

ADVANCE DEVOPS EXP 8

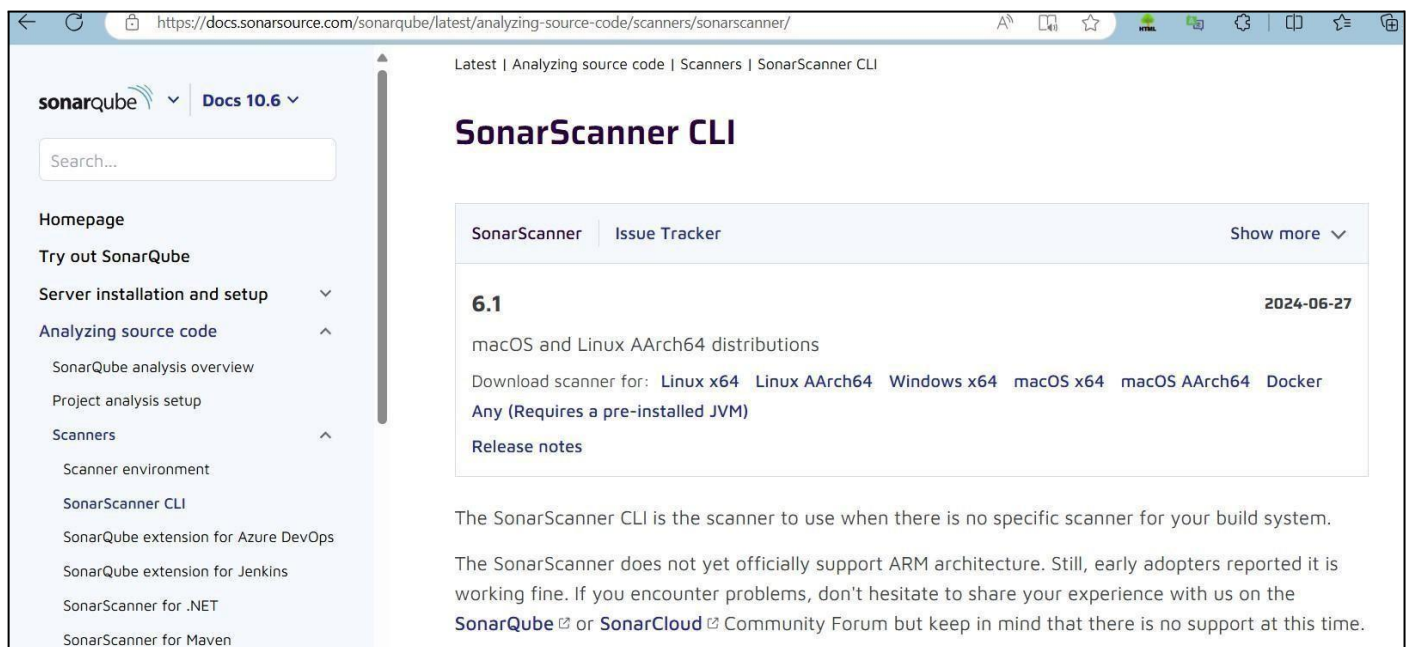
Name: Soham Satpute

Class: D15A Roll

No: 52

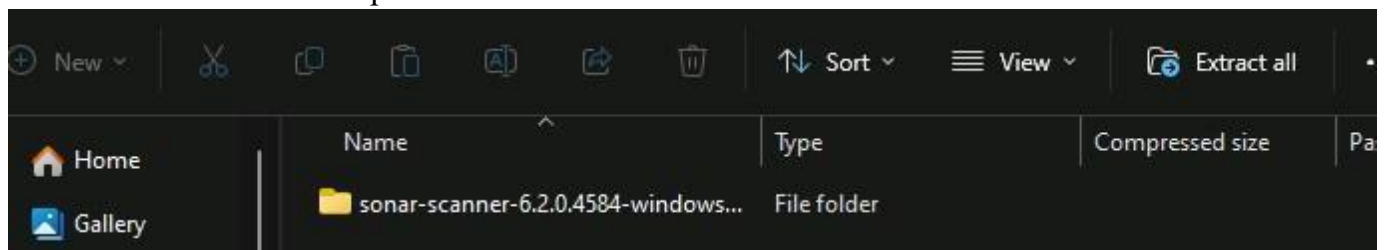
Aim: Create a Jenkins CICD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

Step 1: Download sonar scanner <https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscan>



[ner/](#) Visit this link and download the sonarqube scanner CLI.

