

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.

Prerequisites:

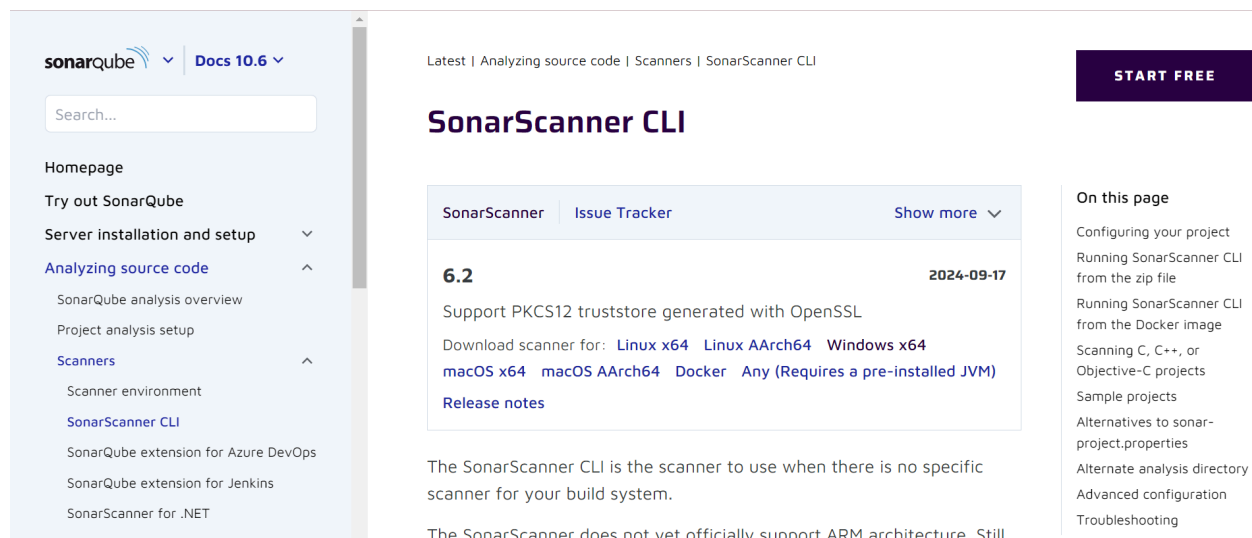
- Jenkins installed
- Docker Installed (for SonarQube)
- SonarQube Docker Image

```
C:\Users\bhumi>docker -v
Docker version 27.2.0, build 3ab4256

C:\Users\bhumi>docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
Digest: sha256:72e9feec71242af65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Image is up to date for sonarqube:latest
docker.io/library/sonarqube:latest

What's next:
View a summary of image vulnerabilities and recommendations → docker scout quickview sonarqube
```

- Download sonar scanner



The screenshot displays the SonarScanner CLI download page. The main content area shows the version 6.2, released on 2024-09-17. It provides download links for Linux x64, Linux AArch64, Windows x64, macOS x64, macOS AArch64, Docker, and Any (Requires a pre-installed JVM). The page also includes a sidebar with navigation links and a 'START FREE' button.

Extract the downloaded zip file in a folder.

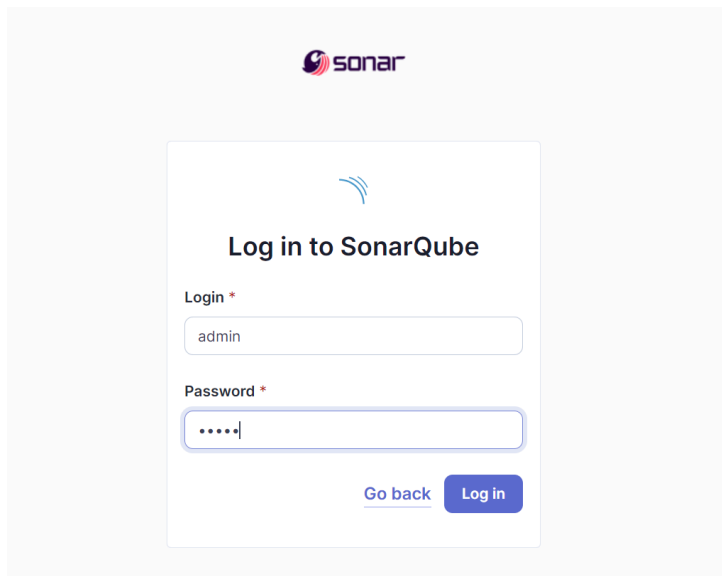
## Steps to create a Jenkins CI/CD Pipeline and use SonarQube to perform SAST

