

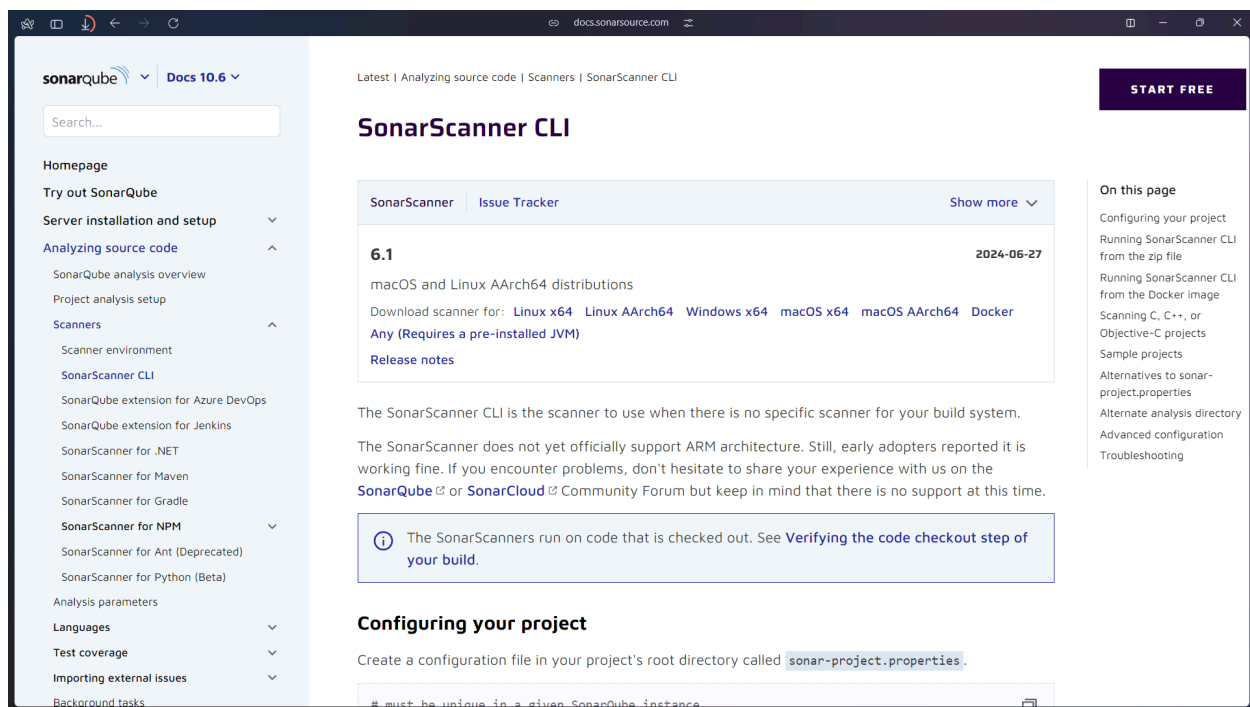
Aim: Create a Jenkins CI/CD Pipeline with SonarQube / GitLab Integration to perform a static analysis of the code to detect bugs, code smells, and security vulnerabilities on a sample Web / Java / Python application.

Prerequisites:

Step 1: Download sonar scanner

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

Visit this link and download the sonarqube scanner CLI.



Extract the downloaded zip file in a folder.

1) Docker

Run docker -v command.

```
PS C:\Users\saira\OneDrive\Desktop\AdvDevOps\lab7> docker -v
Docker version 27.0.3, build 7d4bcd8
```

2) Install sonarqube image

Command: docker pull sonarqube

```
PS C:\Users\saira\OneDrive\Desktop\AdvDevOps\lab7> docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
762bedf4b1b7: Pull complete
95f9bd9906fa: Pull complete
a32d681e6b99: Pull complete
aabdd0a18314: Pull complete
5161e45ecd8d: Pull complete
aeb0020dfa06: Pull complete
01548d361aea: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:bb444c58c1e04d8a147a3bb12af941c57e0100a5b21d10e599384d59bed36c86
Status: Downloaded newer image for sonarqube:latest
docker.io/library/sonarqube:latest

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

3) Keep Jenkins installed on your system.

Experiment Steps:

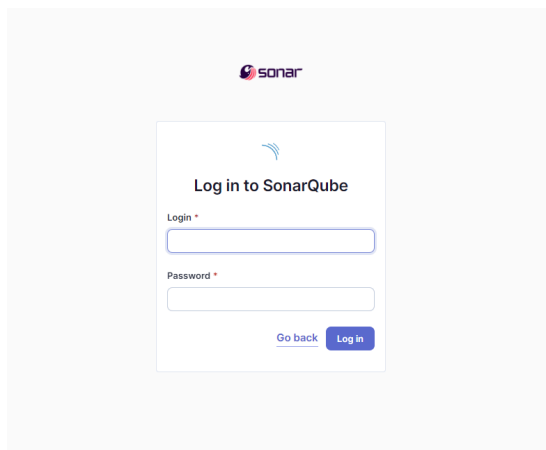
Step 1) Run SonarQube image

