

# ADVANCE DEVOPS EXP-8

PRANAV TITAMBE

D15A/62

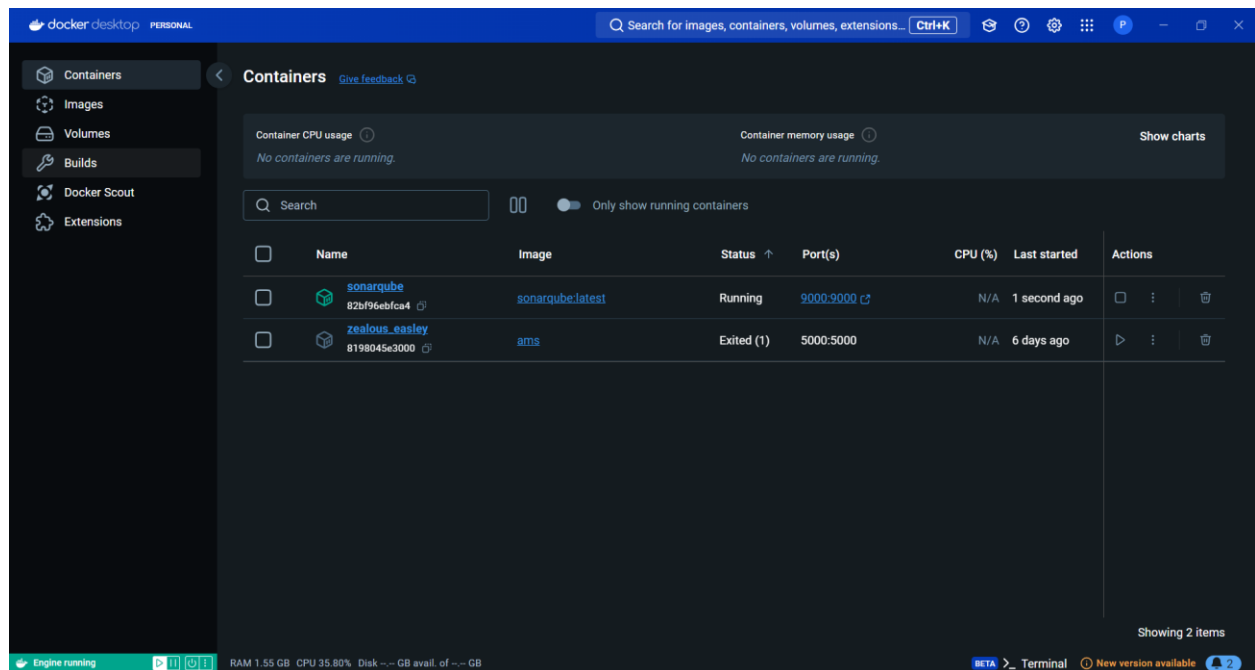
**Aim:** To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.

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

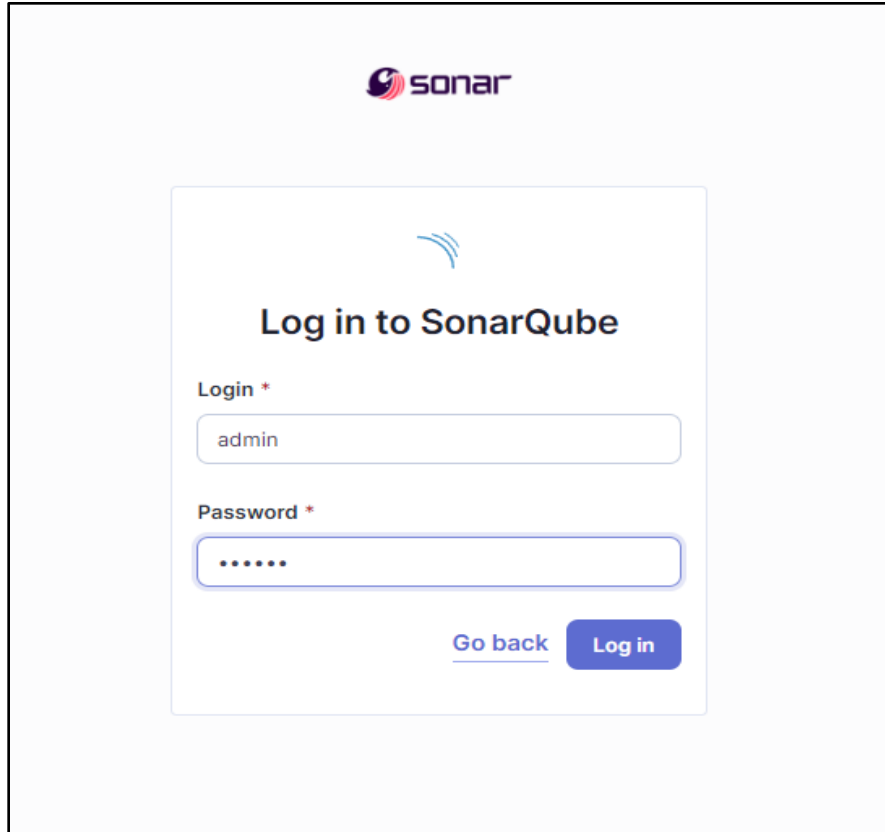
The screenshot shows the Jenkins Dashboard interface. At the top, there's a header with the Jenkins logo, a search bar, and user information (Pranav Pramod Titambe). Below the header, the main content area displays a table of build history. The table has columns for status (S), weather icon (W), name, last success, last failure, and last duration. The builds listed are DevOps Pipeline, maven-project-test, practical-maven-project, practical-pipeline, and sonar-qube-test. On the left sidebar, there are links for 'New Item', 'Build History', 'Project Relationship', 'Check File Fingerprint', 'Manage Jenkins', and 'My Views'. Below these, there are sections for 'Build Queue' (showing no builds) and 'Build Executor Status' (showing two idle executors and one offline executor named 'slave-test-1').

