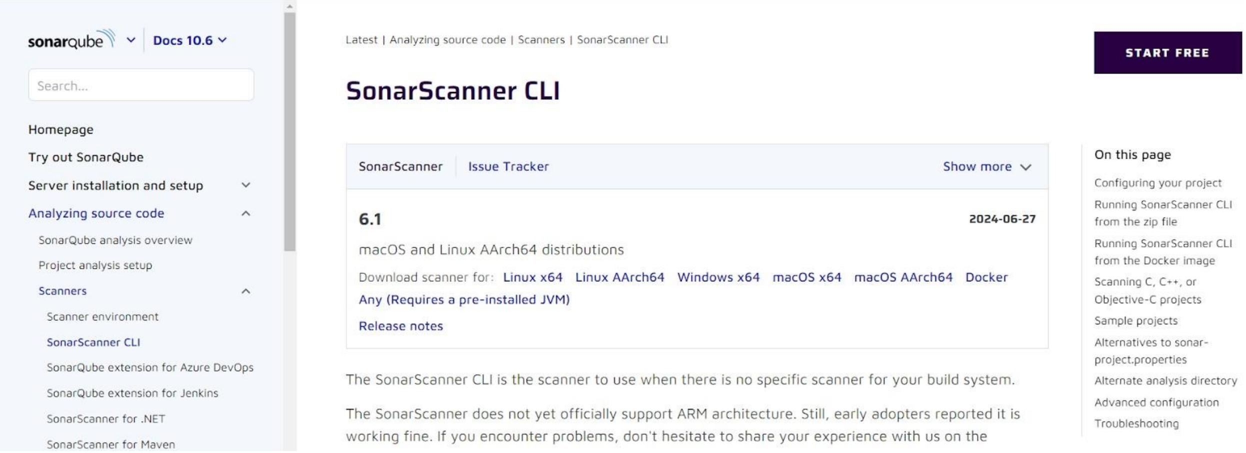
Name:Sahil Ramrakhyani Roll No:42 Div:D15C

Exp: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: Download sonar scanner

https://docs.sonarsource.com/sonarqube/latest/analyzing-source-code/scanners/sonarscanner/


sonarqube
Docs 10.6
Search...
Homepage
Try out SonarQube
Server installation and setup
Analyzing source code
SonarQube analysis overview
Project analysis setup
Scanners
Scanner environment
SonarScanner CLI
SonarQube extension for Azure DevOps
SonarQube extension for Jenkins
SonarScanner for .NET
SonarScanner for Maven
START FREE
On this page
Configuring your project
Running SonarScanner CLI from the zip file
Running SonarScanner CLI from the Docker image
Scanning C, C++, or Objective-C projects
Sample projects
Alternatives to sonar-project.properties
Alternate analysis directory
Advanced configuration
Troubleshooting

Latest | Analyzing source code | Scanners | SonarScanner CLI

SonarScanner CLI

SonarScanner | Issue Tracker | Show more

6.1 2024-06-27

macOS and Linux AArch64 distributions

Download scanner for: Linux x64 Linux AArch64 Windows x64 macOS x64 macOS AArch64 Docker Any (Requires a pre-installed JVM)

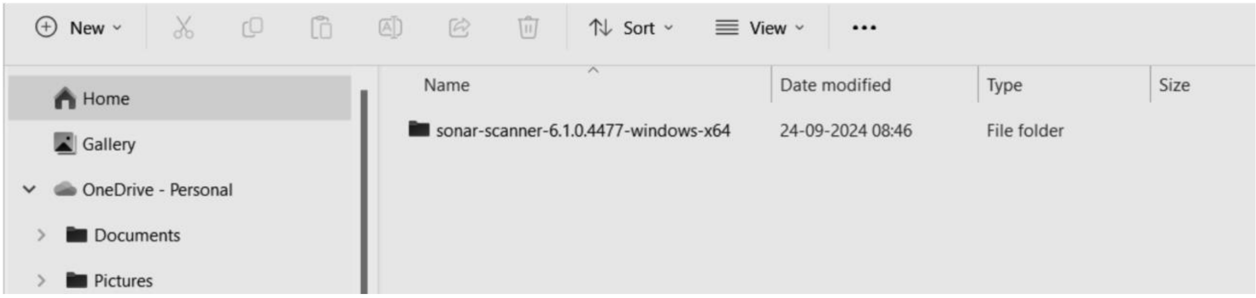
Release notes

The SonarScanner CLI is the scanner to use when there is no specific scanner for your build system.

The SonarScanner does not yet officially support ARM architecture. Still, early adopters reported it is working fine. If you encounter problems, don't hesitate to share your experience with us on the

Visit this link and download the sonarqube scanner CLI.

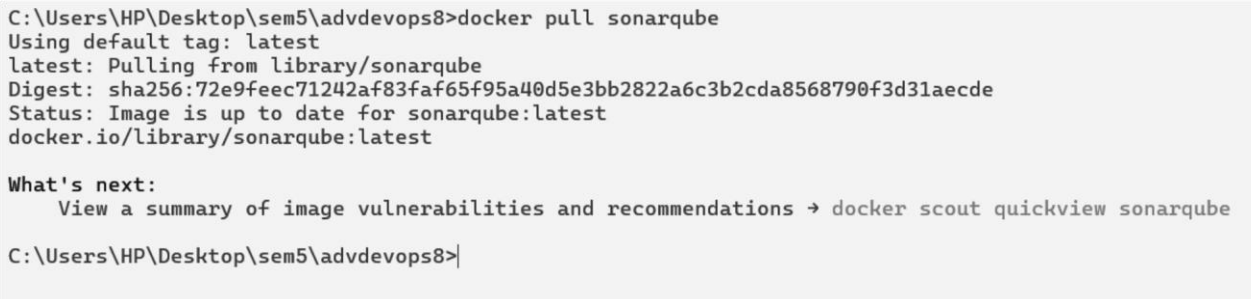
Extract the downloaded zip file in a folder.



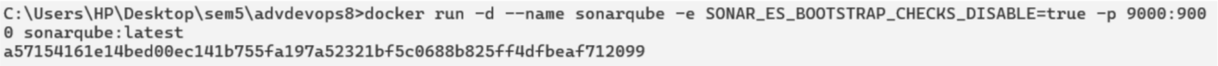
Name	Date modified	Type	Size
sonar-scanner-6.1.0.4477-windows-x64	24-09-2024 08:46	File folder	

