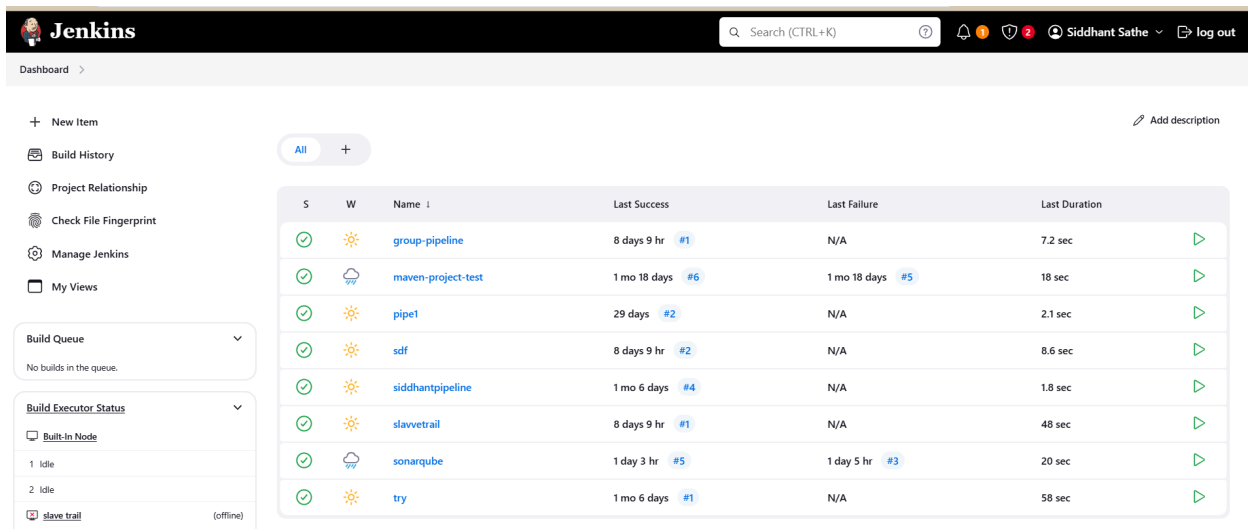


Experiment 8

Aim: Create a Jenkins CI/CD 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.



The screenshot shows the Jenkins Dashboard. On the left, there is a sidebar with navigation links: New Item, Build History, Project Relationship, Check File Fingerprint, Manage Jenkins, and My Views. Below these are sections for Build Queue (No builds in the queue) and Build Executor Status (1 idle, 2 idle, 1 slave trail offline). The main area displays a table of builds with columns: S (Status), W (Icon), Name, Last Success, Last Failure, and Last Duration. The table lists several builds, including 'group-pipeline', 'maven-project-test', 'pipe1', 'sdf', 'siddhantpipeline', 'slavvetrail', 'sonarqube', and 'try'.

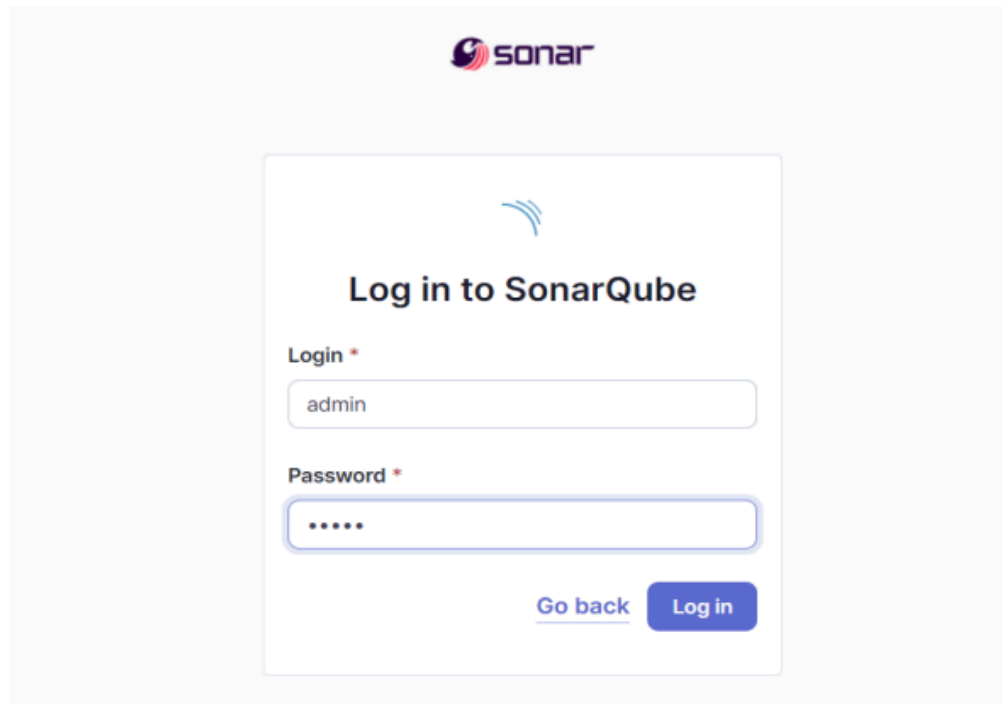
S	W	Name	Last Success	Last Failure	Last Duration
✓	☀	group-pipeline	8 days 9 hr #1	N/A	7.2 sec
✓	☁	maven-project-test	1 mo 18 days #6	1 mo 18 days #5	18 sec
✓	☀	pipe1	29 days #2	N/A	2.1 sec
✓	☀	sdf	8 days 9 hr #2	N/A	8.6 sec
✓	☀	siddhantpipeline	1 mo 6 days #4	N/A	1.8 sec
✓	☀	slavvetrail	8 days 9 hr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

