

Name : **Himesh Pathai**

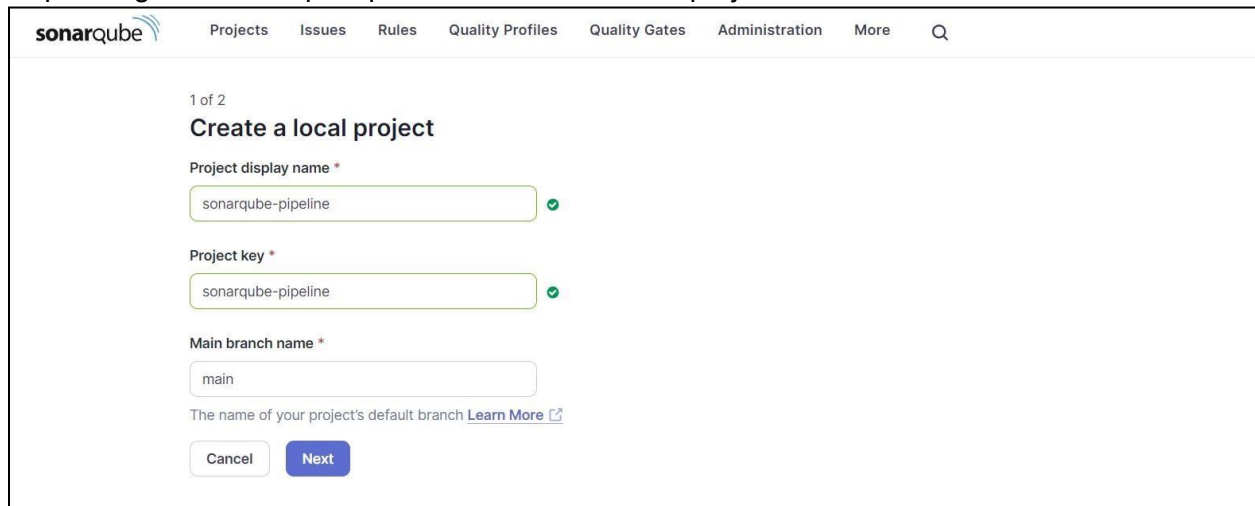
Class : **D15A**

Roll No. : **35**

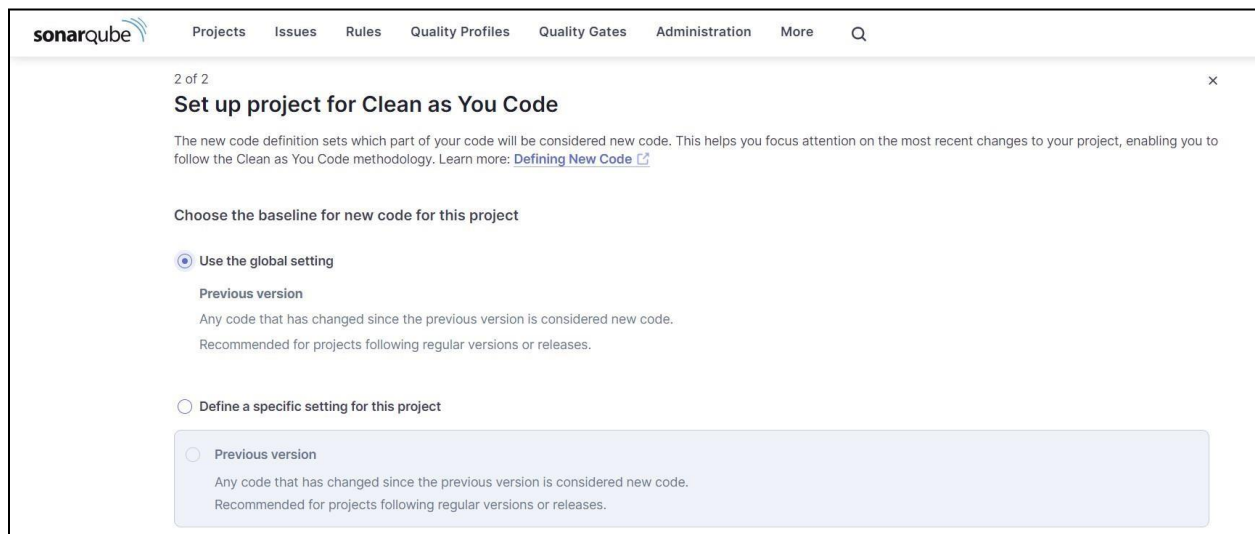
Experiment 8

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: Log in to sonarqube portal and create a local project.