Extract the downloaded zip file in a folder.



1. Install sonarqube image Command: **docker pull sonarqube**

Install the latest PowerShell for new features and improvements! <https://aka.ms/PSWindows>

```
PS C:\Users\Soham Satpute> docker pull sonarqube
```

```
Using default tag: latest
```

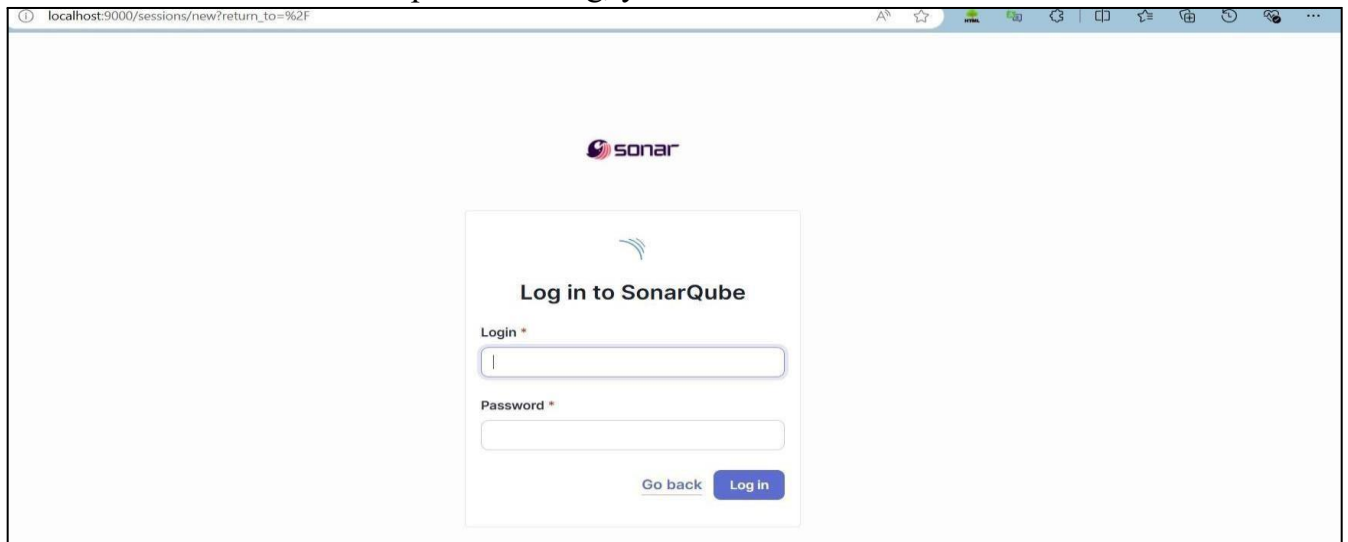
```
latest: Pulling from library/sonarqube
```

```
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
```

```
Status: Image is up to date for sonarqube:latest
```