1. Install sonarqube image

Command: docker pull sonarqube



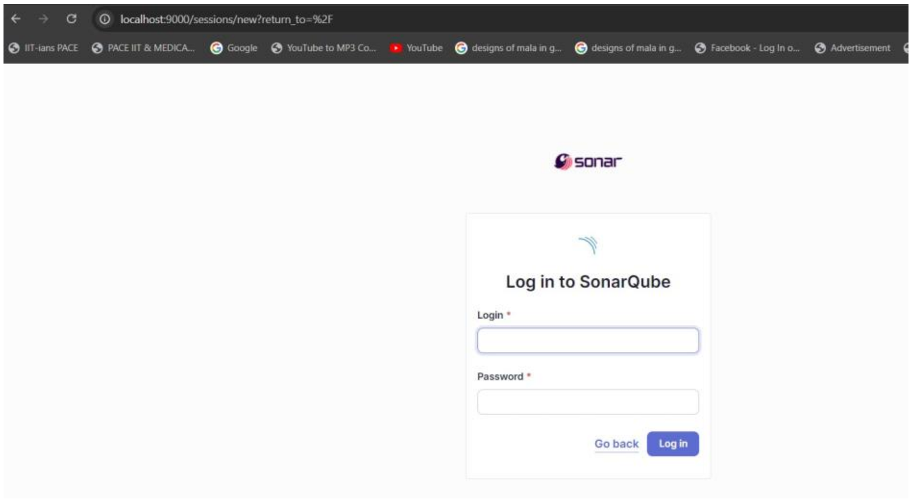
```
C:\Users\HP\Desktop\sem5\advdevops8>docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Image is up to date for sonarqube:latest
docker.io/library/sonarqube:latest

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

C:\Users\HP\Desktop\sem5\advdevops8>
```



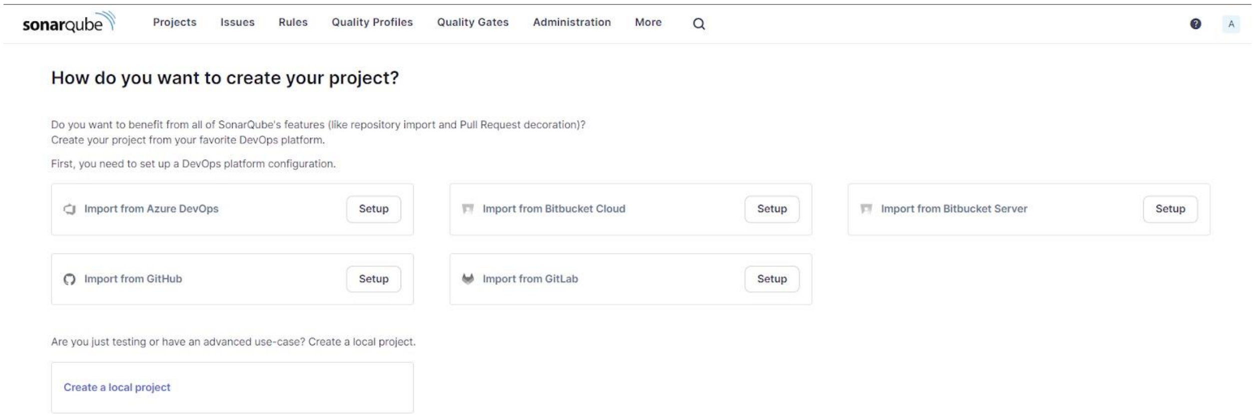
```
C:\Users\HP\Desktop\sem5\advdevops8>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:900
0 sonarqube:latest
a57154161e14bed00ec141b755fa197a52321bf5c0688b825ff4dfbeaf712099
```

Name:Sahil Ramrakhyani Roll No:42 Div:D15C

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.



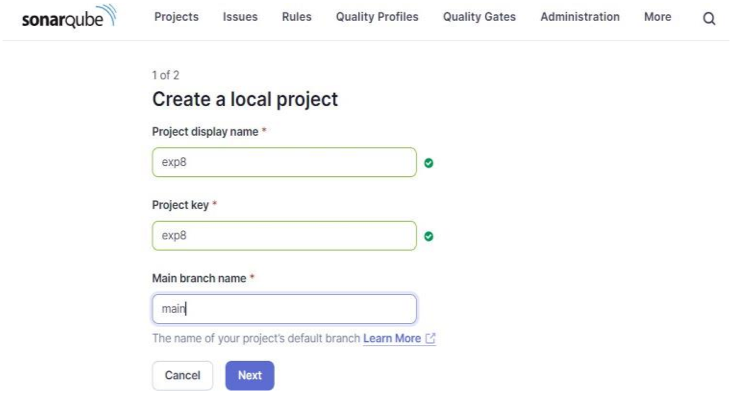
How do you want to create your project?

Do you want to benefit from all of SonarQube's features (like repository import and Pull Request decoration)?
Create your project from your favorite DevOps platform.

First, you need to set up a DevOps platform configuration.

Are you just testing or have an advanced use-case? Create a local project.

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



1 of 2

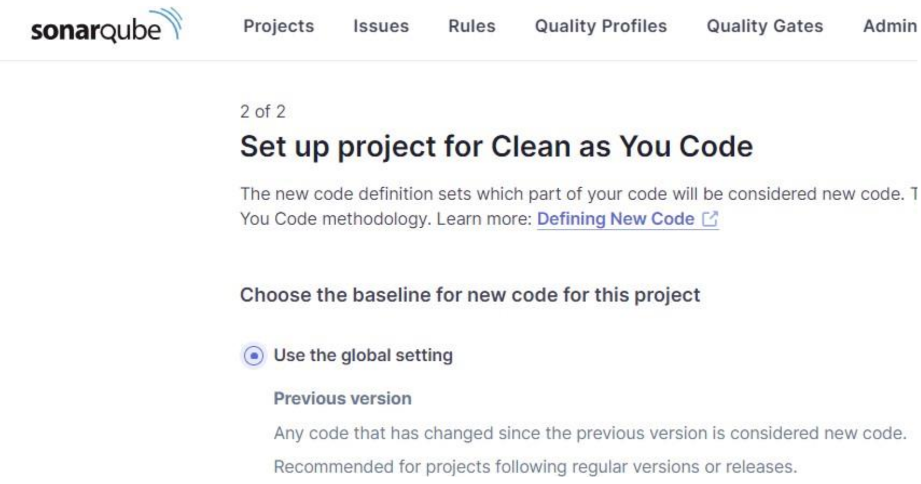
Create a local project

Project display name *: exp8

Project key *: exp8

Main branch name *: main

The name of your project's default branch Learn More



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. T
You Code methodology. Learn more: Defining New Code

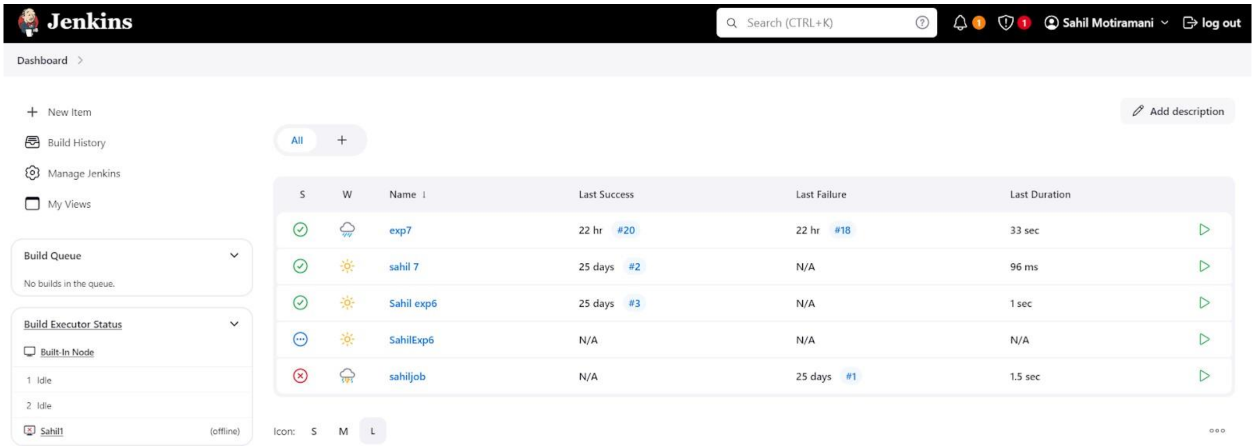
Choose the baseline for new code for this project