1. Run SonarQube image  
docker run -d --name sonarqube -e  
SONAR\_ES\_BOOTSTRAP\_CHECKS\_DISABLE=true -p 9000:9000  
sonarqube:latest

This command will run the SonarQube image that was just installed using docker.

```
C:\Users\bhumi>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest 7401befce9e7a7248c0e5648a2913e99c3843cce08e91d403e5af3a1479a151e
```

2. Once the SonarQube image is started, you can go to <http://localhost:9000> to find the SonarQube that has started.
3. Login to SonarQube using username admin and password admin.



The image shows the SonarQube login page. At the top is the Sonar logo. Below it is a white box with the title "Log in to SonarQube". Inside the box, there are two input fields: "Login \*" with the value "admin" and "Password \*" with masked characters "....". Below the password field are two buttons: "Go back" (a link) and "Log in" (a blue button).

4. Create a local project in SonarQube and enter a name.  
Here I have given the name 'bhumiqube' which is also the project key.

1 of 2

### Create a local project

Project display name \*

bhumiqube.



Project key \*

bhumiqube.



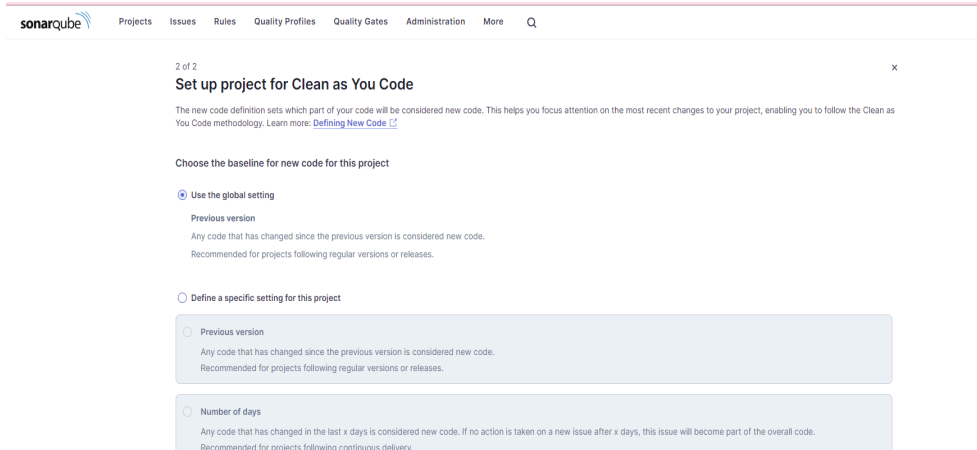
Main branch name \*

main

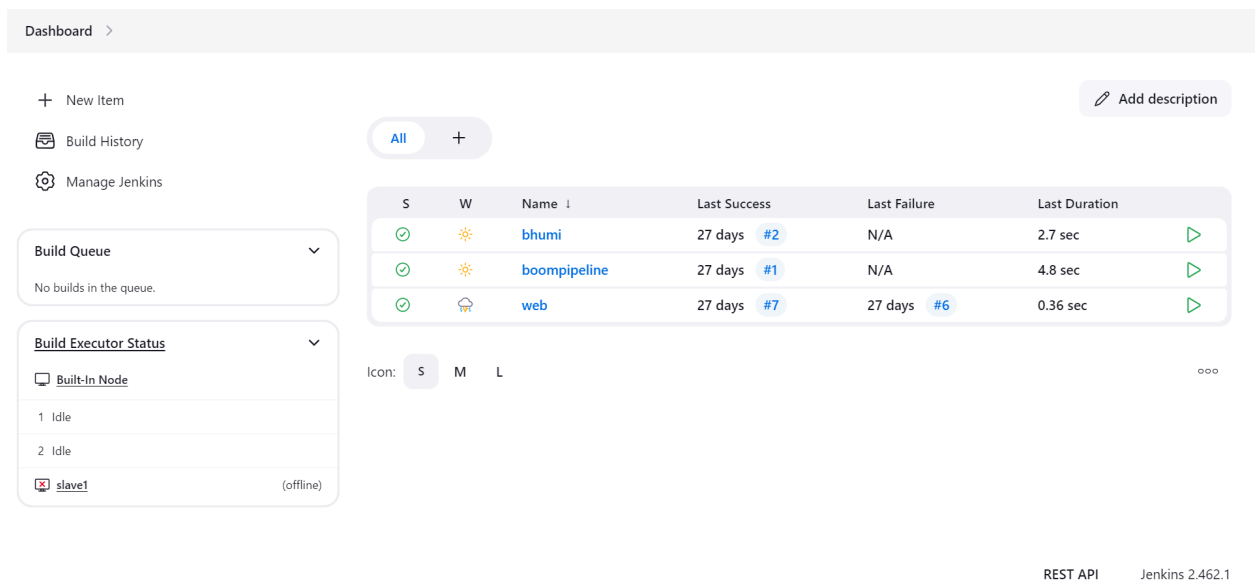
The name of your project's default branch [Learn More](#)