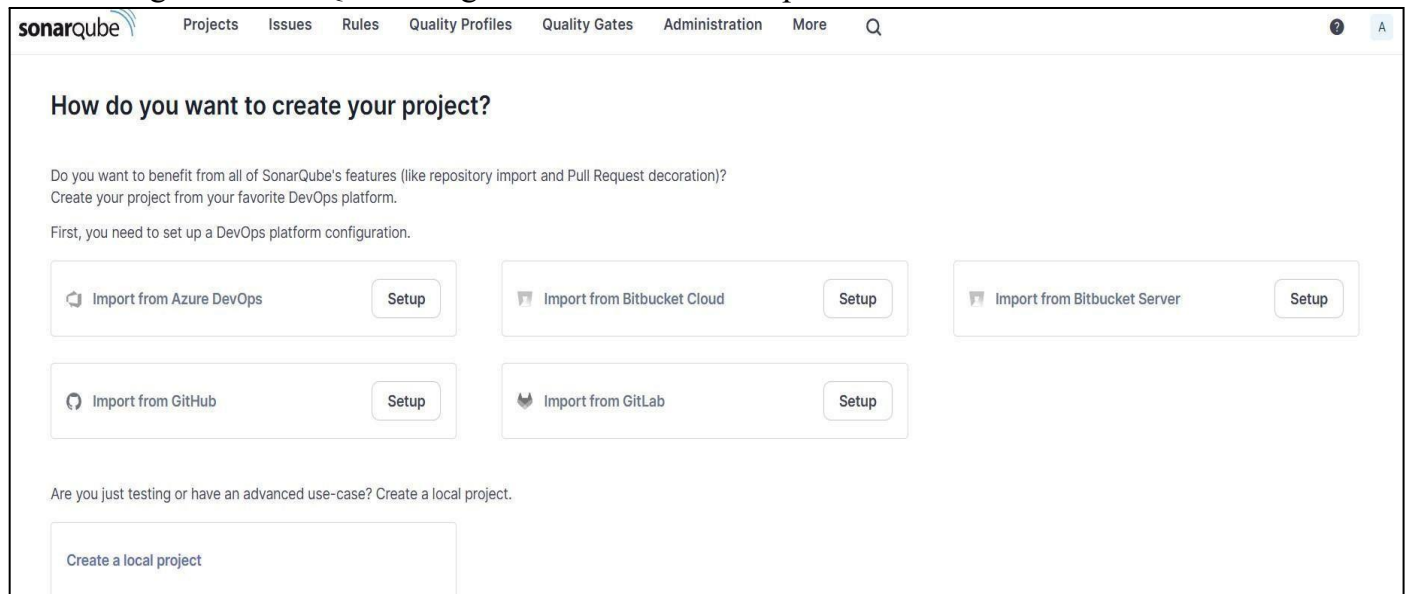
```
docker.io/library/sonarqube:latest
```

2. Once the container is up and running, you can check the status of



SonarQube at localhost port 9000.

3. Login to SonarQube using username admin and password admin.



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

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

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](#)

Cancel

Next

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 new code. 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.

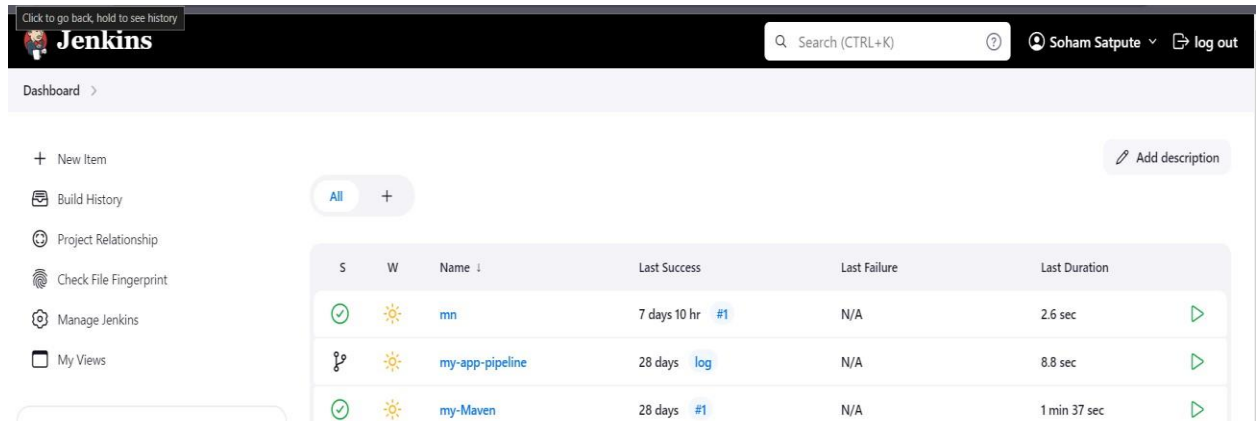
Recommended for projects following regular versions or releases.