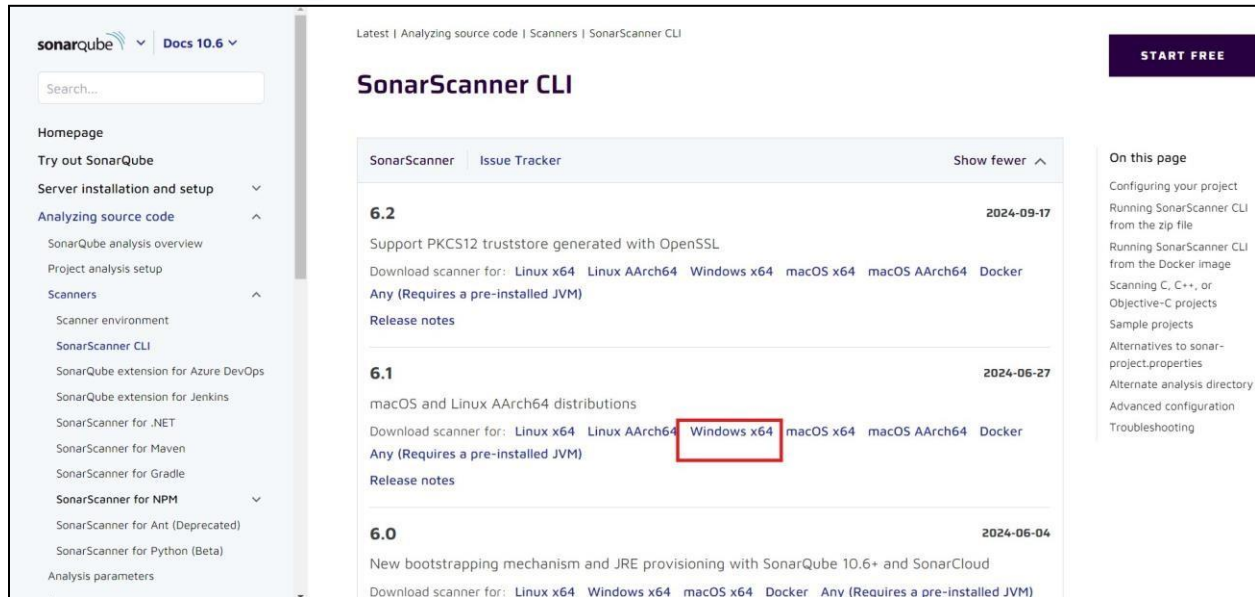


The screenshot shows the SonarQube web interface for creating a local project. The top navigation bar includes links for Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, and More, along with a search icon. The main content area is titled '1 of 2 Create a local project'. It contains three input fields: 'Project display name *' with the value 'sonarqube-pipeline', 'Project key *' with the value 'sonarqube-pipeline', and 'Main branch name *' with the value 'main'. Each field has a green checkmark icon to its right. Below the 'Main branch name' field is a link 'Learn More' with an external link icon. At the bottom are 'Cancel' and 'Next' buttons.