```
docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
```

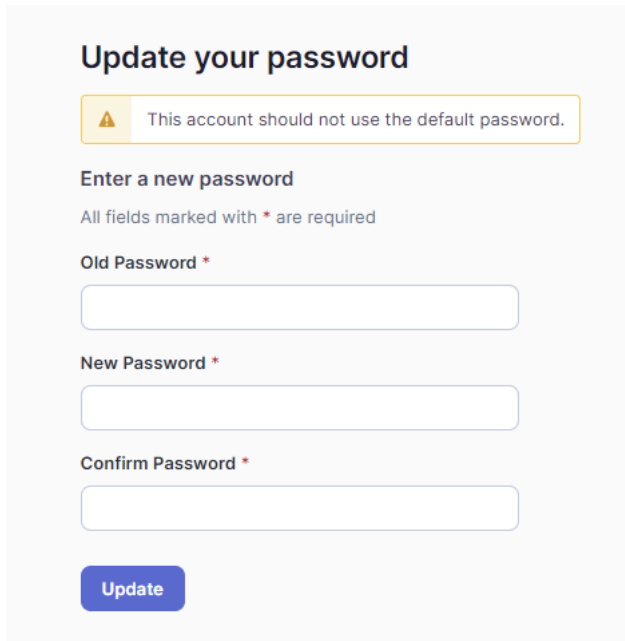
This command will run the SonarQube image that was just installed using docker.