| S | W | Name                    | Last Success    | Last Failure | Last Duration |
|---|---|-------------------------|-----------------|--------------|---------------|
| ✓ | ☀ | DevOps Pipeline         | 27 days #5      | N/A          | 6.6 sec       |
| ✓ | ☀ | maven-project-test      | 1 mo 16 days #3 | N/A          | 1 min 0 sec   |
| ✓ | ☀ | practical-maven-project | 27 days #1      | N/A          | 34 sec        |
| ✓ | ☁ | practical-pipeline      | 27 days #5      | 27 days #4   | 1.5 sec       |
| ✓ | ☀ | sonar-qube-test         | 1 day 2 hr #5   | N/A          | 24 sec        |

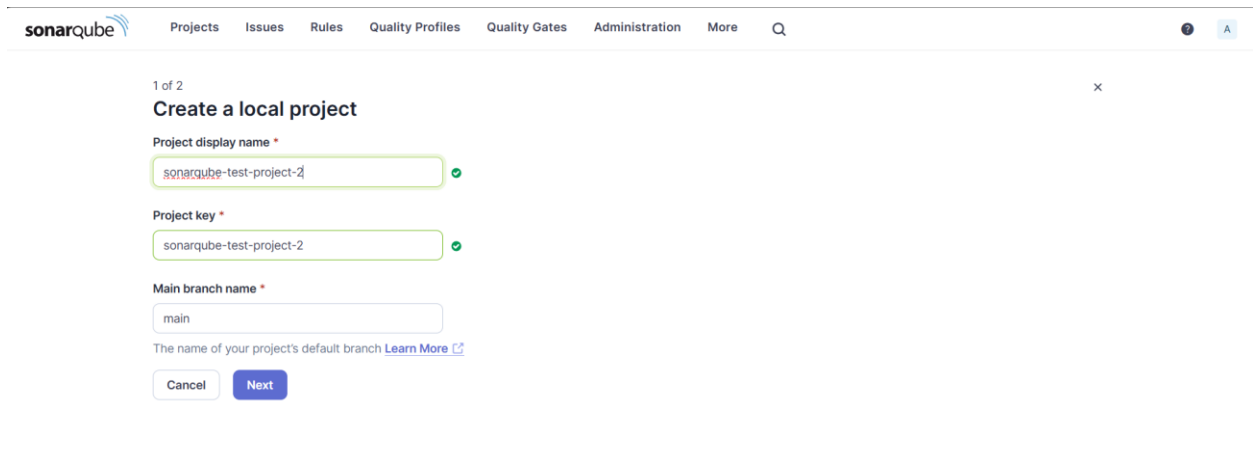
**Step-2:** Run SonarQube in a Docker container using this command :- a]docker -v  
b] docker run -d --name sonarqube -e SONAR\_ES\_BOOTSTRAP\_CHECKS\_DISABLE=true -p 9000:9000 sonarqube:latest



**Step-3:** Once the container is up and running, you can check the status of SonarQube at localhost port 9000. The login id is “admin” and the password is also “pranav”.