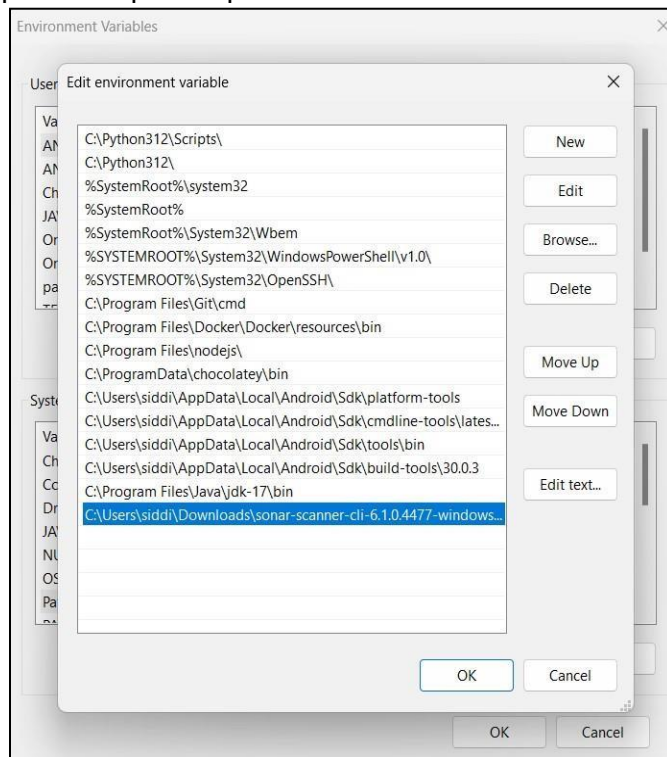


The screenshot shows the second step of the SonarQube setup, titled '2 of 2 Set up project for Clean as You Code'. It includes a close button (X) in the top right corner. A paragraph explains the 'Clean as You Code' methodology. Below this, the section 'Choose the baseline for new code for this project' has two radio button options. The first option, 'Use the global setting', is selected. Below it, the 'Previous version' option is described as 'Any code that has changed since the previous version is considered new code. Recommended for projects following regular versions or releases.' The second option, 'Define a specific setting for this project', is unselected and has a light blue background. Below it, the 'Previous version' option is also described as 'Any code that has changed since the previous version is considered new code. Recommended for projects following regular versions or releases.'

Step 2: Go to [download sonarscanner](#) to download sonar scanner



After the download is complete, extract the file and copy the path to bin folder Go to environment variables, system variables and click on path Add a new path, paste the path copied earlier.








Step 3: Create a New Item in Jenkins, choose Pipeline.

Dashboard > All > New Item

New Item

Enter an item name

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.