● Use the global setting

Previous version

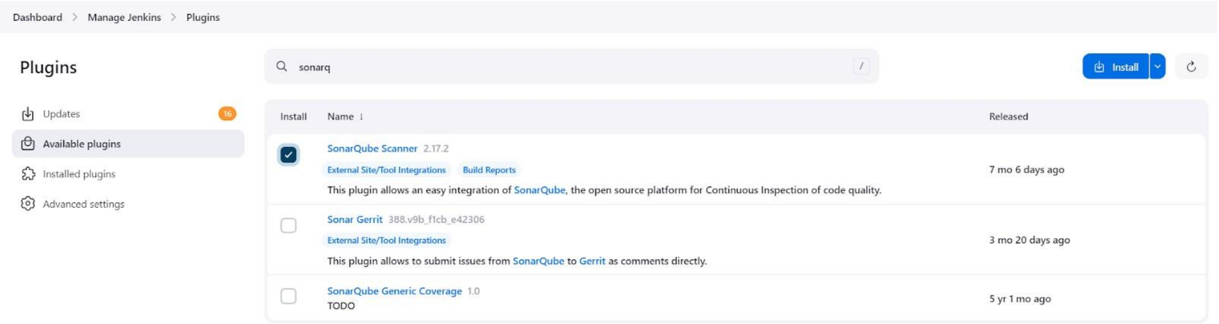
Any code that has changed since the previous version is considered new code.
Recommended for projects following regular versions or releases.

5. Open up Jenkins Dashboard on localhost, port 8090 or whichever port it is at for you.



S	W	Name ↓	Last Success	Last Failure	Last Duration
✓		exp7	22 hr #20	22 hr #18	33 sec
✓		sahil 7	25 days #2	N/A	96 ms
✓		Sahil exp6	25 days #3	N/A	1 sec
⋯		SahilExp6	N/A	N/A	N/A
☒		sahiljob	N/A	25 days #1	1.5 sec

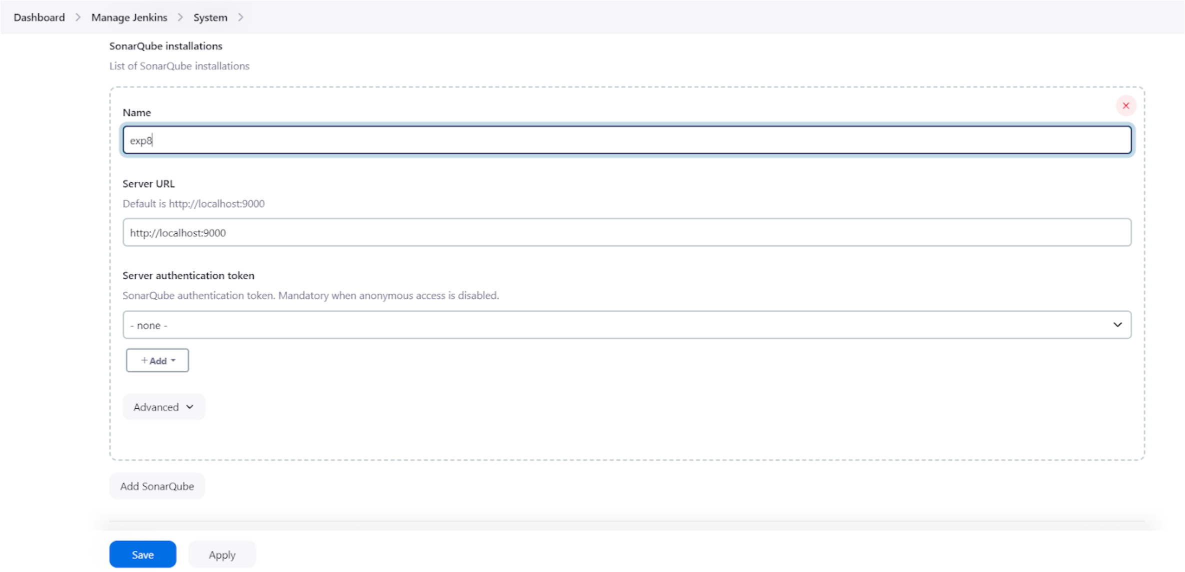
6. Go to Manage Jenkins and search for SonarQube Scanner for Jenkins and install it.



Install	Name ↓	Released
☑	SonarQube Scanner 2.17.2 External Site/Tool Integrations Build Reports This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.	7 mo 6 days ago
□	Sonar Gerrit 388.v9b_f1cb_e42306 External Site/Tool Integrations This plugin allows to submit issues from SonarQube to Gerrit as comments directly.	3 mo 20 days ago
□	SonarQube Generic Coverage 1.0 TODO	5 yr 1 mo ago

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



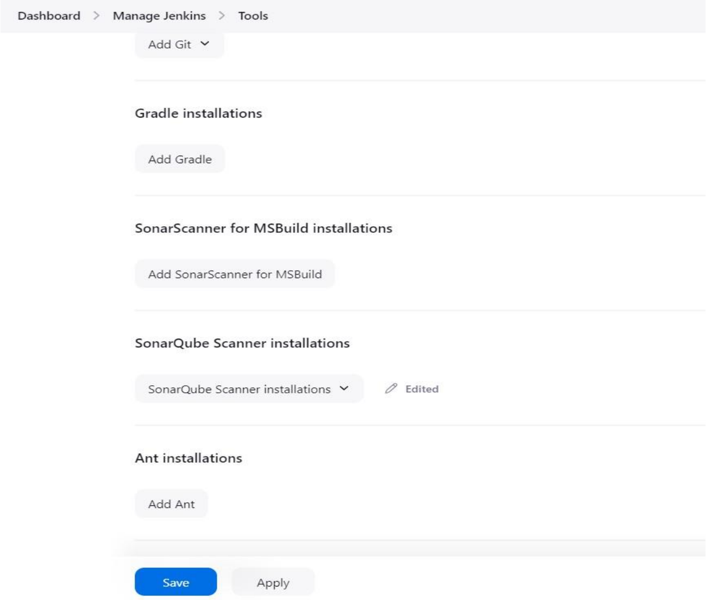
SonarQube installations
List of SonarQube installations