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

The image shows the "Create a local project" form in the SonarQube web interface. The top navigation bar includes the SonarQube logo and links for Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, and More. The form is titled "1 of 2 Create a local project". It contains three input fields: "Project display name \*" with the value "sonarqube-test-project-2" and a green checkmark, "Project key \*" with the value "sonarqube-test-project-2" and a green checkmark, and "Main branch name \*" with the value "main". Below the last field is a note: "The name of your project's default branch [Learn More](#)". At the bottom are "Cancel" and "Next" buttons.

**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.

Back
Create project

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

Jenkins

Search (CTRL+K)

Pranav Pramod Titambe
log out

Dashboard > sonarqube-pipeline > Configuration

Configure

General
Advanced Project Options
Pipeline

General

Description

Plain text Preview

☐ Discard old builds
☐ Do not allow concurrent builds
☐ Do not allow the pipeline to resume if the controller restarts
☐ GitHub project
☐ Pipeline speed/durability override

Save
Apply

Enabled

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

```

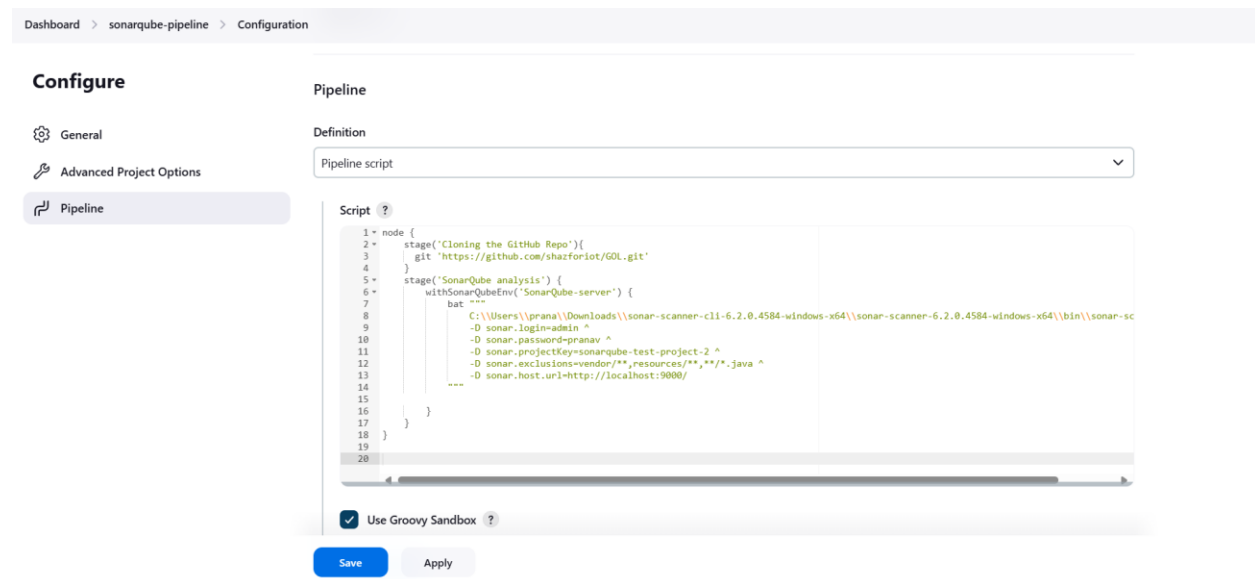
node {
  stage('Cloning the GitHub Repo'){
    git 'https://github.com/shazforiot/GOL.git'
  }
  stage('SonarQube analysis') {