Cancel

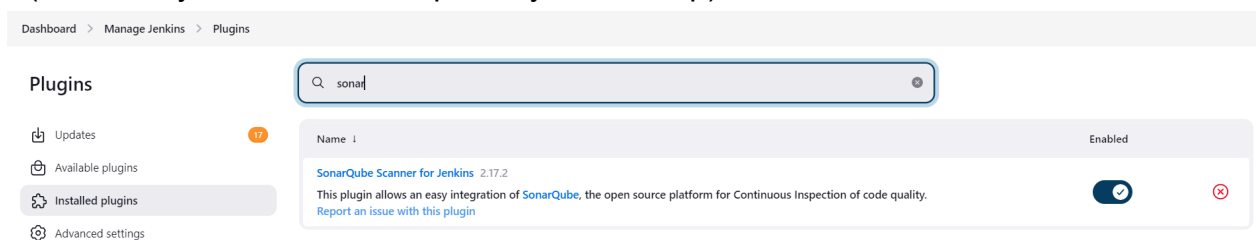
Next



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



- Go to Manage Jenkins and search for SonarQube Scanner for Jenkins and install it.(we already installed it for exp 7 so you can skip)



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

In SonarQube installations: Under Name add <project name of sonarqube> which is 'bhumiqube' for me. In Server URL Default is http://localhost:9000.

Dashboard > Manage Jenkins > System >

### SonarQube servers

If checked, job administrators will be able to inject a SonarQube server configuration as environment variables in the build.

☒ Environment variables

#### SonarQube installations

List of SonarQube installations

**Name**

**Server URL**

Default is http://localhost:9000

**Server authentication token**

SonarQube authentication token. Mandatory when anonymous access is disabled.

- none -

+ Add

Advanced

8. Search for SonarQube Scanner under Global Tool Configuration. Choose the latest configuration and choose Install automatically.

Dashboard > Manage Jenkins > Tools > SonarQube Scanner

### SonarQube Scanner installations

SonarQube Scanner installations ^ Edited

Add SonarQube Scanner

**SonarQube Scanner**

**Name**

☒ Install automatically ?