Name
exp8

Server URL
Default is http://localhost:9000
http://localhost:9000

Server authentication token
SonarQube authentication token. Mandatory when anonymous access is disabled.
- none -

8. Search for SonarQube Scanner under Global Tool Configuration. Choose the latest configuration and choose Install automatically.
Dashboard > Manage Jenkins > Tools


Dashboard > Manage Jenkins > Tools
Add Git
Add Gradle
Add SonarScanner for MSBuild
SonarQube Scanner installations
Edited
Add Ant
Save
Apply

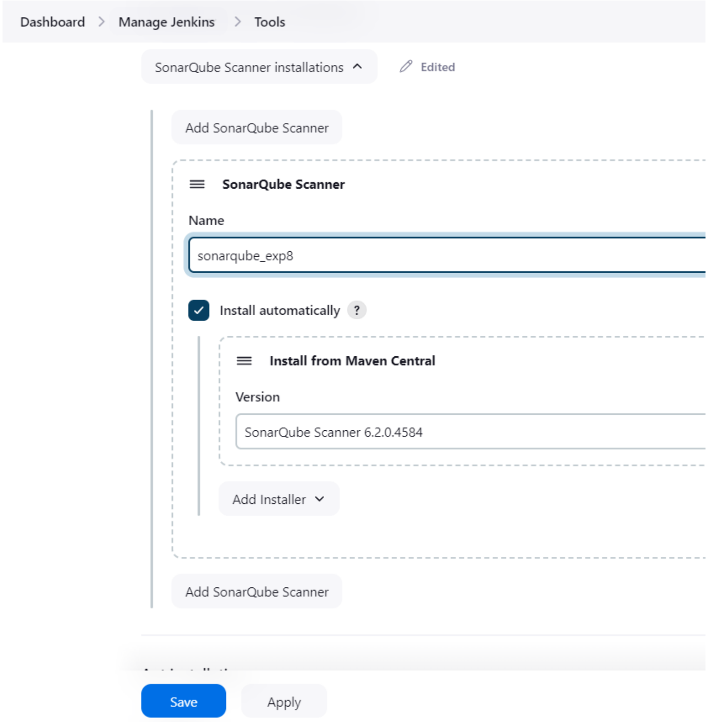
Gradle installations

SonarScanner for MSBuild installations

SonarQube Scanner installations

Ant installations

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



Dashboard > Manage Jenkins > Tools

SonarQube Scanner installations ^ Edited

Add SonarQube Scanner

SonarQube Scanner

Name: sonarqube_exp8

☑ Install automatically ?

Install from Maven Central

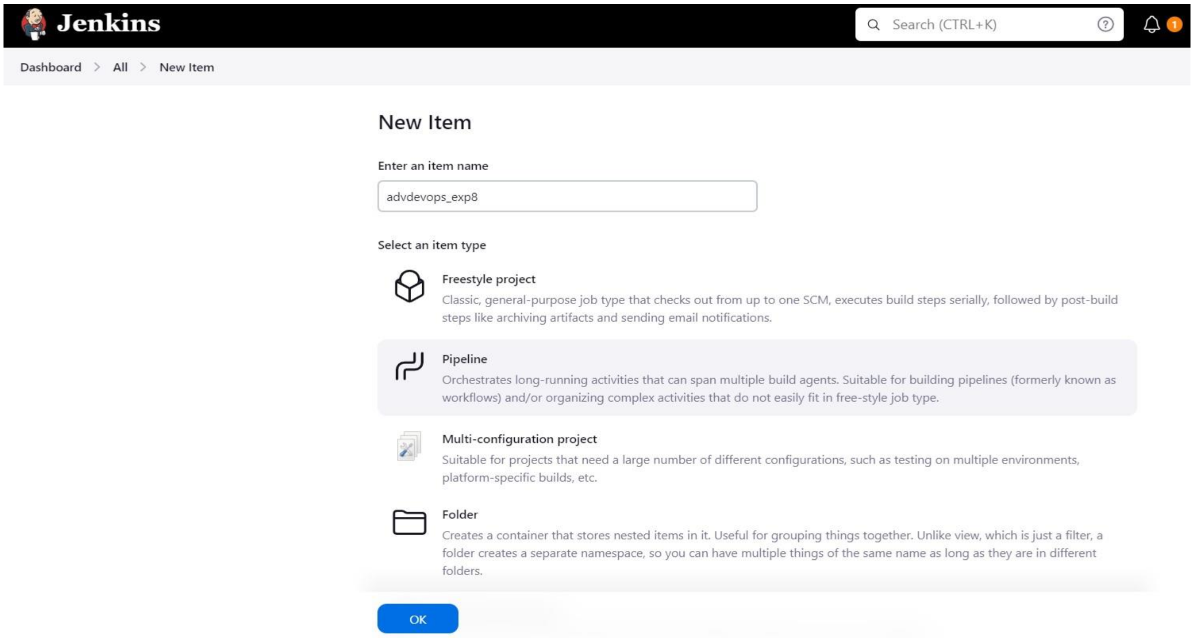
Version: SonarQube Scanner 6.2.0.4584

Add Installer

Add SonarQube Scanner

Save Apply

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



Jenkins — Search (CTRL+K)

Dashboard > All > New Item

New Item

Enter an item name: advdevops_exp8

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.

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.

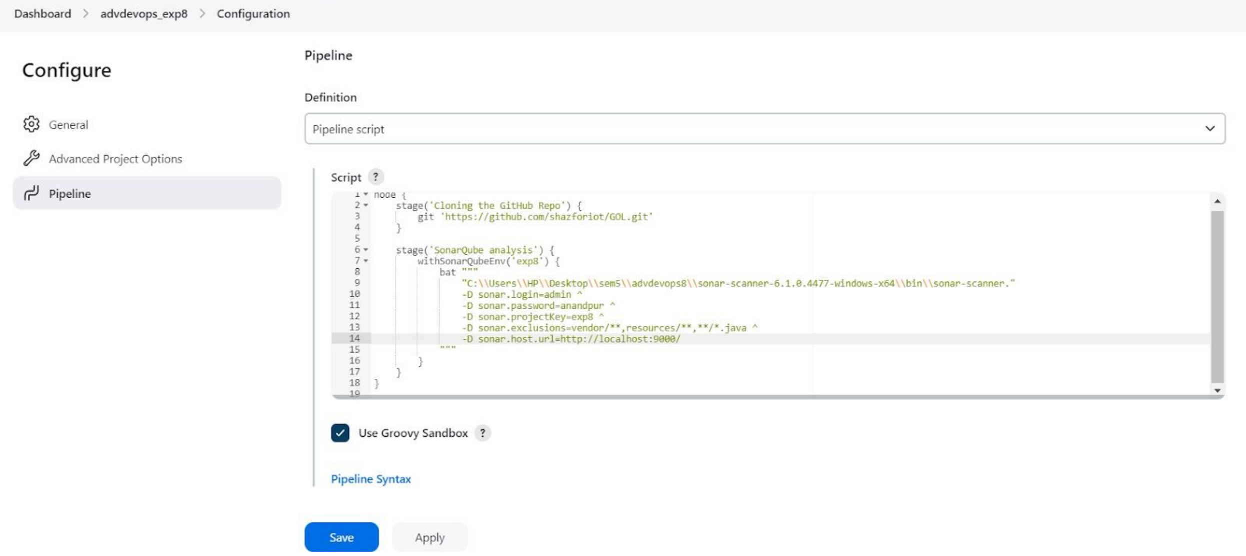
Folder
Creates a container that stores nested items in it. Useful for grouping things together. Unlike view, which is just a filter, a folder creates a separate namespace, so you can have multiple things of the same name as long as they are in different folders.