```

```

withSonarQubeEnv('SonarQube-server') {
    bat """
        C:\\Users\\prana\\Downloads\\sonar-scanner-cli-6.2.0.4584-windows-x64\\sonar-scanner-
6.2.0.4584-windows-x64\\bin\\sonar-scanner.bat ^
        -D sonar.login=admin ^
        -D sonar.password=pranav ^
        -D sonar.projectKey=sonarqube-test-project-2 ^
        -D sonar.exclusions=vendor/**,resources/**,**/*.java ^
        -D sonar.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:

Jenkins

Search (CTRL+K)

Pranav Pramod Titambe log out

Dashboard > sonarqube-pipeline

Status

Changes

Build Now

Configure

Delete Pipeline

Full Stage View

SonarQube

Stages

Rename

Pipeline Syntax

Build History trend

Filter...

sonarqube-pipeline

Add description

Disable Project

Stage View

|   |                          | Cloning the GitHub Repo | SonarQube analysis |
|---|--------------------------|-------------------------|--------------------|
| Average stage times:<br>(Average full run time: ~10min 43s) |                          | 3s                      | 1min 47s           |
| #6  | Sept 25 22:53 No Changes | 2s                      | 10min 40s          |
| #7  | Sept 25 22:48 No Changes | 2s                      | 3s failed          |
| #8  | Sept 25 22:33 No Changes | 2s                      | 1s                 |

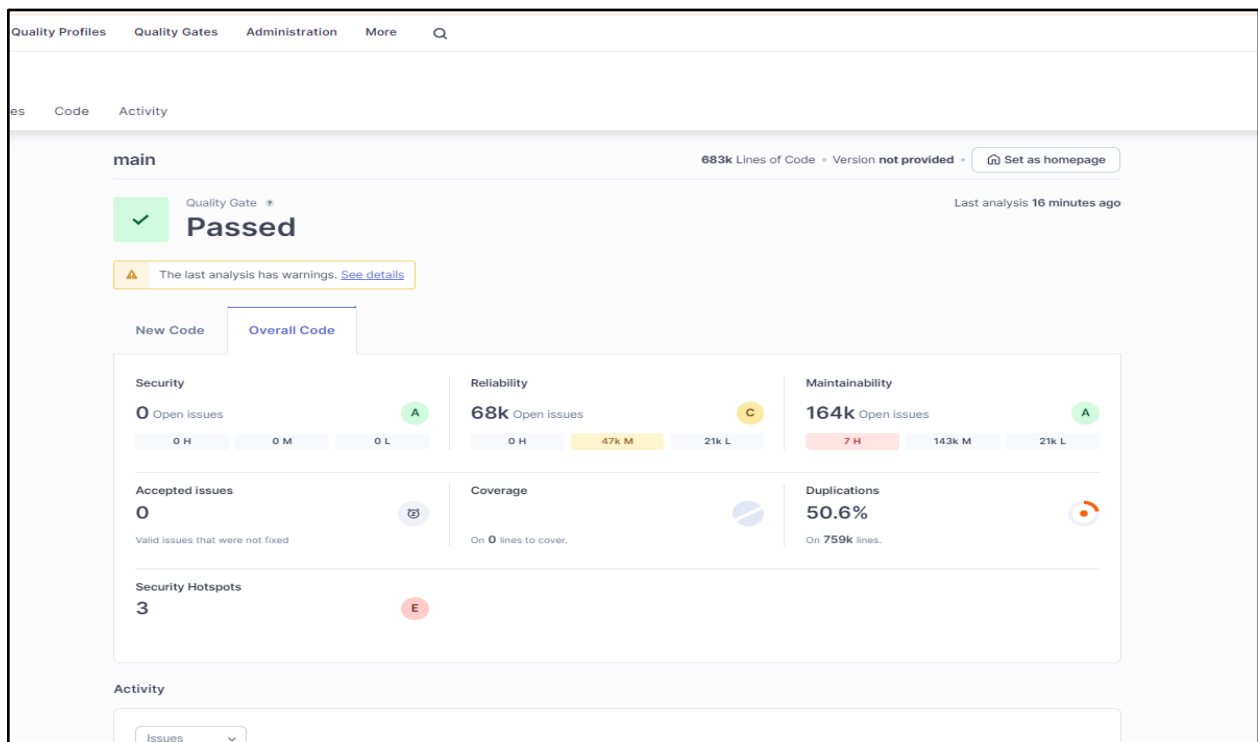
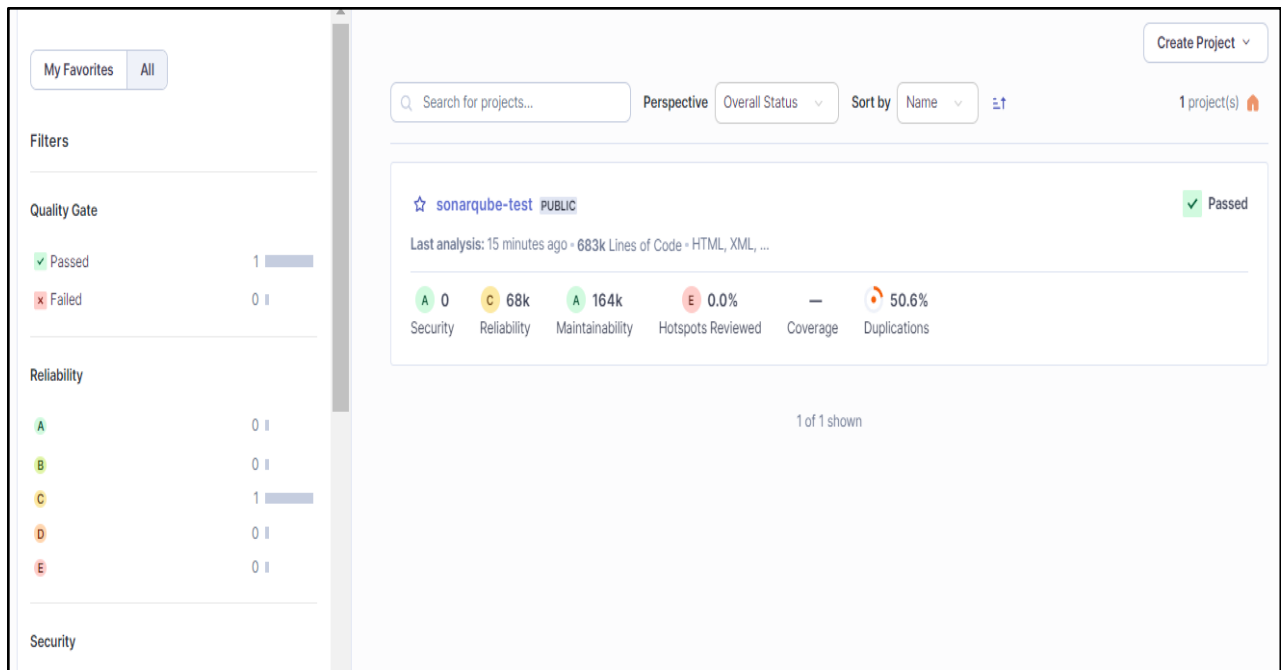
Dashboard > sonarqube-pipeline > #8