☐ Define a specific setting for this project

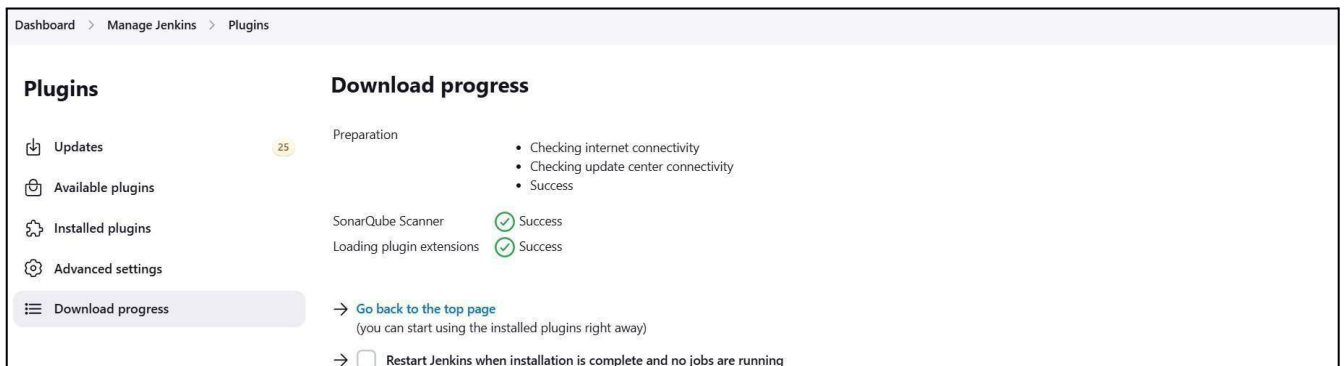
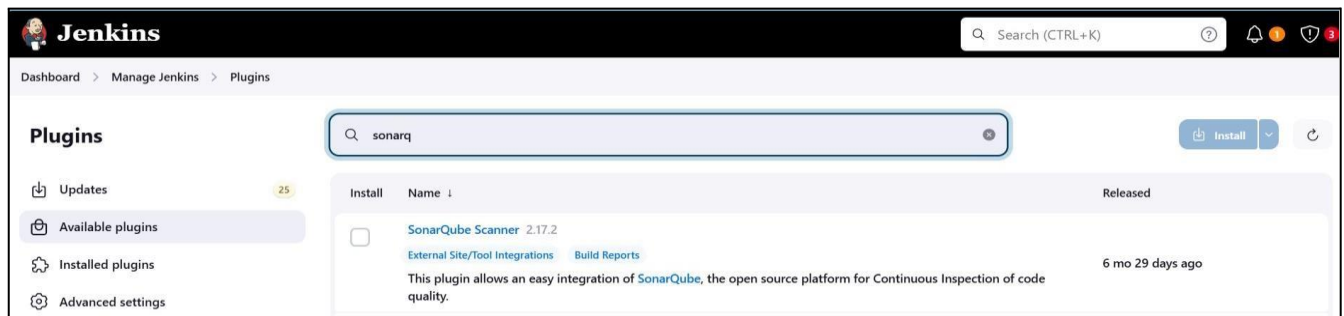
☐ Previous version

Any code that has changed since the previous version is considered new code.

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



6. Go to Manage Jenkins and search for SonarQube Scanner for Jenkins and install it.



7. Under Jenkins 'Manage Jenkins' then go to 'system', scroll and look for **SonarQube Servers** and enter the details.

Enter the Server Authentication token if needed.

In SonarQube installations: Under **Name** add <project name of sonarqube> for me **adv_devops_7_sonarqube**

In **Server URL** Default is <http://localhost:9000>

8. Search for SonarQube Scanner under Global Tool Configuration.

Name

sonarqube

Server URL

Default is http://localhost:9000

http://localhost:9000

Server authentication token

SonarQube authentication token. Mandatory when anonymous access is disabled.

- none -

+ Add

Advanced

Choose the latest configuration and choose Install automatically.

Dashboard > Manage Jenkins > Tools

Dashboard > Manage Jenkins > Tools

Add Git

Gradle installations

Add Gradle

SonarScanner for MSBuild installations

Add SonarScanner for MSBuild


SonarQube Scanner installations

Add SonarQube Scanner

Ant installations

Check the “Install automatically” option. → Under name any name as identifier → Check

Dashboard > Manage Jenkins > Tools

SonarQube Scanner installations ^  Edited

Add SonarQube Scanner

SonarQube Scanner

Name

SonarQube

☒ Install automatically ?

Install from Maven Central

Version

SonarQube Scanner 6.2.0.4584

Add Installer ▾

Add SonarQube Scanner

Save Apply

9. After configuration, create a New Item → choose a pipeline project.


Dashboard > All > New Item


New Item


Enter an item name


AdDevops-8

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.