OK

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_Jenkins>') {
      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.



Pipeline

Definition

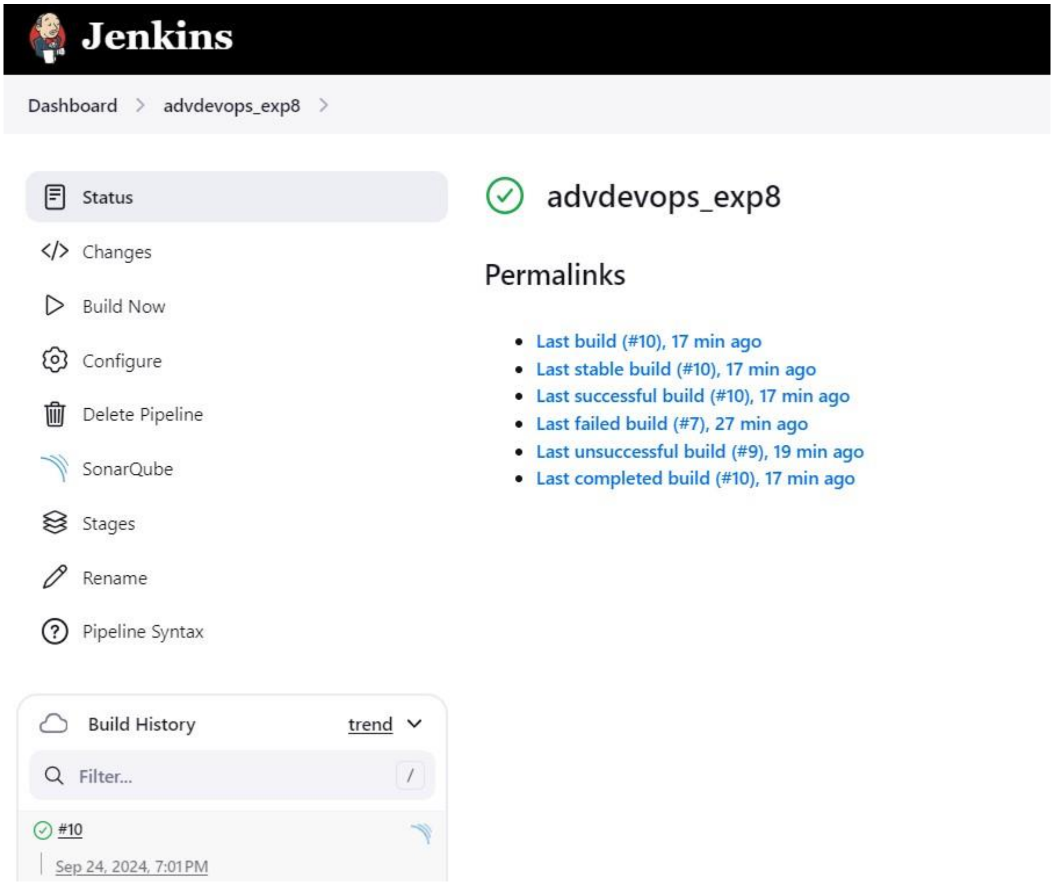
Pipeline script

Script

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

    stage('SonarQube analysis') {
        withSonarQubeEnv('exp8') {
            bat """
                "C:\\Users\\HP\\Desktop\\sem5\\advdevops8\\sonar-scanner-6.1.0.4477-windows-x64\\bin\\sonar-scanner."
                -D sonar.login=admin ^
                -D sonar.password=anandpur ^
                -D sonar.projectKey=exp8 ^
                -D sonar.exclusions=vendor/**,resources/**,**/*.java ^
                -D sonar.host.url=http://localhost:9000/
            """
        }
    }
}
```

☑ Use Groovy Sandbox

11. Build project



advdevops_exp8

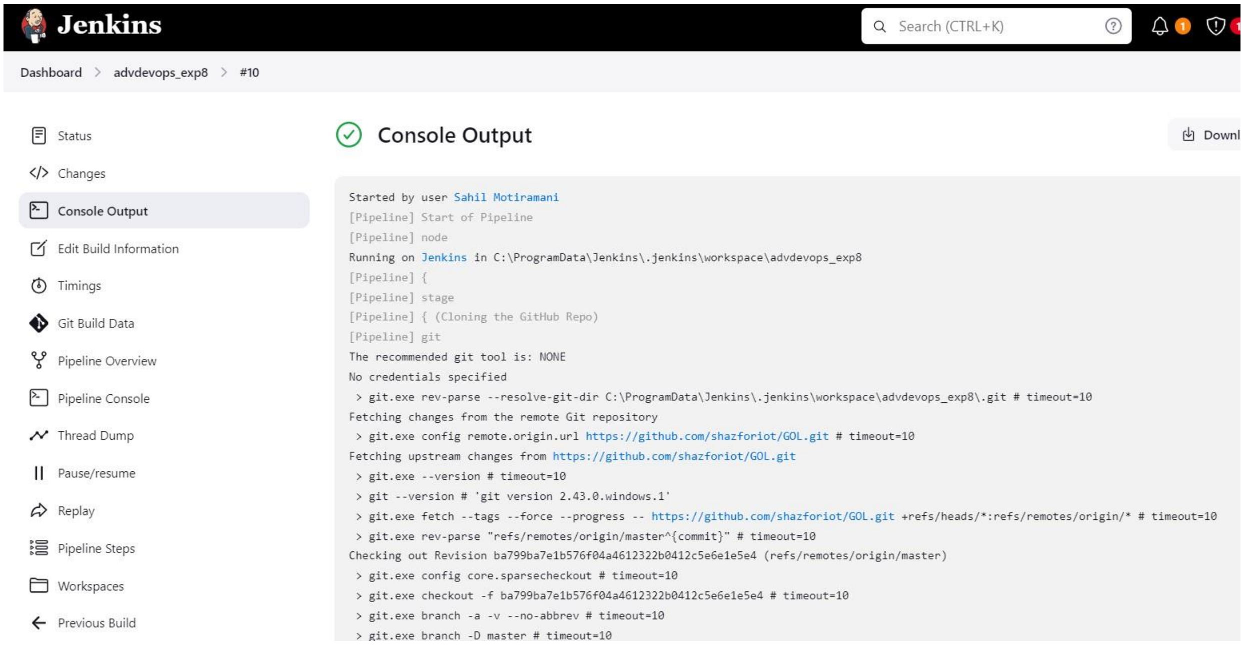
Permalinks

- Last build (#10), 17 min ago
- Last stable build (#10), 17 min ago
- Last successful build (#10), 17 min ago
- Last failed build (#7), 27 min ago
- Last unsuccessful build (#9), 19 min ago
- Last completed build (#10), 17 min ago

#10
Sep 24, 2024, 7:01 PM

Name:Sahil Ramrakhyani Roll No:42 Div:D15C

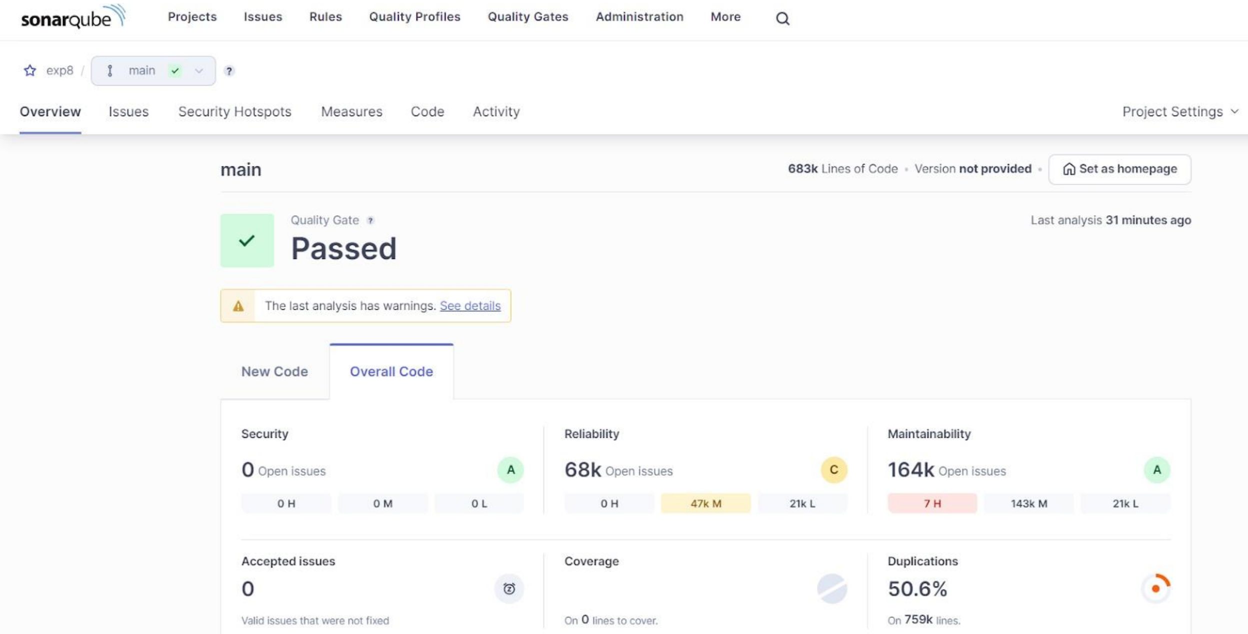
12. Check console



Console Output