```
PS C:\Users\saira\OneDrive\Desktop\AdvDevOps\lab7> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
36ff8a656bd28857ba9a28bf2bb0174099ae3232a9fc9ba2766d46f0c14d08a6
```

Step 2) Once the SonarQube image is started, you can go to <http://localhost:9000> to find the SonarQube that has started

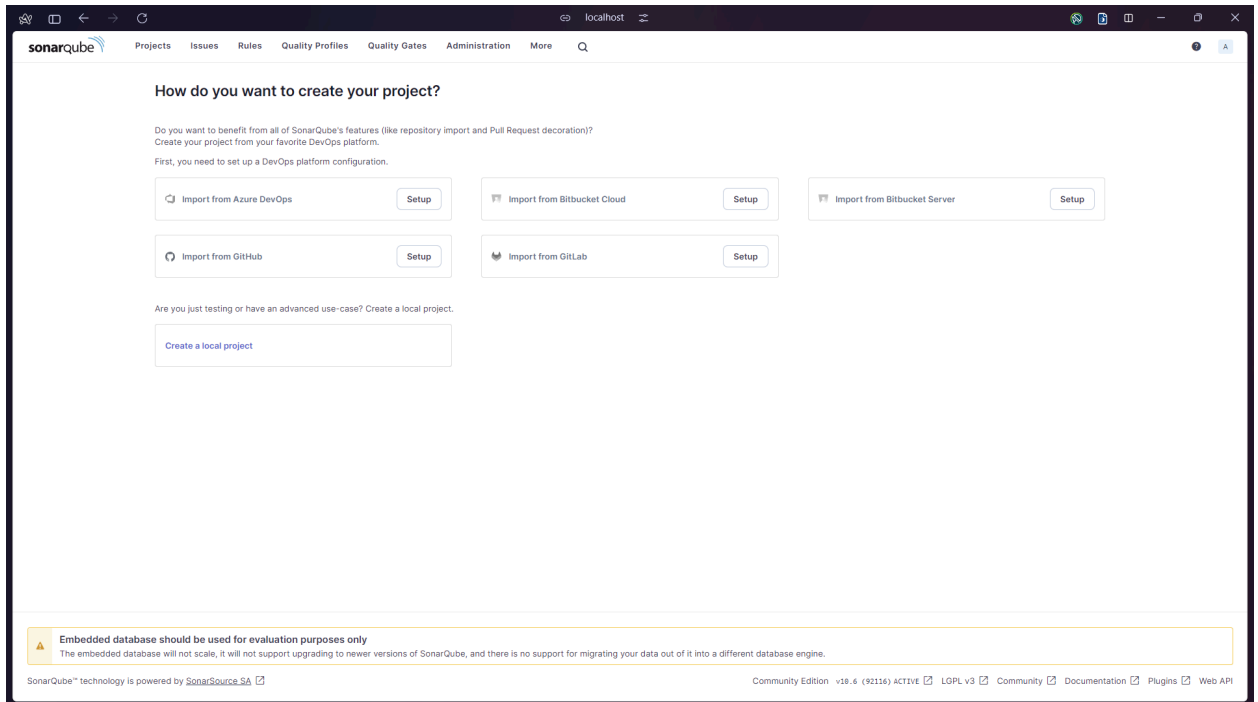


Step 3) On this interface, login with username = 'admin' and password = 'admin'. Once logged in successfully, SonarQube will ask you to reset this password. Reset it and remember this password.



The image shows the 'Update your password' form in SonarQube. At the top, there is a warning message: 'This account should not use the default password.' Below this, the section is titled 'Enter a new password'. A note states: 'All fields marked with * are required'. There are three input fields: 'Old Password *', 'New Password *', and 'Confirm Password *'. Each field is a simple text box. At the bottom of the form is a blue button labeled 'Update'.

Step 4) After changing the password, you will be directed to this screen. Click on Create a Local Project.



The image shows the 'How do you want to create your project?' screen in SonarQube. The page has a navigation bar at the top with links: Projects, Issues, Rules, Quality Profiles, Quality Gates, Administration, and More. Below the navigation bar, the main heading is 'How do you want to create your project?'. A sub-heading asks: '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.' There are five buttons arranged in two rows: 'Import from Azure DevOps', 'Import from Bitbucket Cloud', 'Import from Bitbucket Server', 'Import from GitHub', and 'Import from GitLab'. Each button has a 'Setup' link next to it. Below these buttons, there is a section titled 'Are you just testing or have an advanced use-case? Create a local project.' with a button