**Install from Maven Central**

**Version**

SonarQube Scanner 6.1.0.4477

Add Installer

Add SonarQube Scanner

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

1 of 2

## Create a local project

Project display name \*



Project key \*



Main branch name \*

The name of your project's default branch [Learn More](#)

Cancel

Next

10. Under Pipeline script, enter the following:

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

  stage('SonarQube analysis') {
    withSonarQubeEnv('bhumiqube'){
      bat """
      "C:\\Program
Files\\sonar-scanner\\sonar-scanner-6.2.0.4584-windows-x64\\bin\\sonar-scanner.bat" ^
        -D sonar.login=squ_19c75dfc2e1126a15d28436e4cf82fd4b8cac39a ^
        -D sonar.projectKey=bhumiqube ^
        -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.

## Pipeline

### Definition

Pipeline script

#### Script ?

```
1 node {  
2   stage('Cloning the GitHub Repo') {  
3     git 'https://github.com/shazforiot/GOL.git'  
4   }  
5  
6   stage('SonarQube analysis') {  
7     withSonarQubeEnv('bhumiqube'){  
8       bat  
9       "C:\\Program Files\\sonar-scanner\\sonar-scanner-6.2.0.4584-windows-x64\\bin\\sonar-scanner.bat" ^  
10      -D sonar.login=squ_19c75dfc2e1126a15d28436e4cf82fd4b8cac39a ^  
11      -D sonar.projectKey=bhumiqube ^  
12      -D sonar.exclusions=vendor/**,resources/**,*/.java ^  
13      -D sonar.host.url=http://localhost:9000/  
14      ^^^  
15    }  
16  }  
17 }
```

☒ Use Groovy Sandbox ?

[Pipeline Syntax](#)

Save

Apply


11. Go to the job you had just built and click on Build Now.


Dashboard > bhumiqube >


 Status

 Changes

 Build Now

 Configure

 Delete Pipeline

 SonarQube

 Stages

 Rename

 Pipeline Syntax

12. Once it is built, check the console output.

Status

</> Changes

▷ Build Now

⚙️ Configure

🗑️ Delete Pipeline

🔍 SonarQube

📁 Stages

✎️ Rename

🟢 bhumiqube

Permalinks

- [Last build \(#7\), 2 hr 48 min ago](#)
- [Last stable build \(#7\), 2 hr 48 min ago](#)
- [Last successful build \(#7\), 2 hr 48 min ago](#)
- [Last failed build \(#6\), 2 hr 52 min ago](#)
- [Last unsuccessful build \(#6\), 2 hr 52 min ago](#)
- [Last completed build \(#7\), 2 hr 48 min ago](#)