OK

10. Under Pipeline script, enter the following:

```

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

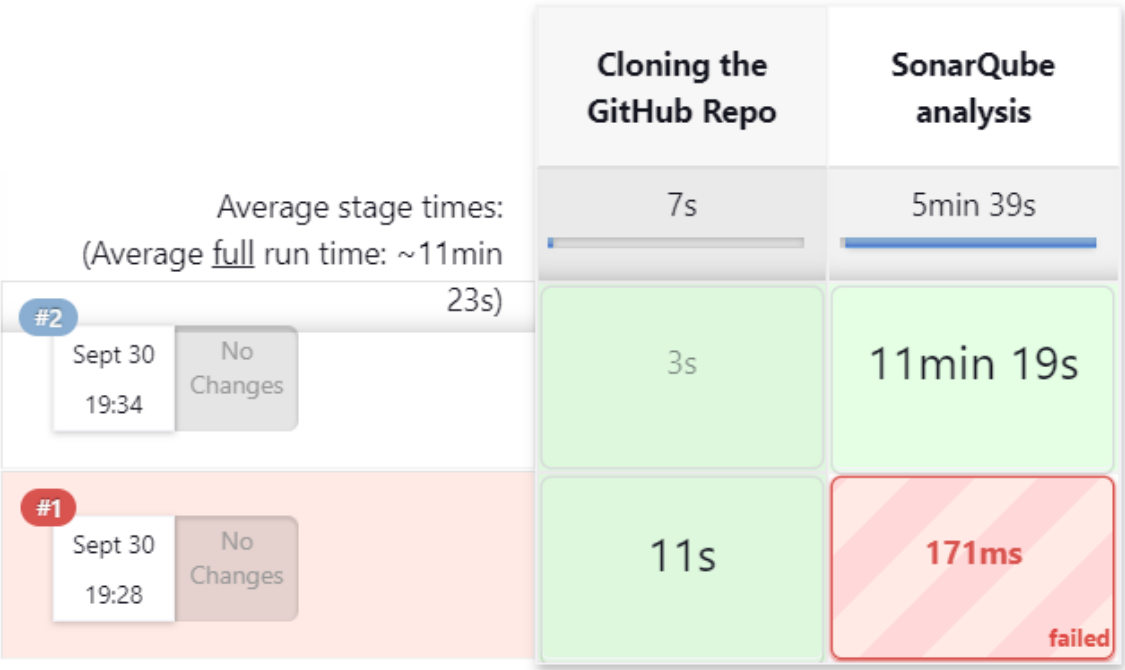
analysis') {

withSonarQubeEnv('<Name_of_SonarQube_environment_on_Jenk
ins>') { sh """
    <PATH_TO_SONARQUBE_SCANNER_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=<SonarQube_URL>(default: http://localhost:9000/)
    """
    }
}
}

```

It is a java sample project which has a lot of repetitions and issues that will be detected by SonarQube.


Stage View





Permalinks

- Last build (#1), 5 min 59 sec ago
- Last failed build (#1). 5 min 59 sec ago

11.Check console

**Jenkins**


Search (CTRL+K)


Soham Satpute   log out


Dashboard > SonarQube_pipeline > #2


Status


</> Changes


 Console Output


 Edit Build Information


 Delete build '#2'


 Timings


 Git Build Data


 Pipeline Overview




 Pipeline Console

 Replay

 Pipeline Steps

 Webpage

 Console Output

 Download  Copy  View as plain text

Skipping 4,247 KB. [Full Log](#)

```
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for block at line 145. Keep only the first 100 references.
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for block at line 506. Keep only the first 100 references.
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for block at line 759. Keep only the first 100 references.
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for block at line 705. Keep only the first 100 references.
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for block at line 659. Keep only the first 100 references.
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for block at line 511. Keep only the first 100 references.
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for block at line 578. Keep only the first 100 references.
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for block at line 707. Keep only the first 100 references.
19:43:43.934 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/gui/LineGraphGui.html for
```

12. Now, check the project in SonarQube:

The screenshot shows the SonarQube project overview for 'Sonarqube-test'. The main status is 'Passed' with a green checkmark icon. A warning message states: 'The last analysis has warnings. [See details](#)'. The 'New Code' tab is active, showing 'Overall Code' analysis. It indicates 'New Code: Since September 26, 2024 Started 4 days ago'. The 'New issues' section shows 0 issues, with a note 'Required = 0'. The 'Accepted issues' section also shows 0 issues, with a note 'Valid issues that were not fixed'. At the bottom, there are three circular progress indicators: 'Coverage' (partially filled), 'Duplications' (mostly filled), and 'Security Hotspots' (0, with a green 'A' grade).