```
Started by user Sahil Motiramani
[Pipeline] Start of Pipeline
[Pipeline] node
Running on Jenkins in C:\ProgramData\Jenkins\.jenkins\workspace\advdevops_exp8
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Cloning the GitHub Repo)
[Pipeline] git
The recommended git tool is: NONE
No credentials specified
 > git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\.jenkins\workspace\advdevops_exp8\.git # timeout=10
Fetching changes from the remote Git repository
 > git.exe config remote.origin.url https://github.com/shazforiot/GOL.git # timeout=10
Fetching upstream changes from https://github.com/shazforiot/GOL.git
 > git.exe --version # timeout=10
 > git --version # 'git version 2.43.0.windows.1'
 > git.exe fetch --tags --force --progress -- https://github.com/shazforiot/GOL.git +refs/heads/*:refs/remotes/origin/* # timeout=10
 > git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10
Checking out Revision ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 (refs/remotes/origin/master)
 > git.exe config core.sparsecheckout # timeout=10
 > git.exe checkout -f ba799ba7e1b576f04a4612322b0412c5e6e1e5e4 # timeout=10
 > git.exe branch -a -v --no-abbrev # timeout=10
 > git.exe branch -D master # timeout=10
```

13. Now, check the project in SonarQube



main

683k Lines of Code • Version not provided

Quality Gate

Passed

Last analysis 31 minutes ago

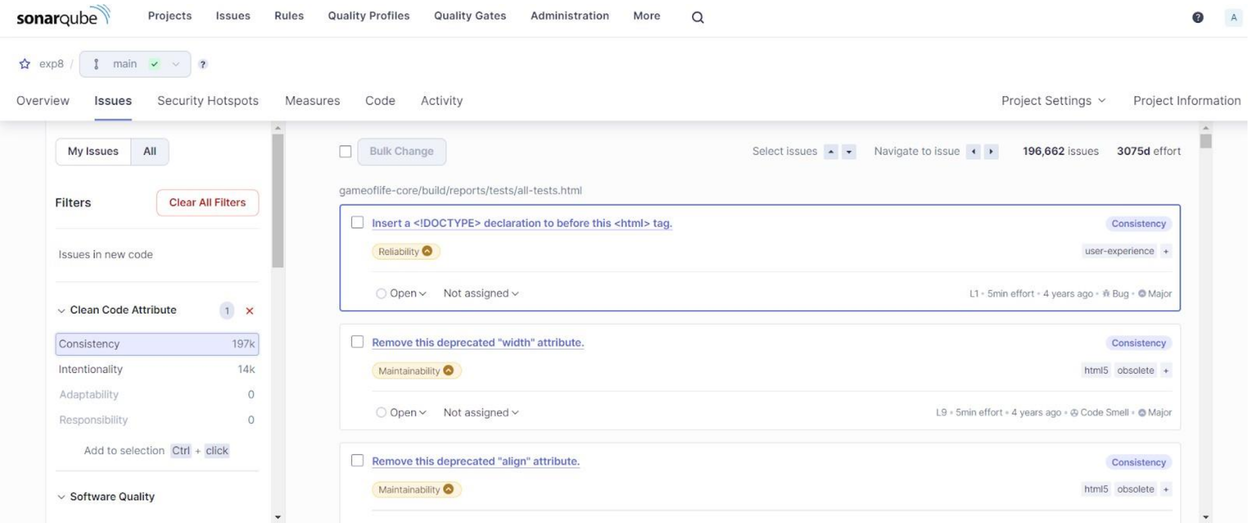
The last analysis has warnings. See details

Security	Reliability	Maintainability
0 Open issues A	68k Open issues C	164k Open issues A
0 H 0 M 0 L	0 H 47k M 21k L	7 H 143k M 21k L
Accepted issues	Coverage	Duplications
0		50.6%
Valid issues that were not fixed	On 0 lines to cover.	On 759k lines.

14. Code Problems

- Consistency