```

23:03:02.024 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/examples/testbeans/example2/package-tree.html for block at line 16. Keep only the first 100 references.
23:03:02.024 WARN Too many duplication references on file gameoflife-
web/tools/jmeter/docs/api/org/apache/jmeter/examples/testbeans/example2/package-tree.html for block at line 137. Keep only the first 100 references.
23:03:02.024 INFO CPD Executor CPD calculation finished (done) | time=196780ms
23:03:02.034 INFO SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
23:03:08.838 INFO Analysis report generated in 4613ms, dir size=127.2 MB
23:03:31.029 INFO Analysis report compressed in 22191ms, zip size=29.6 MB
23:03:32.016 INFO Analysis report uploaded in 987ms
23:03:32.018 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube-test-project-2
23:03:32.018 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
23:03:52.267 INFO Analysis total time: 10:31.289 s
23:03:52.269 INFO SonarScanner Engine completed successfully
23:03:52.972 INFO EXECUTION SUCCESS
23:03:52.972 INFO Total time: 10:37.257s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS

```

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



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

**Code Problems**

**Code issues:**

SonarQube interface showing project measures for sonarqube-test-project-2. The Measures tab is active, displaying a tree view of the project structure and a list of issues.

**Measures Summary:**

- Rating: A
- Remediation Effort: 0
- Reliability: ?
- Overview
- Overall Code
- Issues: 67624
- Rating: C
- Remediation Effort: 1426d
- Maintainability: ?

**Project Structure (Tree View):**

- sonarqube-test-project-2
  - gameoflife-acceptance-tests: 0
  - gameoflife-build: 0