labeled 'Create a local project'. At the bottom of the page, there is a footer with a 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.' The footer also includes the SonarQube logo, the text 'SonarQube™ technology is powered by SonarSource SA', and links for 'Community Edition v10.6 (92116) ACTIVE', 'LGPL v3', 'Community', 'Documentation', 'Plugins', and 'Web API'.

Give the project a display name and project key

1 of 2

Create a local project

Project display name *

sonarqube



Project key *

sonarqube



Main branch name *

main

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

Cancel

Next

Set up the project as required and click on create.

The screenshot shows the SonarQube web interface at localhost. The page is titled 'Set up project for Clean as You Code' and is the second step in a two-step process. It explains that the new code definition sets which part of the code will be considered new code, helping to focus attention on recent changes. The page offers three options for choosing the baseline for new code: 'Use the global setting' (selected), 'Define a specific setting for this project' (with sub-options for 'Previous version', 'Number of days', and 'Reference branch'), and 'Create project' button. A warning message at the bottom states: '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.'

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.

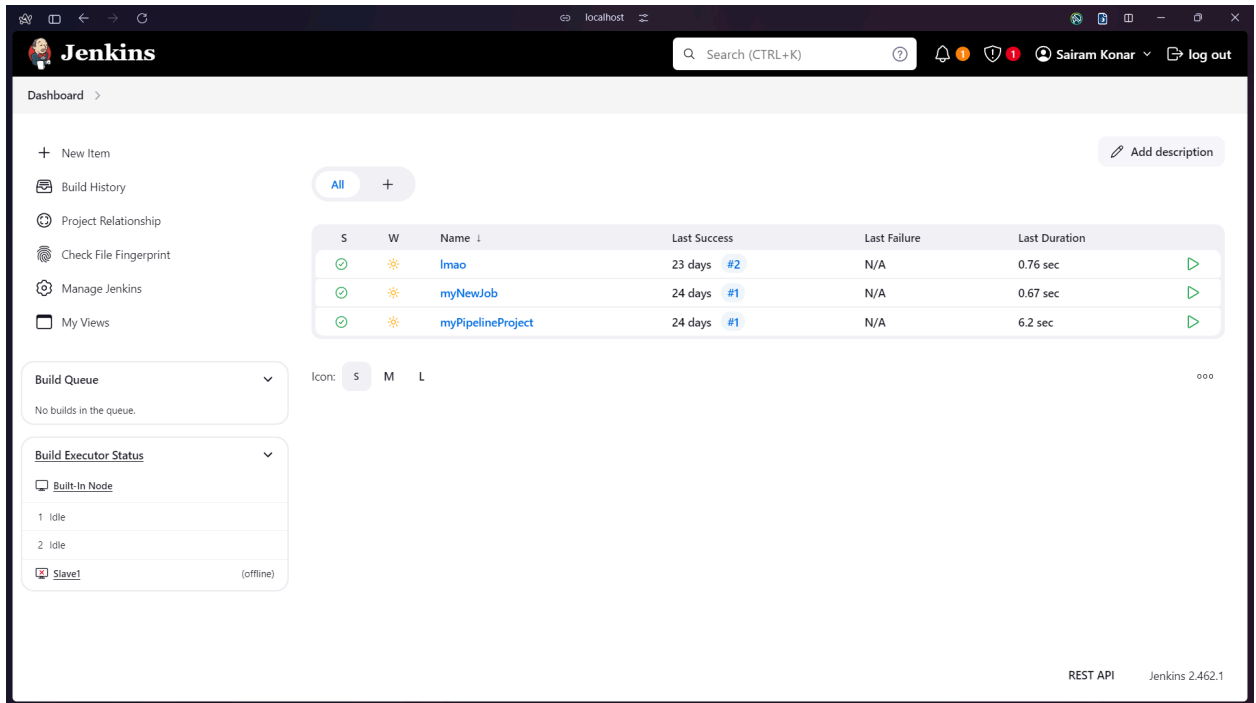
☐ Number of days
Any code that has changed in the last x days is considered new code. If no action is taken on a new issue after x days, this issue will become part of the overall code.
Recommended for projects following continuous delivery.

☐ Reference branch
Choose a branch as the baseline for the new code.
Recommended for projects using feature branches.

[Back](#) [Create project](#)