🟢 Console Output

📄 Download

📋 Copy

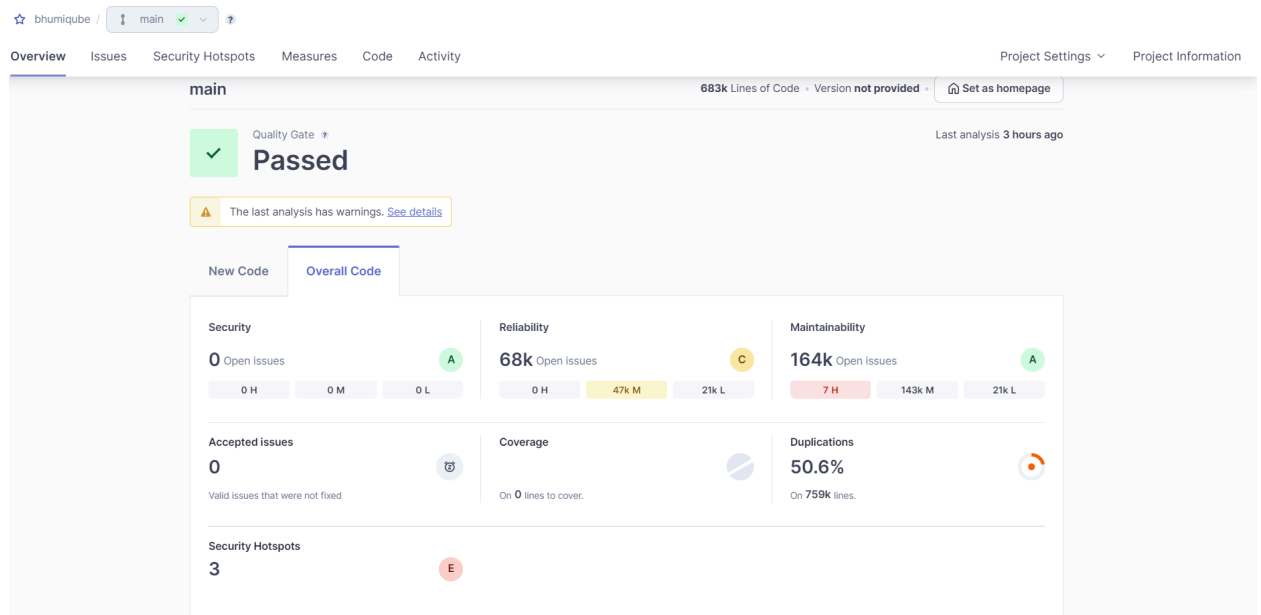
📄 View as plain text

Skipping 4.249 KB. [Full Log](#)

```
21:00:36.356 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/writers/ReportSummary.html for block at line 41. Keep only the first 100 references.
21:00:36.356 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/writers/ReportSummary.html for block at line 17. Keep only the first 100 references.
21:00:36.356 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/report/writers/ReportSummary.html for block at line 303. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 312. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 315. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 649. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 312. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 651. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 17. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 312. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 315. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 653. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 655. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 315. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 325. Keep only the first 100 references.
21:00:36.502 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 32. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 312. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 697. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 315. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 64. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 707. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 64. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 40. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 74. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 41. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 17. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 136. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 136. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 655. Keep only the first 100 references.
21:00:36.504 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jorphan/math/StatCalculator.html for block at line 74. Keep only the first 100 references.
21:00:36.526 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/package-tree.html for block at line 39. Keep only the first 100 references.
21:00:36.526 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/package-tree.html for block at line 16. Keep only the first 100 references.
21:00:36.526 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/control/gui/package-tree.html for block at line 219. Keep only the first 100
```