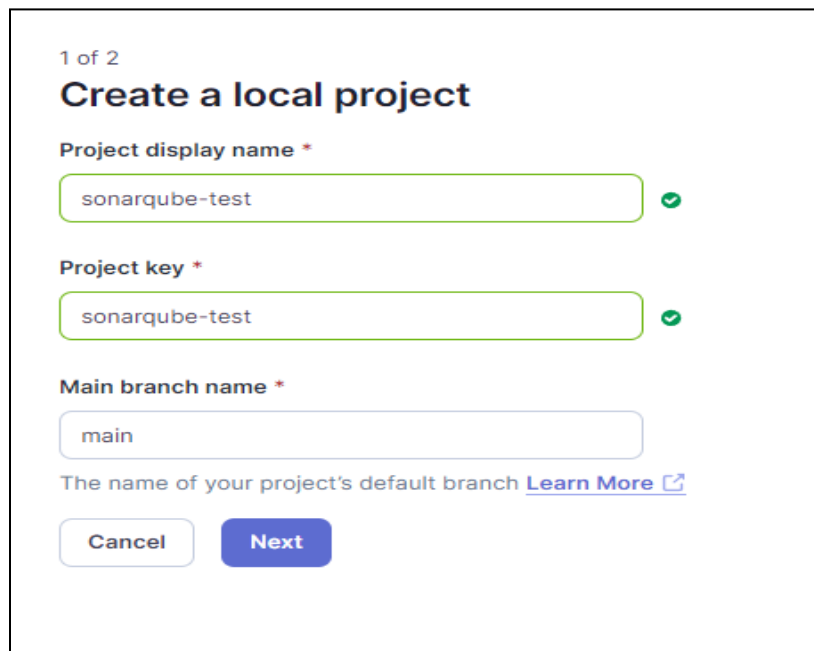
C:\Users\sathe>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecd
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 9001.



The image shows the SonarQube login interface. At the top is the Sonar logo. Below it is a white box with a blue Sonar icon and the text "Log in to SonarQube". There are two input fields: "Login *" with the value "admin" and "Password *" with masked characters ".....". At the bottom right of the box are two buttons: "Go back" (a link) and "Log in" (a blue button).

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



The image shows the "Create a local project" form in SonarQube. It is labeled "1 of 2" at the top. The title is "Create a local project". There are three input fields: "Project display name *" with the value "sonarqube-test" and a green checkmark, "Project key *" with the value "sonarqube-test" and a green checkmark, and "Main branch name *" with the value "main". Below the fields is a link "The name of your project's default branch [Learn More](#)". At the bottom are two buttons: "Cancel" and "Next".

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

6/17/20

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.

Back

Create project

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.

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=admin \
            -D sonar.projectKey=sonarqube-test \
            -D sonar.exclusions=vendor/**,resources/**,**/*.java \
            -D sonar.host.url=http://localhost:9000/"
        }
    }
}
```

Pipeline

Definition

Pipeline script

Script ?