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.

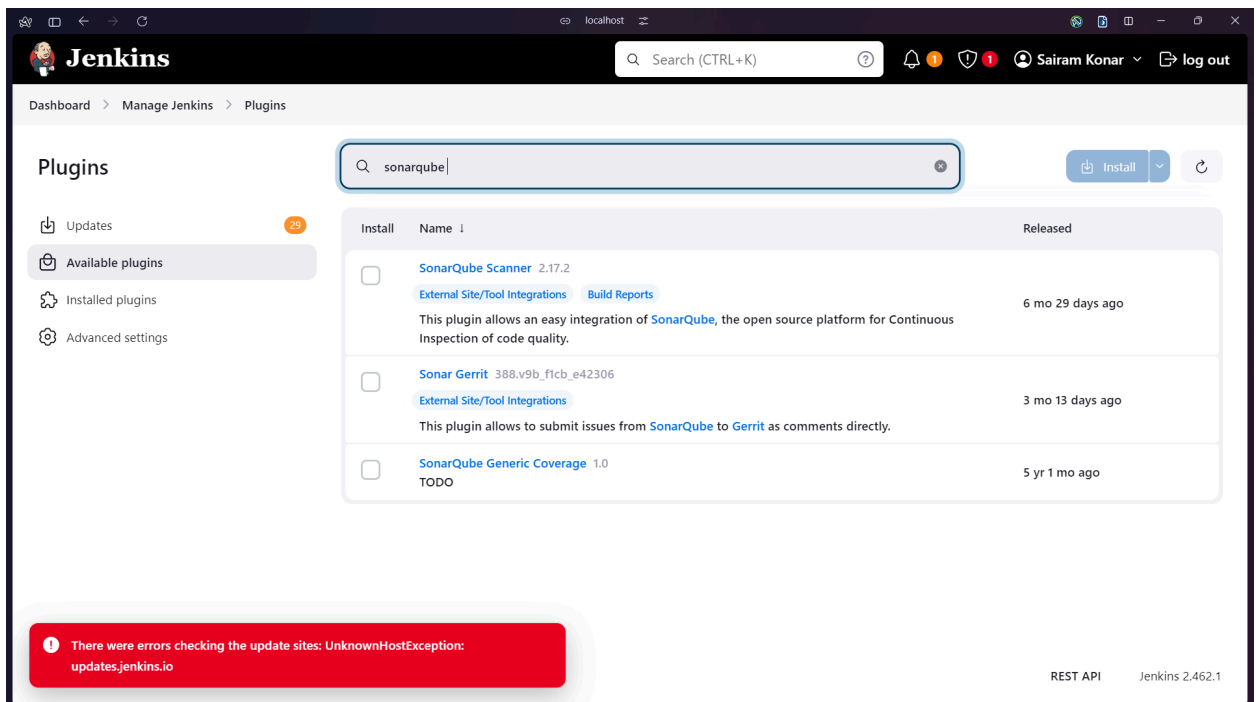
Step 5) Open Jenkins on whichever port it is installed. (http://localhost:<port_number>).



The screenshot shows the Jenkins Dashboard interface. The top navigation bar includes the Jenkins logo, a search bar, and user information (Sairam Konar) with a log out button. The main content area features a sidebar with navigation links: New Item, Build History, Project Relationship, Check File Fingerprint, Manage Jenkins, and My Views. The central panel displays a table of recent builds with columns for status (S), warnings (W), name, last success, last failure, and last duration. Below the table, there are sections for 'Build Queue' (showing no builds) and 'Build Executor Status' (showing 1 idle and 2 offline executors). The bottom right corner indicates the REST API and Jenkins version 2.462.1.

S	W	Name	Last Success	Last Failure	Last Duration
✓	⚠	Imao	23 days #2	N/A	0.76 sec
✓	⚠	myNewJob	24 days #1	N/A	0.67 sec
✓	⚠	myPipelineProject	24 days #1	N/A	6.2 sec

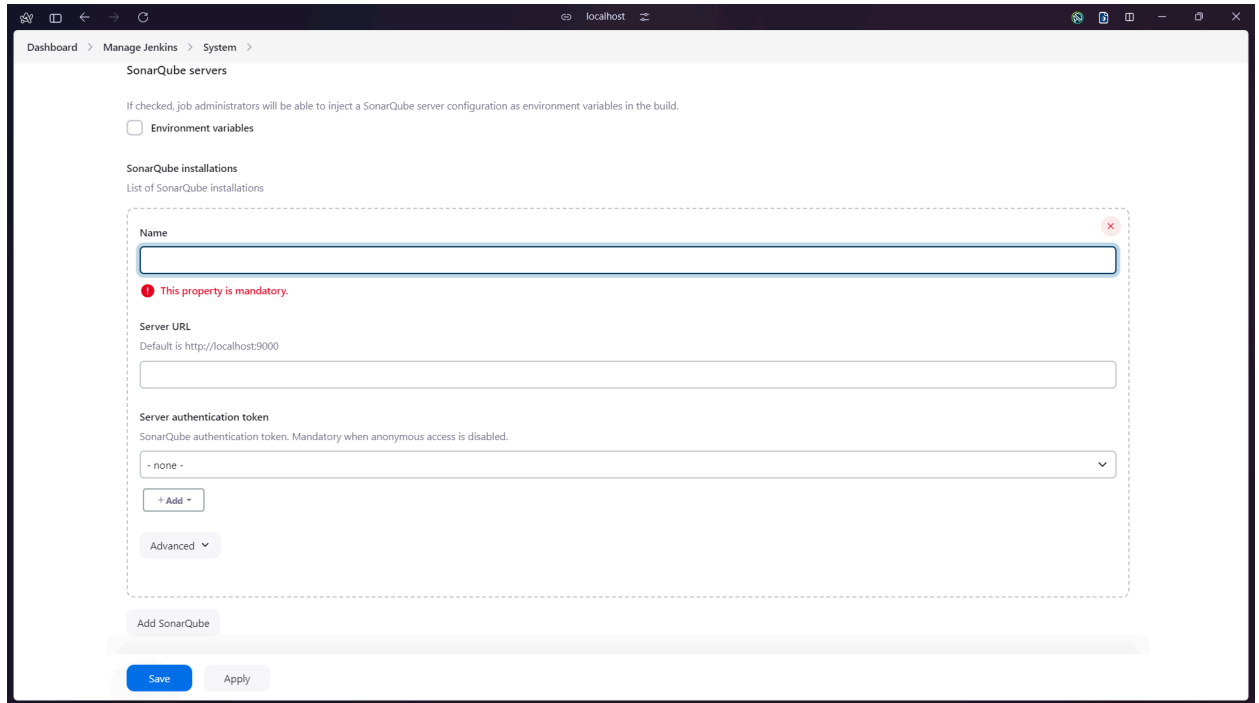
Step 6) Go to manage jenkins → Search for Sonarqube Scanner for Jenkins and install it.



The screenshot shows the Jenkins 'Manage Jenkins' > 'Plugins' page. A search bar at the top contains 'sonarqube'. The left sidebar shows navigation links: Updates (29), Available plugins, Installed plugins, and Advanced settings. The main content area displays a table of available plugins with columns for 'Install', 'Name', and 'Released'. The 'SonarQube Scanner' plugin is highlighted. A red error banner at the bottom states: 'There were errors checking the update sites: UnknownHostException: updates.jenkins.io'. The bottom right corner indicates the REST API and Jenkins version 2.462.1.

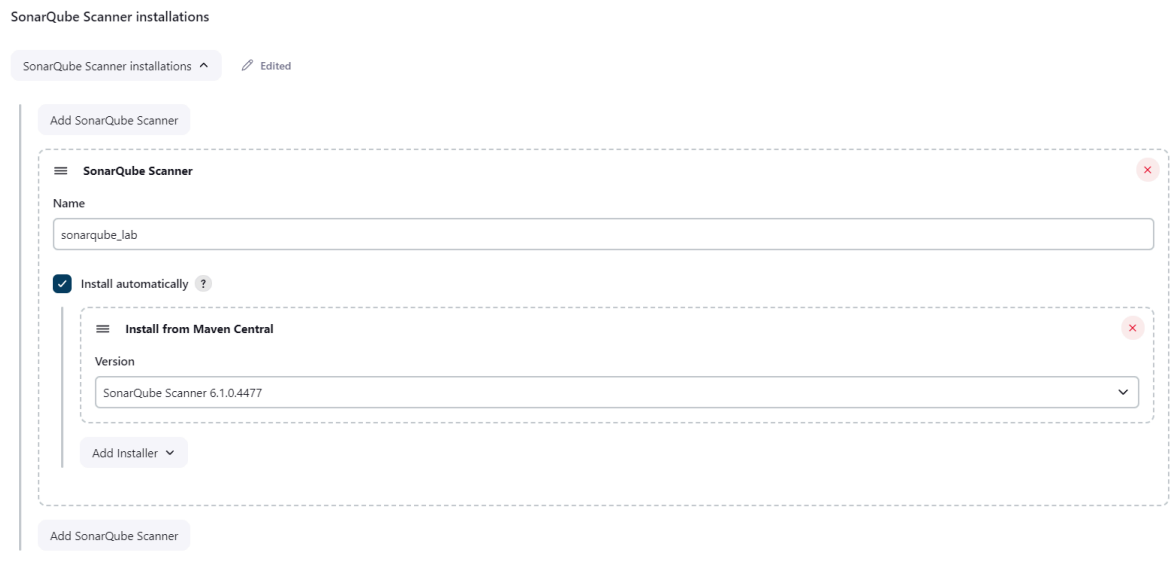
Install	Name	Released