OK

Dashboard > sonarqube-pipeline > Configuration

Configure

- General
- Advanced Project Options
- Pipeline**

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\sliddi\Downloads\sonar-scanner-cli-6.1.0.4477-windows-x64\sonar-scanner-6.1.0.4477-windows-x64\bin\sonar-scan
9       -Dsonar.login=admin ^
10      -Dsonar.password=Mahvish ^
11      -Dsonar.projectKey=sonarqube-pipeline ^
12      -Dsonar.exclusions=vendor/**,resources/**,**/*.java ^
13      -Dsonar.host.url=http://localhost:9000/
14      ^
15     }
16   }
17 }
```

☒ Use Groovy Sandbox ?

[Pipeline Syntax](#)

Save Apply

Step 4: Save the pipeline and build it.

Dashboard > sonarqube-pipeline >

Status

</> Changes

▶ Build Now

⚙️ Configure

🗑️ Delete Pipeline

🔍 Full Stage View

🌊 SonarQube

📁 Stages

✎ Rename

❓ Pipeline Syntax

Build History

trend ▾

Filter...

#2

Sep 26, 2024, 8:42 PM

#1

Sep 26, 2024, 8:24 PM

sonarqube-pipeline

Stage View

Average stage times:
(Average full run time: ~7min 49s)

	Cloning the GitHub Repo	SonarQube analysis
#2 Sep 26 20:42 No Changes	2s	7min 46s
#1 Sep 26 20:24 No Changes	15s	1s failed

Permalinks

- Last build (#2), 9 min 1 sec ago
- Last stable build (#2), 9 min 1 sec ago
- Last successful build (#2), 9 min 1 sec ago
- Last failed build (#1), 26 min ago
- Last unsuccessful build (#1), 26 min ago
- Last completed build (#2), 9 min 1 sec ago

Console output:

Dashboard > sonarqube-pipeline > #2

Status

Console Output

Edit Build Information

Delete build '#2'

Timings

Git Build Data

Pipeline Overview

Pipeline Console

Replay

Pipeline Steps

Workspaces

Previous Build

Console Output

Download Copy View as plain text

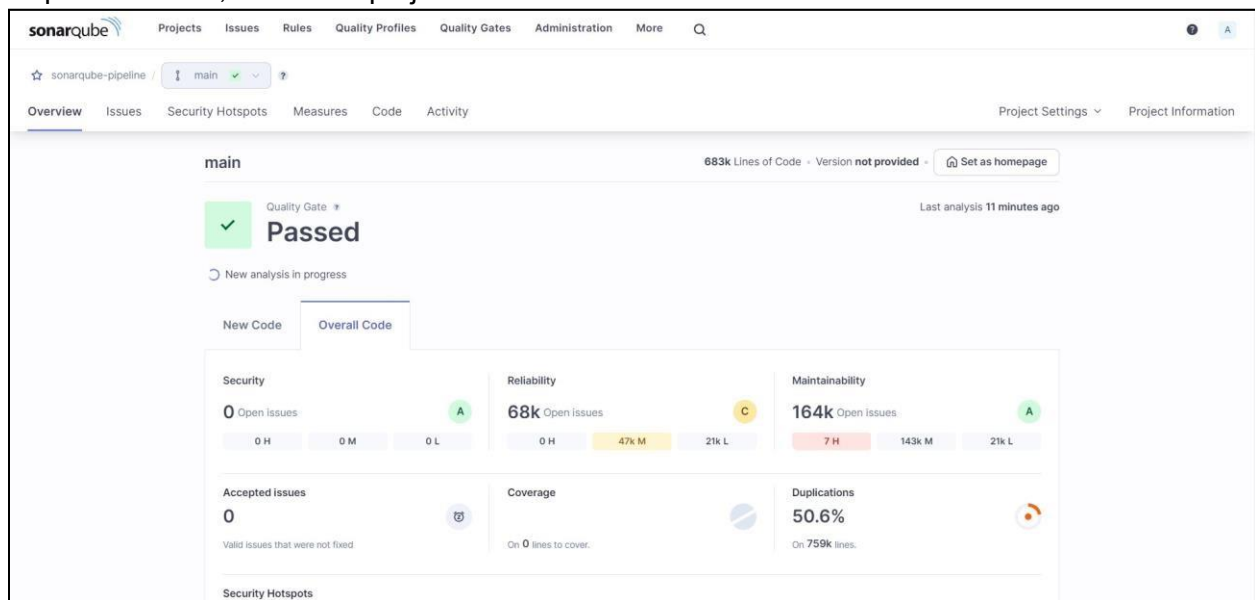
Skipping 4,248 KB. Full Log

20:49:35.711 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 40. Keep only the first 100 references.
20:49:35.712 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 65. Keep only the first 100 references.
20:49:35.712 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 41. Keep only the first 100 references.
20:49:35.712 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 17. Keep only the first 100 references.
20:49:35.712 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/GuiPackage.html for block at line 1487. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 226. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 229. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 225. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 226. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 424. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at line 17. Keep only the first 100 references.
20:49:35.812 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/functions/LongSum.html for block at

```
20:50:01.832 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube-pipeline
20:50:01.832 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
20:50:01.832 INFO More about the report processing at http://localhost:9000/api/ce/task?id=159a9d05-1f5f-4e17-bd27-3643a32a836a
20:50:12.108 INFO Analysis total time: 7:37.235 s
20:50:12.110 INFO SonarScanner Engine completed successfully
20:50:12.849 INFO EXECUTION SUCCESS
20:50:12.851 INFO Total time: 7:44.878s

[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

Step 5: After that, check the project in SonarQube



Under different tabs, check all different issues with the code.