  - gameoflife-core: 172
  - gameoflife-deploy: 0
  - gameoflife-web: 67452

## Consistency:

SonarQube interface showing project issues for sonarqube-test-project-2. The Issues tab is active, displaying a list of issues with filters and details.

**Filters:**

- Issues in new code
- Clean Code Attribute
  - Consistency: 197k
  - Intentionality: 14k
  - Adaptability: 0
  - Responsibility: 0
- Software Quality

**Issue Details:**

- gameoflife-acceptance-tests/Dockerfile
  - ☐ Use a specific version tag for the image. (Intentionality) No tags
  - ☐ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. (Intentionality) No tags
  - ☐ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. (Intentionality) No tags

**Warning:**

Embedded database should be used for evaluation purposes only  
The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

## Intentionally:



sonarqube

Projects Issues Rules Quality Profiles Quality Gates Administration More

sonarqube-test / main

Overview Issues Security Hotspots Measures Code Activity

Project Settings Project Information

My Issues All

Filters Clear All Filters

Issues in new code

Clean Code Attribute 1 x

Consistency 197k

Intentionality 14k

Adaptability 0

Responsibility 0

Add to selection Ctrl + click

Software Quality 1 x

Security 0

Reliability 14k

Maintainability 15

Severity

Type

Bulk Change

Select issues Navigate to issue 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:

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 x

Consistency 54k

Intentionality 14k

Adaptability 0

Responsibility 0

Add to selection Ctrl + click

Software Quality 1 x

Security 0

Reliability 14k

Maintainability 15

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

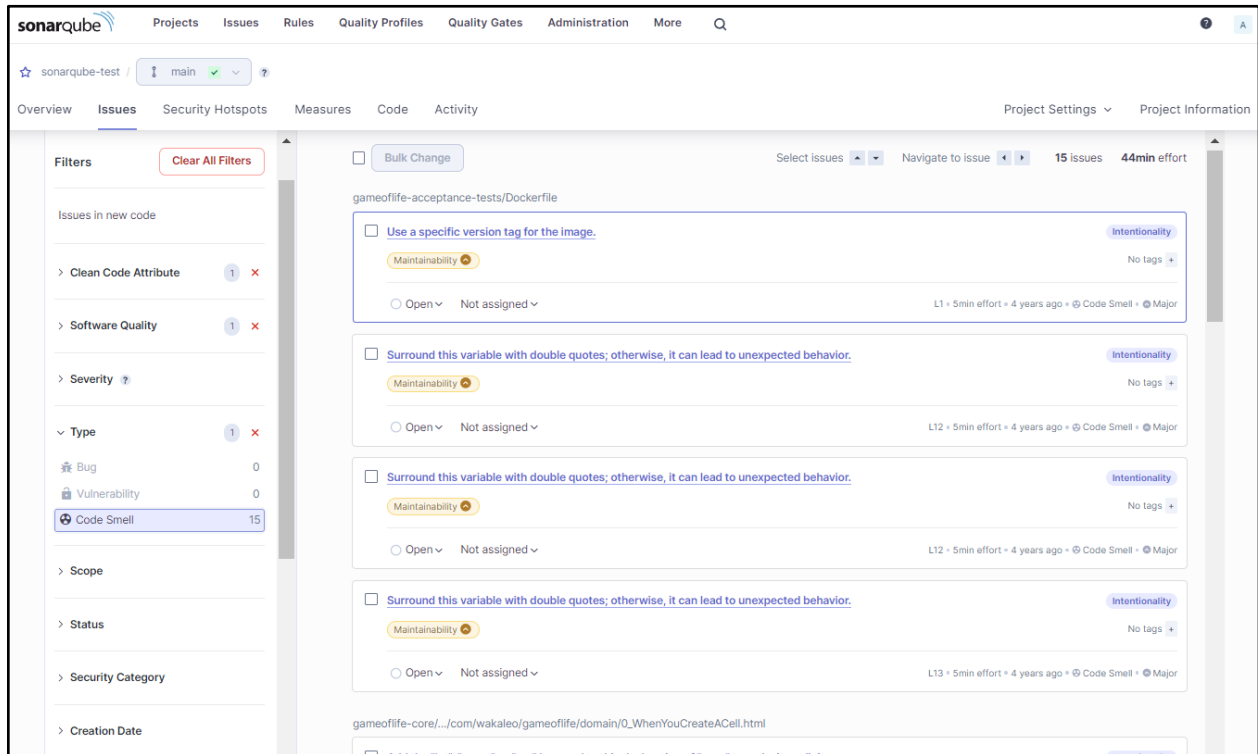