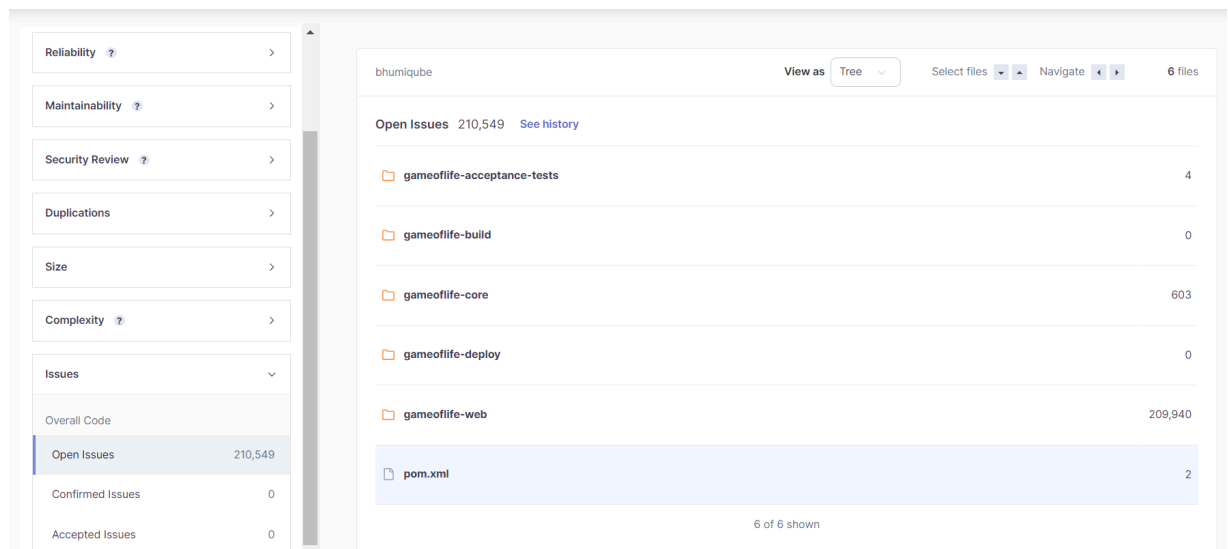
```
21:00:42.043 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/control/gui/LdapExtTestSamplerGui.html for block at line 155. Keep only the first 100 references.
21:00:42.643 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/control/gui/LdapExtTestSamplerGui.html for block at line 515. Keep only the first 100 references.
21:00:42.643 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/control/gui/LdapExtTestSamplerGui.html for block at line 768. Keep only the first 100 references.
21:00:42.643 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/control/gui/LdapExtTestSamplerGui.html for block at line 714. Keep only the first 100 references.
21:00:42.643 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/ldap/control/gui/LdapExtTestSamplerGui.html for block at line 668. Keep only the first 100 references.
21:00:42.643 INFO CPD Executor CPD calculation finished (done) | time=187786ms
21:00:42.660 INFO SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
21:02:50.519 INFO Analysis report generated in 5916ms, dir size=127.2 MB
21:03:11.285 INFO Analysis report compressed in 20750ms, zip size=29.6 MB
21:03:11.715 INFO Analysis report uploaded in 430ms
21:03:11.717 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=bhumiqube
21:03:11.717 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
21:03:11.717 INFO More about the report processing at http://localhost:9000/api/ce/task?id=2bf5a9f3-919a-4725-94d5-474d4773e610
21:03:26.163 INFO Analysis total time: 16:37.760 s
21:03:26.163 INFO SonarScanner Engine completed successfully
21:03:26.916 INFO EXECUTION SUCCESS
21:03:26.916 INFO Total time: 16:42.318s
[Pipeline] }
[Pipeline] // withSonarQubeEnv
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // node
[Pipeline] End of Pipeline
Finished: SUCCESS
```

13. Once the build is complete, go back to SonarQube and check the project linked.



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

- Code Problems





## Consistency

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

Security	0
Reliability	54k
Maintainability	164k

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

☐ Bulk Change Select Issues Navigate to issue 196,662 issues 3075d effort

☐ Insert a `<!DOCTYPE>` declaration to before this `<html>` tag. Consistency Reliability user-experience L1 • 5min effort • 4 years ago • Bug • Major

☐ Remove this deprecated "width" attribute. Consistency Maintainability html5 obsolete L9 • 5min effort • 4 years ago • Code Smell • Major

☐ Remove this deprecated "align" attribute. Consistency Maintainability html5 obsolete L11 • 5min effort • 4 years ago • Code Smell • Major

☐ Remove this deprecated "align" attribute. Consistency Maintainability html5 obsolete

## Intentionality

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

Security	0
Reliability	14k
Maintainability	15

gameoflife-acceptance-tests/Dockerfile

☐ Bulk Change Select Issues Navigate to issue 13,887 issues 59d effort

☐ 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

☐ Surround this variable with double quotes; otherwise, it can lead to unexpected behavior. Intentionality Maintainability No tags

## • Bugs

☆ bhumique / ⓘ main ✓ ?

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

▼ Software Quality

Security 0

Reliability 14k

Maintainability 0

> Severity ?

▼ Type 1 ✕

🔍 Bug 14k

🔒 Vulnerability 0

🐛 Code Smell 268

Add to selection **Ctrl + click**

> Scope

> Status

> Security Category

☐ 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

gameoflife-core/build/reports/tests/allclasses-frame.html

☐ 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

## • Code Smells

☆ bhumique / ⓘ main ✓ ?