```
1 node {
2     stage('Cloning the GitHub Repo') {
3         git 'https://github.com/shazforiot/GOL.git'
4     }
5     stage('SonarQube analysis') {
6         withSonarQubeEnv('sonarqube') {
7             bat """
8                 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 ^
9                 -D sonar.login=admin ^
10                -D sonar.password=ansh16 ^
11                -D sonar.projectKey=sonarqube-test ^
12                -D sonar.exclusions=vendor/**,resources/**,**/*.java ^
13                -D sonar.host.url=http://127.0.0.1:9001/
14            """
15        }
16    }
17 }
```

☒ Use Groovy Sandbox ?

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:

Dashboard > sonarqube-test >

Status

Changes

Build Now

Configure

Delete Pipeline

Full Stage View

SonarQube

Rename

Pipeline Syntax

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

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

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

Status

Changes

Console Output

View as plain text

Edit Build Information

Delete build '#4'

Git Build Data

Replay

Pipeline Steps

Workspaces

Previous Build

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-

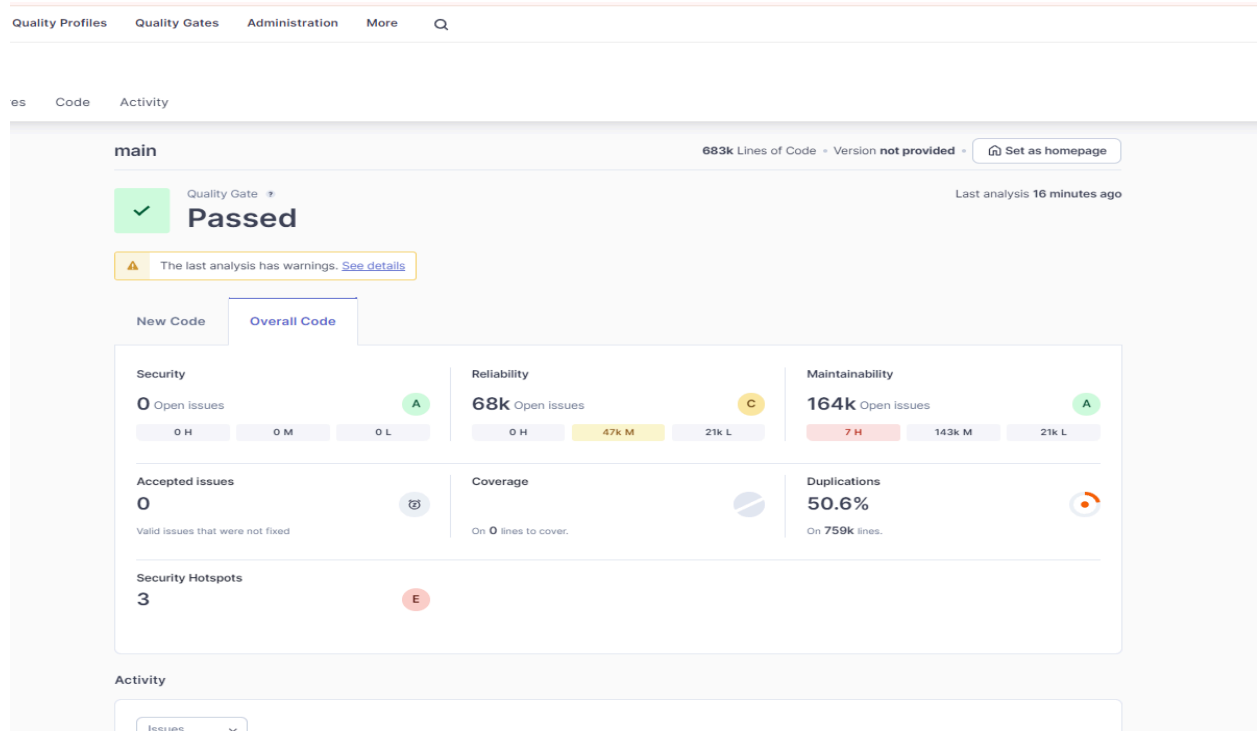
```