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Reliability

Maintainability

Security Review

Duplications

Size

Complexity

Issues

Overall Code

Open Issues210,549

Confirmed Issues0

Accepted Issues0

False Positive Issues0

sonarqube-pipeline

View asTree

Select files

Navigate

6 files

Open Issues210,549See history

gameoflife-acceptance-tests4

gameoflife-build0

gameoflife-core603

gameoflife-deploy0

gameoflife-web209,940

pom.xml2

6 of 6 shown

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

My IssuesAll

Filters

Clear All Filters

Issues in new code

Clean Code Attribute

Consistency197k

Intentionality14k

Adaptability0

Responsibility0

Add to selectionCtrl + click

Software Quality

Security0

Reliability54k

Maintainability164k

Bulk Change

Select issues

Navigate to issue

196,662 issues3075d effort

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

Insert a <!DOCTYPE> declaration to before this <html> tag.

Consistency

Reliability

user-experience

OpenNot assigned

L1 - 5min effort - 4 years ago - R Bug - Major

Remove this deprecated "width" attribute.

Consistency

Maintainability

html5obsolete

OpenNot assigned

L9 - 5min effort - 4 years ago - Code Smell - Major

Remove this deprecated "align" attribute.

Consistency

Maintainability

html5obsolete

OpenNot assigned

L11 - 5min effort - 4 years ago - Code Smell - Major

Remove this deprecated "align" attribute.

Consistency

Maintainability

html5obsolete

OpenNot assigned

L11 - 5min effort - 4 years ago - Code Smell - Major

sonarqube

Projects Issues Rules Quality Profiles Quality Gates Administration More

sonarqube-pipeline / 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

Consistency 197k

Intentionality 14k

Adaptability 0

Responsibility 0

Add to selection Ctrl + click

Software Quality

Security 0

Reliability 14k

Maintainability 15

Add to selection Ctrl + click

gameoflife-acceptance-tests/Dockerfile

Use a specific version tag for the image.

Maintainability

Open Not assigned

Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.

Maintainability

Open Not assigned

Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.

Maintainability

Open Not assigned

Surround this variable with double quotes; otherwise, it can lead to unexpected behavior.

Maintainability

Open Not assigned

Introducing Clean Code Attributes

Clean Code attributes are the characteristics that your code must have to be considered Clean Code.

You can now filter by these attributes to evaluate why your code is breaking away from being clean.

1 of 5

Next

sonarqube

Projects Issues Rules Quality Profiles Quality Gates Administration More

sonarqube-pipeline / 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

Consistency 54k

Intentionality 14k

Adaptability 0

Responsibility 0

Add to selection Ctrl + click

Software Quality

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

Reliability

Open Not assigned

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

Add "lang" and/or "xml:lang" attributes to this "html" element

Reliability

Open Not assigned

Add "tbody" headers to this "table".

Reliability

Open Not assigned

Add "tbody" headers to this "table".

Reliability

Open Not assigned

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

0.0% Security Hotspots Reviewed

3 Security Hotspots

Review priority: Medium

Permission

The tomcat image runs with root as the default user. Make sure it is safe here.

Review priority: Low

Encryption of Sensitive Data

Others

3 of 3 shown

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 riskHow can I fix it?Activity

gameoflife-web/Dockerfile

Open in IDE

```
1FROM tomcat:8-jre8
2
3
4RUN rm -rf /usr/local/tomcat/webapps/*
5COPY target/gameoflife.war /usr/local/tomcat/webapps/ROOT.war
6
7EXPOSE 8080
8CMD ["catalina.sh", "run"]
9
```

The tomcat image runs with root as the default user. Make sure it is safe here.

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Reliability

Maintainability

Security Review

Duplications

Overview

Overall Code

Density50.6%

Duplicated Lines384,007

Duplicated Blocks42,808

Duplicated Files979

Size

sonarqube-pipeline

View asTree

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

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-pipeline / main

OverviewIssuesSecurity HotspotsMeasuresCodeActivity

Project SettingsProject Information

Security Review

Duplications

Overview

Overall Code

Density50.6%

Duplicated Lines384,007

Duplicated Blocks42,808

Duplicated Files979

Size

Complexity

Cyclomatic Complexity1,112

sonarqube-pipeline

View asTree

Select files

Navigate

6 files

Cyclomatic Complexity1,112

gameoflife-acceptance-tests

gameoflife-build

gameoflife-core18

gameoflife-deploy

gameoflife-web1,094

pom.xml

6 of 6 shown