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

▼ Software Quality

Security 0

Reliability 253

Maintainability 15

> Severity ?

▼ Type 1 ✕

🔍 Bug 14k

🔒 Vulnerability 0

🐛 Code Smell 268

Add to selection **Ctrl + click**

> Scope

> Status

> Security Category

☐ Bulk Change

Select Issues ▾

Navigate to Issue ▾

268 issues

2d 5h 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

gameoflife-acceptance-tests/Dockerfile

☐ 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

gameoflife-acceptance-tests/Dockerfile

☐ 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

gameoflife-acceptance-tests/Dockerfile

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

Intentionality

Maintainability

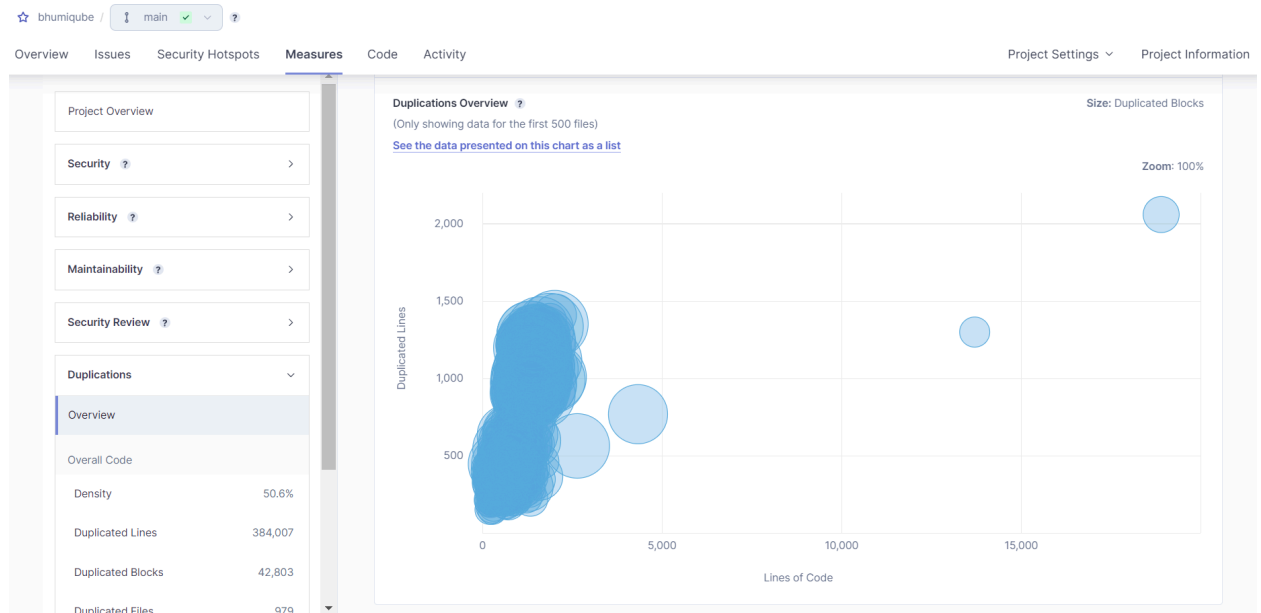
No tags ▾

Open ▾ Not assigned ▾

L12 • 5min effort • 4 years ago • 🟡 Code Smell • 🟡 Major

⚠ Embedded database should be used for evaluation purposes only

## • Duplications



### Conclusion:

In this experiment, we successfully integrated Jenkins with SonarQube to automate continuous monitoring of code quality within our CI/CD pipeline. The process involved deploying SonarQube using Docker, setting up a project for code analysis, and configuring Jenkins with the SonarQube Scanner plugin. After configuring the tools and providing the SonarQube server details, we developed a Jenkins pipeline that automatically clones code from GitHub and runs static analysis. This integration helps us identify bugs, code smells, and security vulnerabilities throughout the development process, ensuring better code quality and smoother development workflows.