<input type="checkbox"/>	SonarQube Scanner 2.17.2 External Site/Tool Integrations Build Reports This plugin allows an easy integration of SonarQube , the open source platform for Continuous Inspection of code quality.	6 mo 29 days ago
<input type="checkbox"/>	Sonar Gerrit 388.v9b_f1cb_e42306 External Site/Tool Integrations This plugin allows to submit issues from SonarQube to Gerrit as comments directly.	3 mo 13 days ago
<input type="checkbox"/>	SonarQube Generic Coverage 1.0 TODO	5 yr 1 mo ago

Step 7) Now, go to Manage Jenkins → System. Under Sonarqube servers, add a server. Add server authentication token if needed.



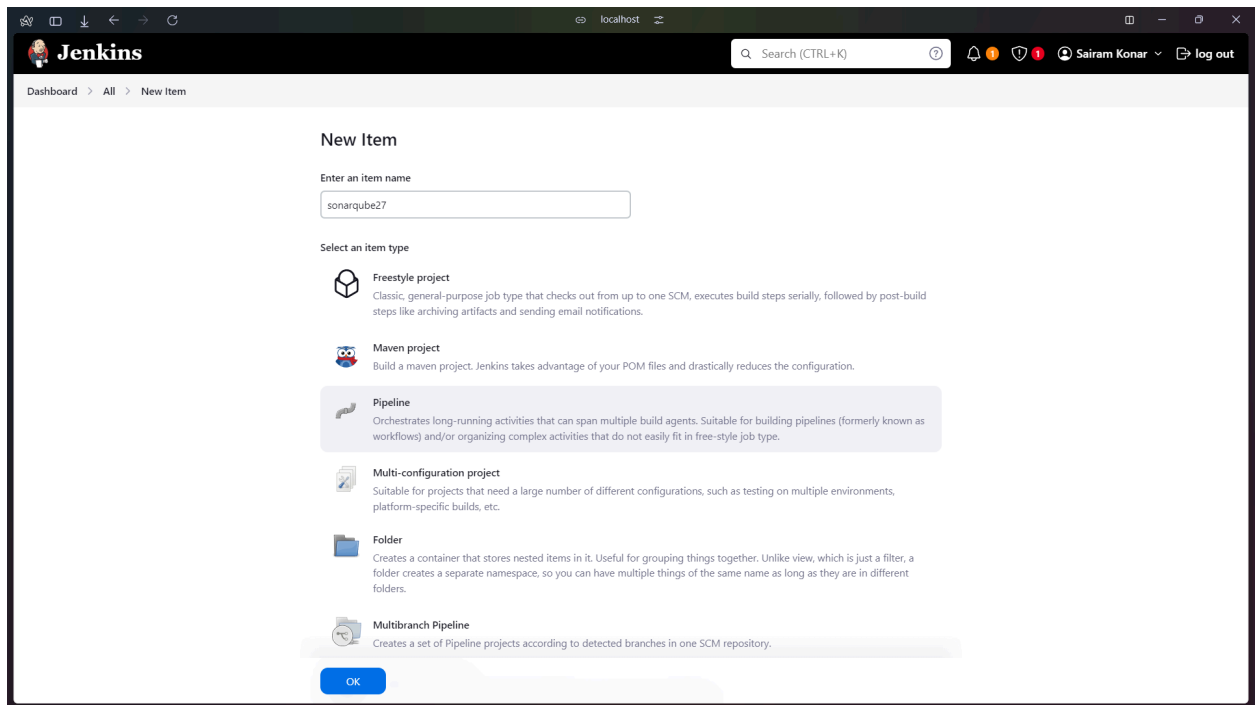
The screenshot shows the 'SonarQube servers' configuration page in Jenkins. The page has a breadcrumb trail: Dashboard > Manage Jenkins > System > SonarQube servers. It includes a checkbox for 'Environment variables' with a note: 'If checked, job administrators will be able to inject a SonarQube server configuration as environment variables in the build.' Below this is the 'SonarQube installations' section, titled 'List of SonarQube installations'. It contains a form for adding a new installation with fields for 'Name' (with a red error message 'This property is mandatory.'), 'Server URL' (with a default value of 'http://localhost:9000'), and 'Server authentication token' (a dropdown menu currently set to '- none -'). There are '+ Add +' and 'Advanced' buttons at the bottom of the form. At the very bottom of the page are 'Save' and 'Apply' buttons.

Step 8) Go to Manage Jenkins → Tools. Go to SonarQube scanner, choose the latest configuration and choose install automatically.