Reliability

accessibility wcag2-a

Open Not assigned

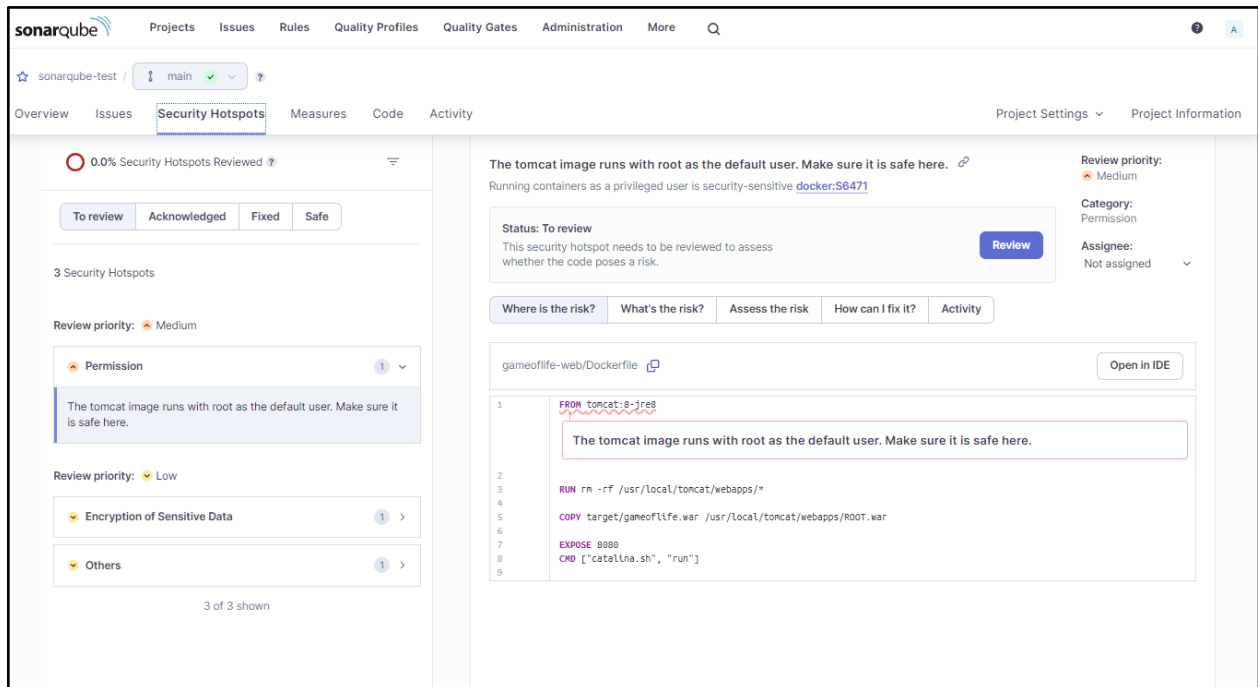
L9 • 2min effort • 4 years ago • Bug • Major

## Code smells:



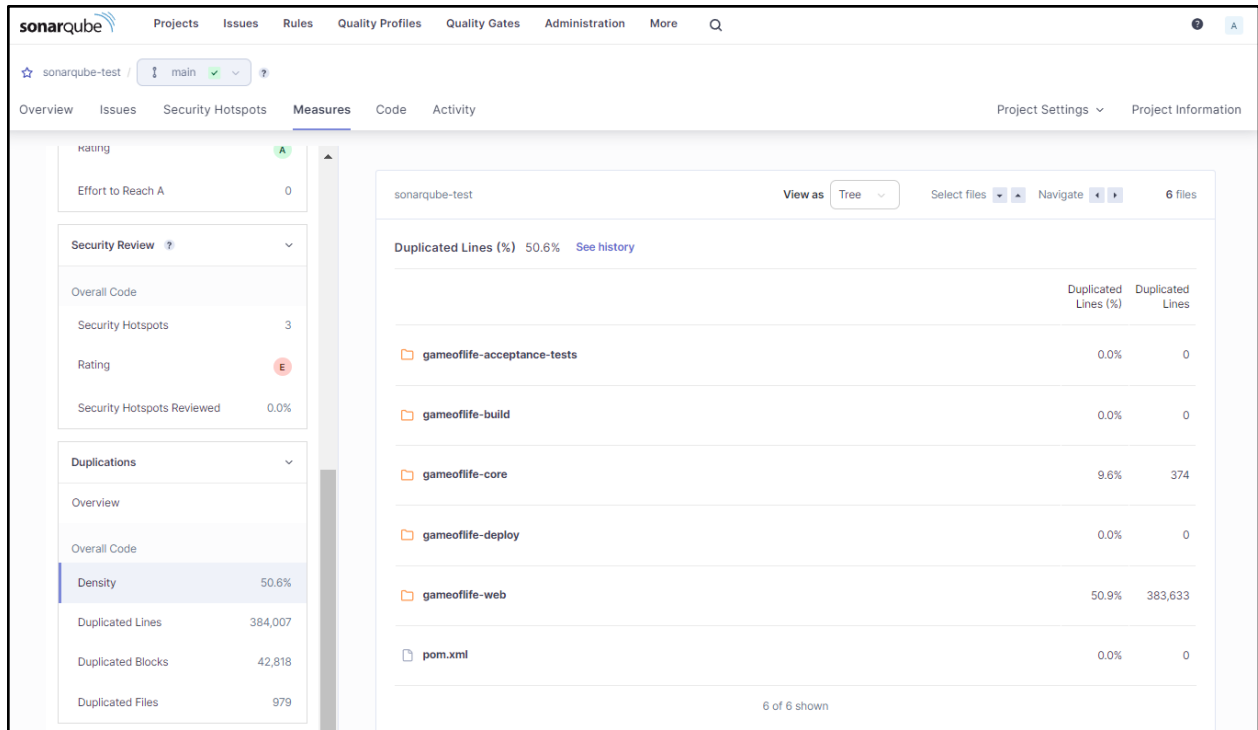
The SonarQube interface displays the 'Issues' tab for the 'sonarqube-test' project. The left sidebar shows filters for 'Issues in new code', 'Clean Code Attribute', 'Software Quality', 'Severity', 'Type' (with 'Code Smell' selected), 'Scope', 'Status', 'Security Category', and 'Creation Date'. The main area shows a list of code smells, including 'Use a specific version tag for the image' and 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior'. Each issue is marked as 'Intentionality' and 'Maintainability'.

## Security hotspot:

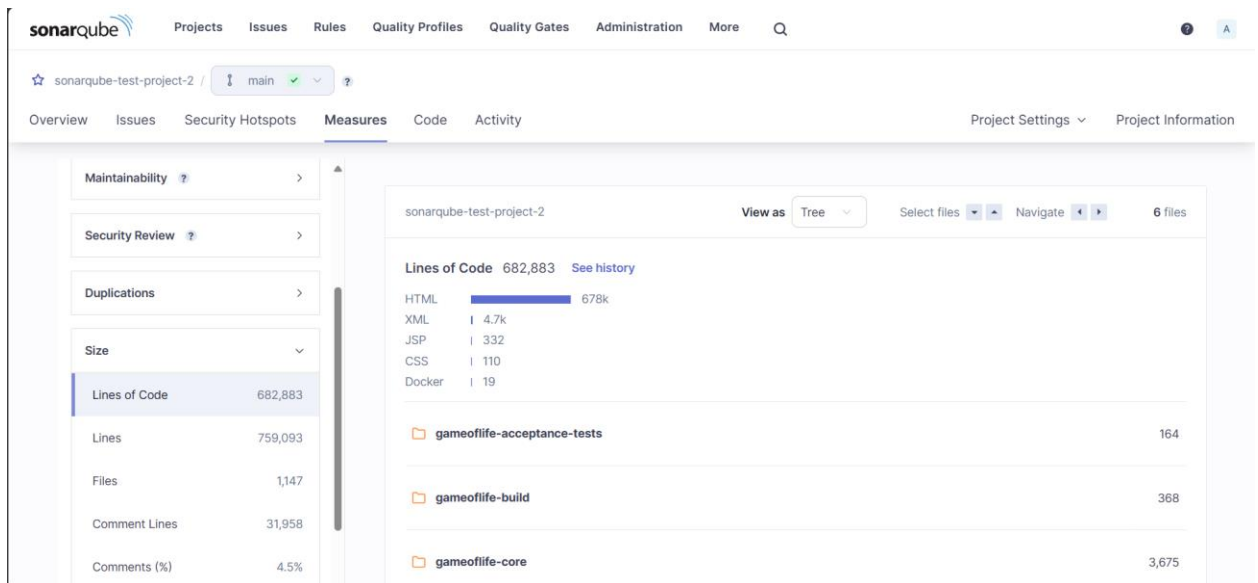


The SonarQube interface displays the 'Security Hotspots' tab for the 'sonarqube-test' project. The left sidebar shows filters for 'Security Hotspots', 'Acknowledged', 'Fixed', 'Safe', 'Review priority' (Medium), 'Permission', 'Encryption of Sensitive Data', and 'Others'. The main area shows a list of security hotspots, including 'The tomcat image runs with root as the default user. Make sure it is safe here.' The interface includes a 'Review' button and a 'Where is the risk?' tab.

## Duplicates:



## Size:



## Complexity:

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-test / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

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%

Complexity

Cyclomatic Complexity1,112

sonarqube-testView asTreeSelect filesNavigate6 files

Cyclomatic Complexity1,112See history

gameoflife-acceptance-tests

gameoflife-build

gameoflife-core18

gameoflife-deploy

gameoflife-web1,094

pom.xml

6 of 6 shown