13. code problems consistency:

The screenshot shows a list of issues in SonarQube for the project 'gameoflife-acceptance-tests/Dockerfile'. The left sidebar contains filters: 'My Issues' and 'All' tabs, and a 'Filters' section with 'Issues in new code'. Under 'Clean Code Attribute', it lists 'Consistency' (197k), 'Intentionality' (14k), 'Adaptability' (0), and 'Responsibility' (0). Under 'Software Quality', it lists 'Consistency' (197k), 'Intentionality' (14k), 'Adaptability' (0), and 'Responsibility' (0). The main area shows a list of issues. The first issue is 'Use a specific version tag for the image.' with a 'Maintainability' severity and 'Intentionality' category. The second issue is 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.' with a 'Maintainability' severity and 'Intentionality' category. The third issue is also 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.' with a 'Maintainability' severity and 'Intentionality' category. The right sidebar shows '210,549 issues' and '3135d effort'.

14.Intentionality:

The screenshot displays a software quality tool interface. On the left, a sidebar contains a 'Filters' section with a 'Clear All Filters' button. Below this, a 'Clean Code Attribute' filter is active, showing a list of attributes: Consistency (197k), Intentionality (14k), Adaptability (0), and Responsibility (0). The 'Intentionality' attribute is selected. The main area shows a list of issues. The first issue is 'Use a specific version tag for the image.' with a 'Maintainability' tag and 'Intentionality' label. The second issue is 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.' with a 'Maintainability' tag and 'Intentionality' label. The third issue is also 'Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.' with a 'Maintainability' tag and 'Intentionality' label. The interface includes a 'Bulk Change' button, 'Select issues' and 'Navigate to issue' dropdowns, and a summary of '13,887 issues' and '59d effort'.

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](#)

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 [+](#)

15.Bugs

The screenshot displays a software quality tool interface. On the left, a sidebar contains a 'Software Quality' filter section with a list of attributes: Security (0), Reliability (14k), and Maintainability (0). Below this, a 'Severity' filter is active, showing a list of types: Bug (14k), Vulnerability (0), and Code Smell (268). The 'Bug' type is selected. The main area shows a list of issues. The first issue is 'Add "lang" and/or "xml:lang" attributes to this "<html>" element' with a 'Reliability' tag and 'Intentionality' label. The second issue is 'Add "<th>" headers to this "<table>:" with a 'Reliability' tag and 'Intentionality' label. The interface includes a 'Bulk Change' button, 'Select issues' and 'Navigate to issue' dropdowns, and a summary of '13,619 issues' and '56d effort'.

Software Quality

Security 0

Reliability 14k

Maintainability 0

Severity ?

Type 1 x

Bug 14k

Vulnerability 0

Code Smell 268

Add to selection [Ctrl + click](#)

Bulk Change

Select issues [▲ ▼](#) Navigate to issue [◀ ▶](#) 13,619 issues 56d 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

Embedded database should be used for evaluation purposes only

Code smells:

Sonarqube-test / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Type1

Bug14k

Vulnerability0

Code Smell253

Add to selectionCtrl + click

Scope

Status

Security Category

gameoflife-web/tools/jmeter/printable_docs/building.html

Add an "alt" attribute to this image.

Intentionality

Reliability

accessibilitywcag2-a

OpenNot assigned

L29 • 5min effort • 4 years ago • Code Smell • Minor

gameoflife-web/tools/jmeter/printable_docs/changes.html

Add an "alt" attribute to this image.

Intentionality

Reliability

accessibilitywcag2-a

OpenNot assigned

L31 • 5min effort • 4 years ago • Code Smell • Minor

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.