The screenshot shows the 'SonarQube Scanner installations' page in Jenkins. It has a breadcrumb trail: Dashboard > Manage Jenkins > Tools > SonarQube Scanner installations. The page title is 'SonarQube Scanner installations' with an 'Edited' status. There is an 'Add SonarQube Scanner' button at the top. The main form is titled 'SonarQube Scanner' and contains a 'Name' field with the value 'sonarqube_lab'. Below this is a checked checkbox for 'Install automatically' with a help icon. Underneath is a sub-section titled 'Install from Maven Central' with a 'Version' dropdown menu set to 'SonarQube Scanner 6.1.0.4477'. There is an 'Add Installer' button at the bottom of the form. At the very bottom of the page is another 'Add SonarQube Scanner' button.

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



Step 10) Under Pipeline script, enter the following:

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

    stage('SonarQube analysis') {
        withSonarQubeEnv('sonarqube lab') {
            bat """
                <PATH_TO_SONARSCANNER_FOLDER>\\bin\\sonar-scanner.bat ^
                -D sonar.login=<SONARQUBE_LOGIN> ^
                -D sonar.password=<SONARQUBE_PASSWORD> ^
                -D sonar.projectKey=<PROJECT_KEY> ^
                -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.

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('sonarqube lab') {

8 bat """

9 C:\Users\saira\Downloads\sonar-scanner-cli-6.1.0.4477-windows-x64\sonar-scanner-6.1.0.4477-windows-x64\bin\sonar-scanner.bat ^

10 -D sonar.login=admin ^

11 -D sonar.password=123456 ^

12 -D sonar.projectKey=sonarqube27 ^

13 -D sonar.exclusions=vendor/**,resources/**,**/*.java ^

14 -D sonar.host.url=http://localhost:9000/

15 """

16 }

17 }

18 }

19 }

try sample Pipeline...


☒ Use Groovy Sandbox ?

[Pipeline Syntax](#)

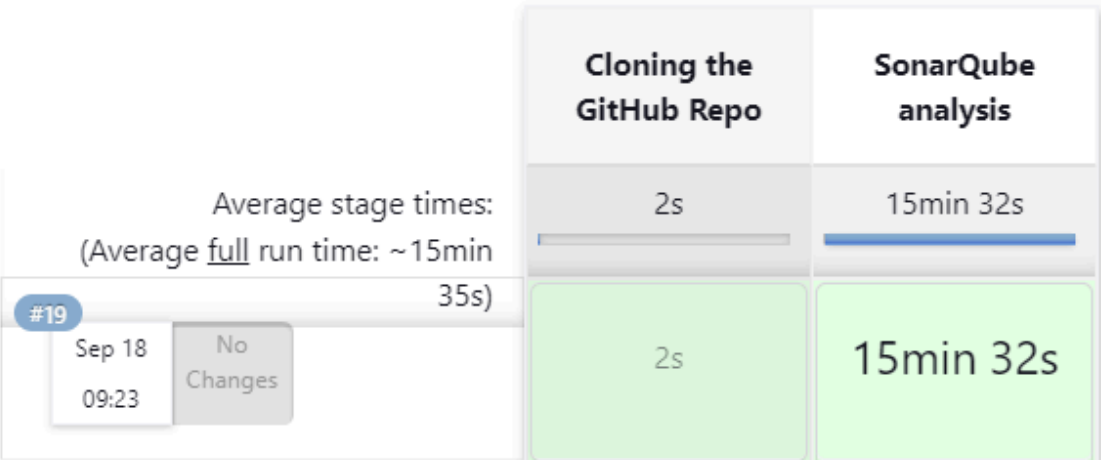
Save

Apply

Step 11) Go back to jenkins. Go to the job you had just built and click on Build Now.

 sonarqube27

Stage View



Permalinks

Check the console output once