00:49:56.325 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 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 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 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 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 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 referen
00:49:56.350 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
00:51:44.090 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

```

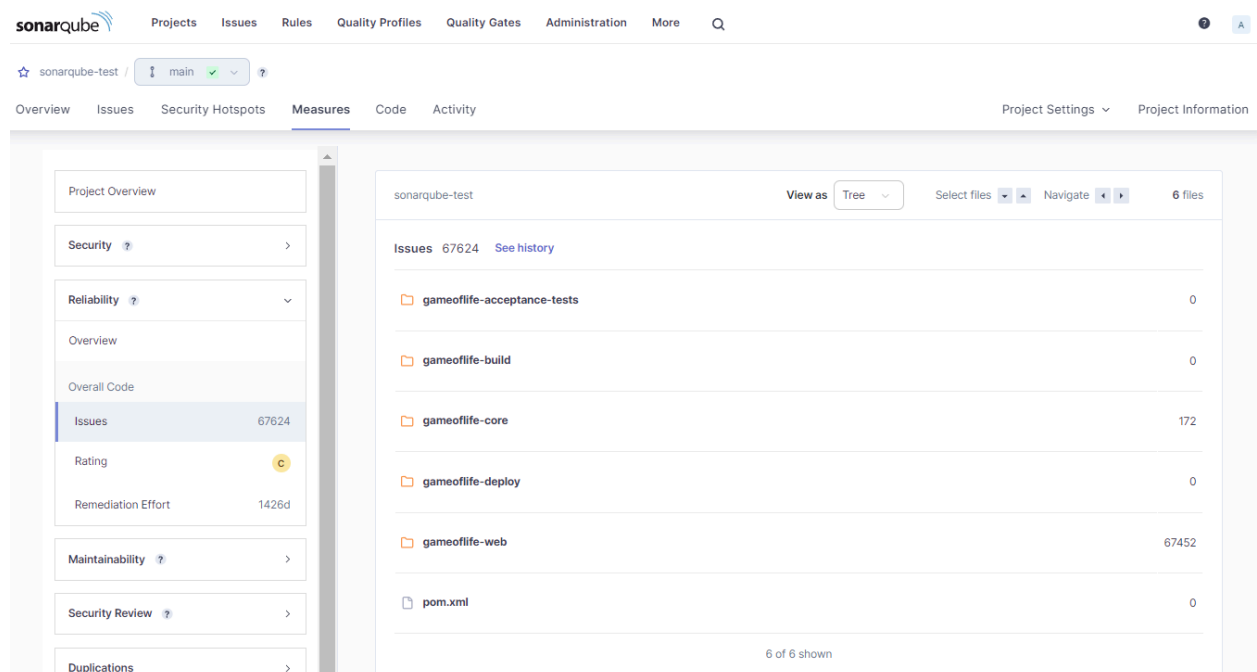
Step-9: After that, check the project in SonarQube.

The screenshot shows the SonarQube web interface. On the left, there is a sidebar with 'My Favorites' and 'All' tabs. Below these are sections for 'Filters', 'Quality Gate', and 'Reliability'. The 'Quality Gate' section shows 'Passed' with a green checkmark and 'Failed' with a red X. The 'Reliability' section shows a table with columns A, B, C, D, and E, and their respective counts. The main content area displays the project 'sonarqube-test' in the 'Perspective' view. It shows the project's overall status as 'Passed' with a green checkmark. Below this, it indicates the last analysis was 15 minutes ago and shows the project's metrics: 683k Lines of Code, HTML, XML, etc. The metrics are displayed as a horizontal bar chart with segments for Security (0), Reliability (68k), Maintainability (164k), Hotspots Reviewed (0.0%), Coverage (50.6%), and Duplications (50.6%).



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

Code issues:



Consistency:

The screenshot displays the SonarQube web interface for a project named 'sonarqube-test' on the 'main' branch. The 'Issues' tab is active, showing a list of 196,662 issues with a total effort of 3075d. The left sidebar contains filters for 'Clean Code Attribute' and 'Software Quality'. Under 'Clean Code Attribute', 'Consistency' is selected with 197k issues. Under 'Software Quality', 'Maintainability' is selected with 164k issues. The main panel shows a list of issues related to 'gameoflife-core/build/reports/tests/all-tests.html'. The issues are:

- Insert a <DOCTYPE> declaration to before this <html> tag.** (Consistency, Reliability, L1, 5min effort, 4 years ago, Bug, Major)
- Remove this deprecated "width" attribute.** (Consistency, Maintainability, L9, 5min effort, 4 years ago, Code Smell, Major)
- Remove this deprecated "align" attribute.** (Consistency, Maintainability, L11, 5min effort, 4 years ago, Code Smell, Major)
- Remove this deprecated "align" attribute.** (Consistency, Maintainability, L12, 5min effort, 4 years ago, Code Smell, Major)
- Remove this deprecated "size" attribute.** (Consistency, Maintainability)

Intentionally:

The screenshot displays the SonarQube web interface for the same project 'sonarqube-test' on the 'main' branch. The 'Issues' tab is active, showing a list of 13,887 issues with a total effort of 59d. The left sidebar shows the same filters as the previous screenshot, but 'Intentionally' is selected under 'Clean Code Attribute' with 14k issues. The main panel shows a list of issues related to 'gameoflife-acceptance-tests/Dockerfile'. The issues are:

- Use a specific version tag for the image.** (Intentionally, Maintainability, No tags, L1, 5min effort, 4 years ago, Code Smell, Major)
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.** (Intentionally, Maintainability, No tags, L12, 5min effort, 4 years ago, Code Smell, Major)
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.** (Intentionally, Maintainability, No tags, L12, 5min effort, 4 years ago, Code Smell, Major)
- Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.** (Intentionally, Maintainability, No tags, L13, 5min effort, 4 years ago, Code Smell, Major)

