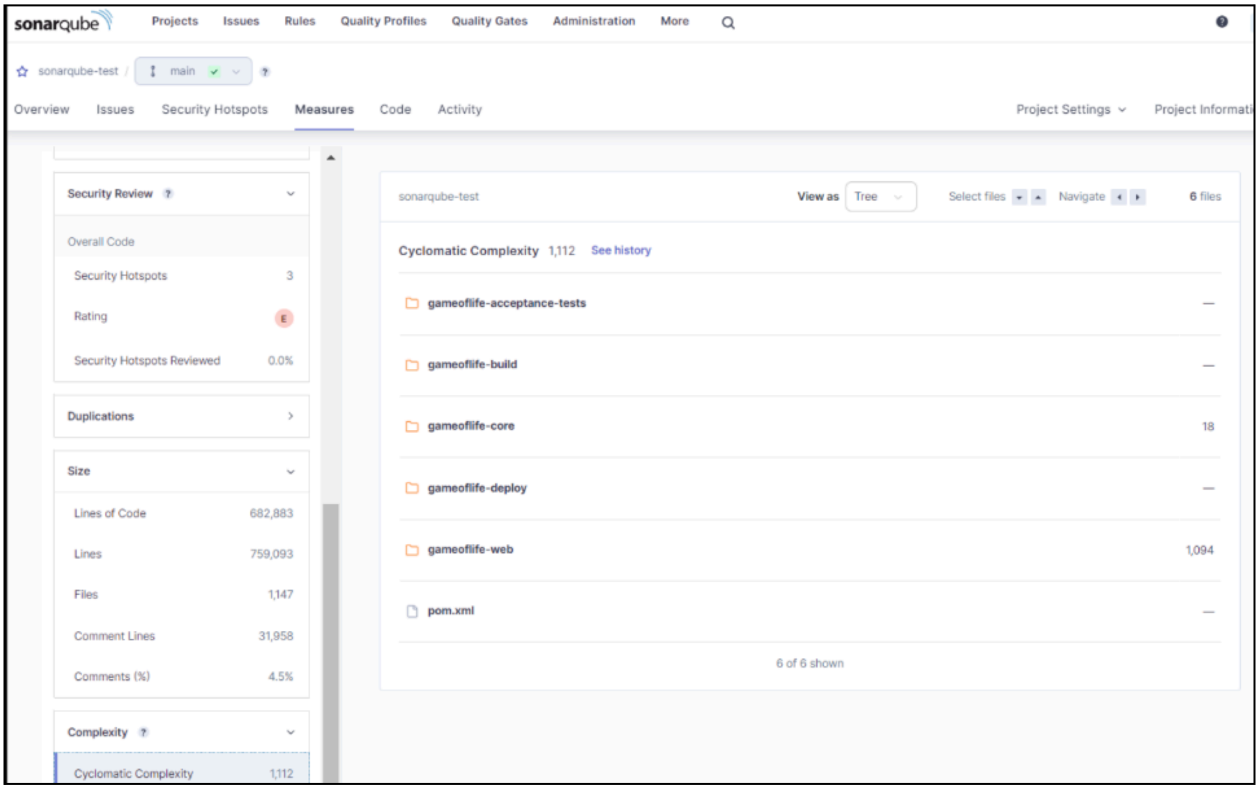
Effort to Reach A	0
Security Review	
Overall Code	
Security Hotspots	3
Rating	E
Security Hotspots Reviewed	0.0%
Duplications	
Size	
Lines of Code	682,883
Lines	759,093
Files	1,147
Comment Lines	31,958
Comments (%)	4.5%

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



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