Name:Sahil Ramrakhyani Roll No:42 Div:D15C



196,662 issues 3075d effort

Filters — Clear All Filters

Issues in new code

Clean Code Attribute 1 ✕

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection Ctrl + click

Software Quality

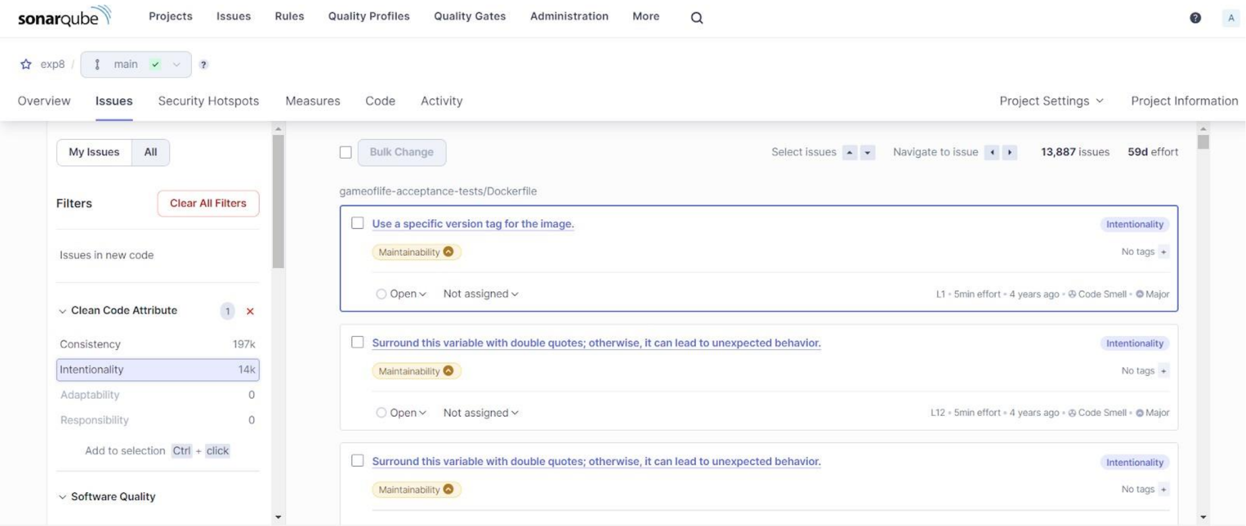
gameoflife-core/build/reports/tests/all-tests.html

□ Insert a <!DOCTYPE> declaration to before this <html> tag. — Consistency
Reliability — user-experience +
○ Open ⌄ Not assigned ⌄ — L1 • 5min effort • 4 years ago • Bug • Major

□ Remove this deprecated "width" attribute. — Consistency
Maintainability — html5 obsolete +
○ Open ⌄ Not assigned ⌄ — L9 • 5min effort • 4 years ago • Code Smell • Major

□ Remove this deprecated "align" attribute. — Consistency
Maintainability — html5 obsolete +

- Intentionality



13,887 issues 59d effort

Filters — Clear All Filters

Issues in new code

Clean Code Attribute 1 ✕

Consistency	197k
Intentionality	14k
Adaptability	0
Responsibility	0

Add to selection Ctrl + click

Software Quality

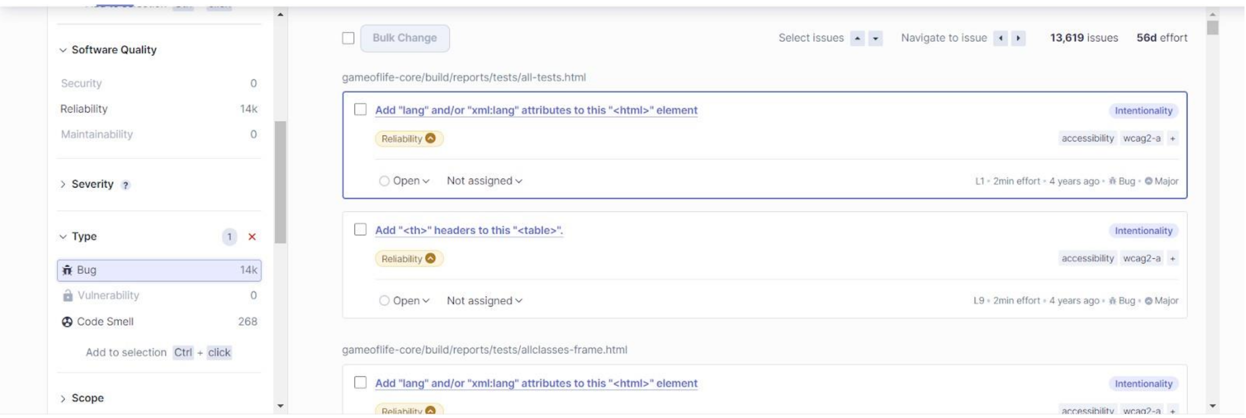
gameoflife-acceptance-tests/Dockerfile

□ 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 +

- Bugs



13,619 issues 56d effort

Software Quality

Security	0
Reliability	14k
Maintainability	0

Severity ?

Type 1 ✕

Bug	14k
Vulnerability	0
Code Smell	268

Add to selection Ctrl + click

Scope

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

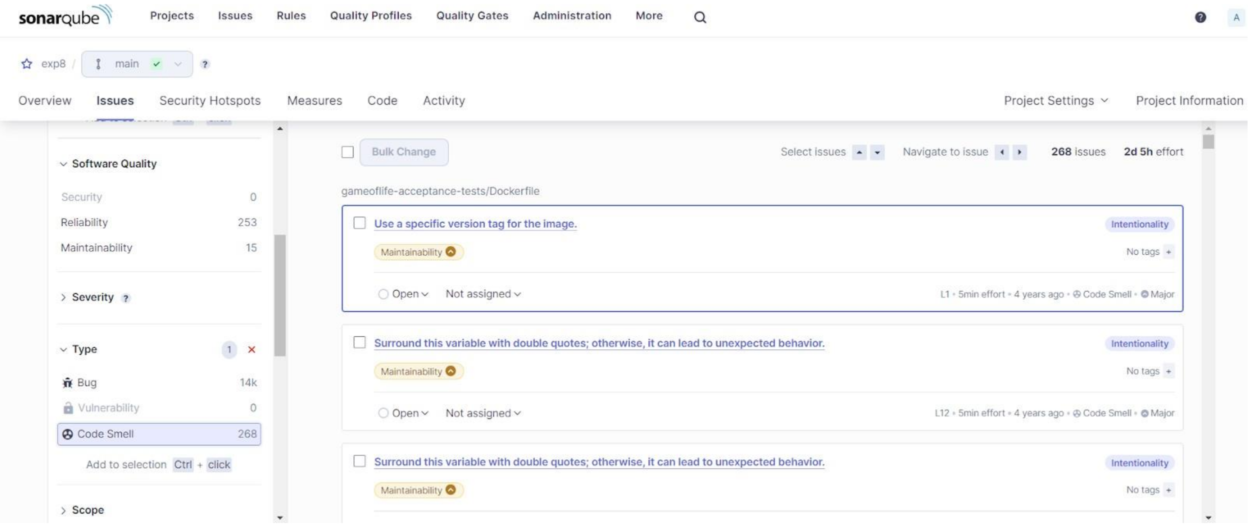
□ Add "<th>" headers to this "<table>". — Intentionality
Reliability — accessibility wcag2-a +
○ Open ⌄ Not assigned ⌄ — L9 • 2min effort • 4 years ago • Bug • Major

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

□ Add "lang" and/or "xml:lang" attributes to this "<html>" element — Intentionality