Reliability:

The screenshot shows the SonarQube web interface for a project named 'sonarqube-test'. The 'Issues' tab is active, displaying a list of 13,872 issues with a total effort of 59d. The left sidebar contains filters for 'Clean Code Attribute' and 'Software Quality'. Under 'Clean Code Attribute', 'Intentionality' is selected with 14k issues. Under 'Software Quality', 'Reliability' is selected with 14k issues. The main content area shows a list of issues related to 'gameoflife-core/build/reports/tests/all-tests.html'. The issues are: 'Add "lang" and/or "xml:lang" attributes to this "<html>" element' (Intentionality, Reliability, accessibility wcag2-a, L1, 2min effort, 4 years ago, Bug, Major) and 'Add "<th>" headers to this "<table>:"' (Intentionality, Reliability, accessibility wcag2-a, L9, 2min effort, 4 years ago, Bug, Major). Both issues are currently 'Open' and 'Not assigned'.

Code smells:

The screenshot shows the SonarQube web interface for the same project 'sonarqube-test'. The 'Issues' tab is active, displaying a list of 15 issues with a total effort of 44min. The left sidebar shows filters for 'Clean Code Attribute', 'Software Quality', 'Severity', and 'Type'. Under 'Type', 'Code Smell' is selected with 15 issues. The main content area shows a list of issues related to 'gameoflife-acceptance-tests/Dockerfile'. The issues are: 'Use a specific version tag for the image.' (Intentionality, Maintainability, No tags, 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, 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, L12, 5min effort, 4 years ago, Code Smell, Major), and 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.' (Intentionality, Maintainability, No tags, L13, 5min effort, 4 years ago, Code Smell, Major). All issues are currently 'Open' and 'Not assigned'.

Security hotspot:

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-test / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

0.0% Security Hotspots Reviewed

To review

Acknowledged

Fixed

Safe

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

Where is the risk?

What's the risk?

Assess the risk

How can I fix it?

Activity

gameoflife-web/Dockerfile

Open in IDE

1

FROM tomcat:8-jre8

2

3

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

4

5

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

6

7

EXPOSE 8080

8

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

9

Duplicates:

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-test / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

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

Size:

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-test

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Effort to Reach A0

Security Review

Overall Code

Security Hotspots3

RatingE

Security Hotspots Reviewed0.0%

Duplications

Size

Lines of Code682,883

Lines759,093

Files1,147

Comment Lines31,958

Comments (%)4.5%

sonarqube-test

View asTree

Select files

Navigate

6 files

Lines of Code682,883

HTML678k

XML4.7k

JSP332

CSS110

Docker19

gameoflife-acceptance-tests164

gameoflife-build368

gameoflife-core3,675

gameoflife-deploy69

gameoflife-web678,148

pom.xml459

Complexity:

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-test

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Security Review

Overall Code

Security Hotspots3

RatingE

Security Hotspots Reviewed0.0%

Duplications

Size

Lines of Code682,883

Lines759,093

Files1,147

Comment Lines31,958

sonarqube-test

View asTree

Select files

Cyclomatic Complexity1,112

gameoflife-acceptance-tests

gameoflife-build

gameoflife-core

gameoflife-deploy

gameoflife-web

pom.xml

6 of 6 shown