SonarQube™ technology is powered by SonarSource SA

Community Edition v10.6 (92116) ACTIVE LGPL v3 Community Documentation Plugins Web API

Duplications:

Sonarqube-test / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Coverage

Duplications

Overview

New Code

Duplicated Lines0

Duplicated Blocks0

Overall Code

Density50.6%

Duplicated Lines384,007

Duplications Overview

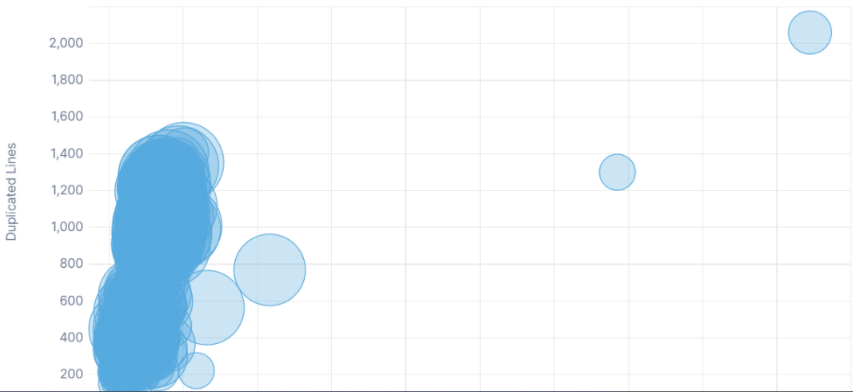
(Only showing data for the first 500 files)

See the data presented on this chart as a list

Size: Duplicated Blocks

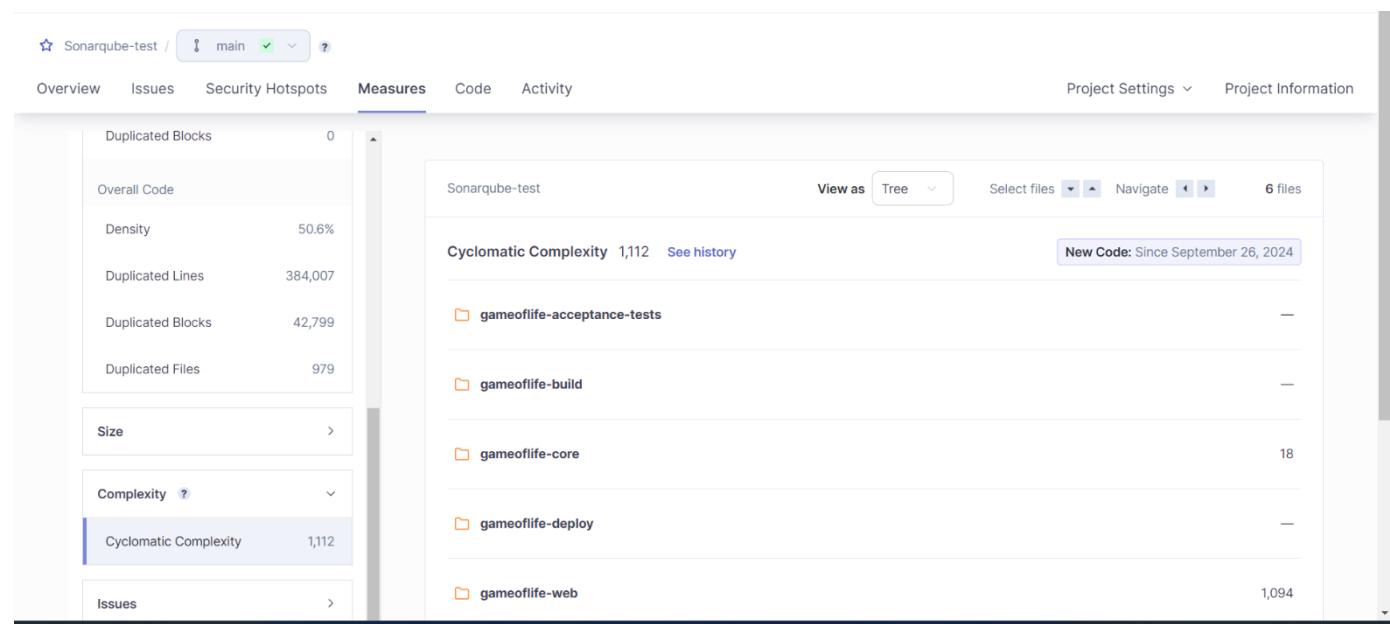
Zoom: 100%

Duplicated Lines



localhost:9000/component_measures/metric=Duplications&id=Sonarqube-test#

Cyclomatic Complexities:



In this way, we have integrated Jenkins with SonarQube for SAST.