Reliability — accessibility wcag2-a +

Name:Sahil Ramrakhyani Roll No:42 Div:D15C

- Code Smells



Software Quality

Security	0
Reliability	253
Maintainability	15

Severity

Type 1

Bug	14k
Vulnerability	0
Code Smell	268

Add to selection Ctrl + click

Scope

268 issues 2d 5h effort

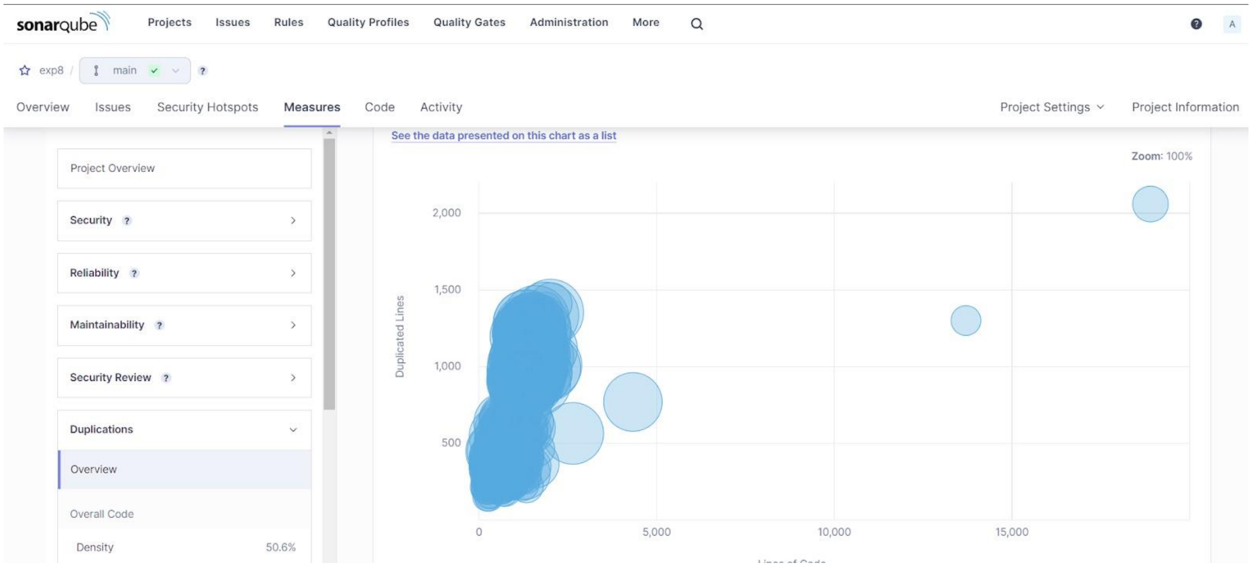
gameoflife-acceptance-tests/Dockerfile

□ Use a specific version tag for the image. Intentionality
Maintainability No tags
○ Open Not assigned L1 • 5min effort • 4 years ago • Code Smell • Major

□ 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

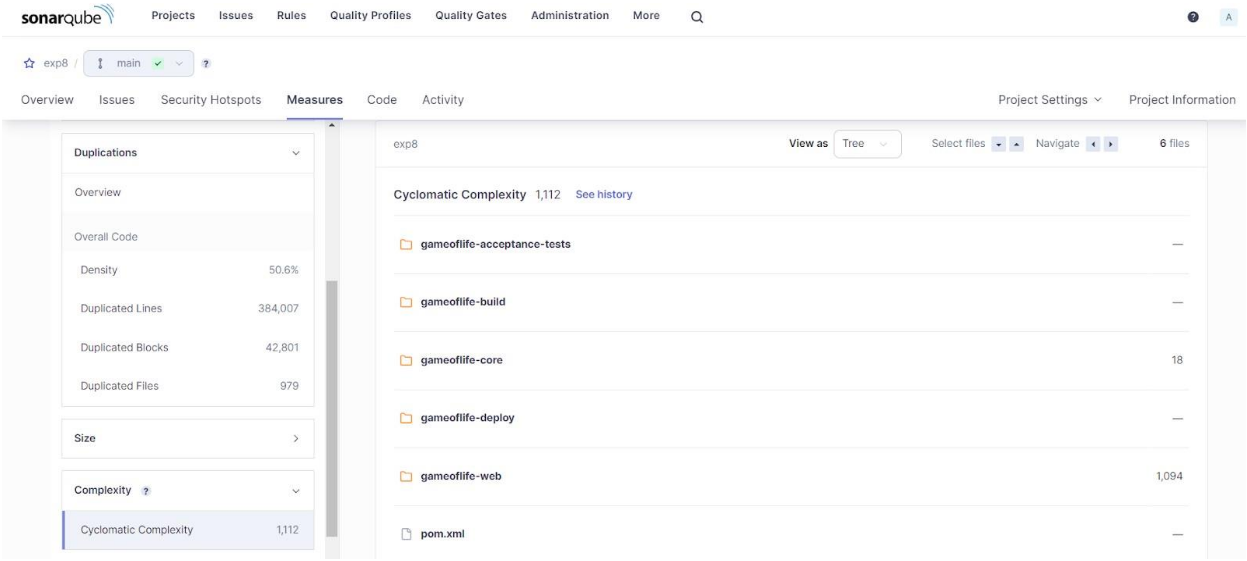
- Duplications



Overall Code

Density	50.6%

- Cyclomatic Complexities



Duplications

Overview

Overall Code

Density	50.6%
Duplicated Lines	384,007
Duplicated Blocks	42,801
Duplicated Files	979

Size

Complexity

Cyclomatic Complexity	1,112

exp8

Cyclomatic Complexity 1,112

gameoflife-acceptance-tests	—
gameoflife-build	—
gameoflife-core	18
gameoflife-deploy	—
gameoflife-web	1,094
pom.xml	—

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

Conclusion:

In this experiment, we integrated Jenkins with SonarQube to enable automated code quality checks within our CI/CD pipeline. We started by deploying SonarQube using Docker, setting up a project, and configuring it to analyze code quality. Next, we configured Jenkins by installing the SonarQube Scanner plugin, adding SonarQube server details, and setting up the scanner tool. We then developed a Jenkins pipeline to automate the process of cloning a GitHub repository and running SonarQube analysis on the code. This integration helps ensure continuous monitoring of code quality, detecting issues such as bugs, code smells, and security vulnerabilities throughout the development process.