```

+first 100 references.
09:36:08.013 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/gui/action/Cut.html for block at line 75. Keep only the
first 100 references.
09:36:08.029 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/jdbc/config/package-summary.html for block at
line 39. Keep only the first 100 references.
09:36:08.029 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/jdbc/config/package-summary.html for block at
line 40. Keep only the first 100 references.
09:36:08.054 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/util/accesslog/Generator.html for block at
line 40. Keep only the first 100 references.
09:36:08.054 WARN Too many duplication references on file gameoflife-web/tools/jmeter/docs/api/org/apache/jmeter/protocol/http/util/accesslog/Generator.html for block at
line 41. Keep only the first 100 references.
09:36:08.055 INFO CPD Executor CPD calculation finished (done) | time=163405ms
09:36:08.069 INFO SCM revision ID 'ba799ba7e1b576f04a4612322b0412c5e6e1e5e4'
09:38:20.750 INFO Analysis report generated in 4390ms, dir size=127.2 MB
09:38:45.857 INFO Analysis report compressed in 25089ms, zip size=29.6 MB
09:38:46.532 INFO Analysis report uploaded in 675ms
09:38:46.533 INFO ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarqube27
09:38:46.533 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
09:38:46.533 INFO More about the report processing at http://localhost:9000/api/ce/task?id=46576333-cbde-4277-89d7-471ee554de32
09:39:00.038 INFO Analysis total time: 15:24.256 s
09:39:00.041 INFO SonarScanner Engine completed successfully
09:39:00.810 INFO EXECUTION SUCCESS
09:39:00.811 INFO Total time: 15:29.301s

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

```

Step 12) Once the build is complete, go back to SonarQube and check the project linked.

The screenshot shows the SonarQube web interface for project 'sonarqube27'. The status is 'Passed' with a green checkmark. A warning message states: 'The last analysis has warnings. See details'. The interface displays various quality metrics:

- Security:** 0 Open Issues (Grade A)
- Reliability:** 68k Open Issues (Grade C)
- Maintainability:** 164k Open Issues (Grade A)
- Accepted issues:** 0 (Valid issues that were not fixed)
- Coverage:** On 0 lines to cover.
- Duplications:** 50.6% (On 759k lines)
- Security Hotspots:** 3 (Grade E)

The 'Activity' section at the bottom shows a list of recent issues.

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

- Code Problems

- Consistency

☐ Bulk Change

Select issues

Navigate to issue

196,662 issues

3075d effort

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

Open

Not assigned

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

☐ Remove this deprecated "align" attribute.

Consistency

Maintainability

html5 obsolete

Open

Not assigned

for evaluation purposes only

⚠️ 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.

- Intentionality

☐ 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

for evaluation purposes only

⚠️ 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.

Bugs

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

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

for evaluation purposes only

ill 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.

Code Smells

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

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

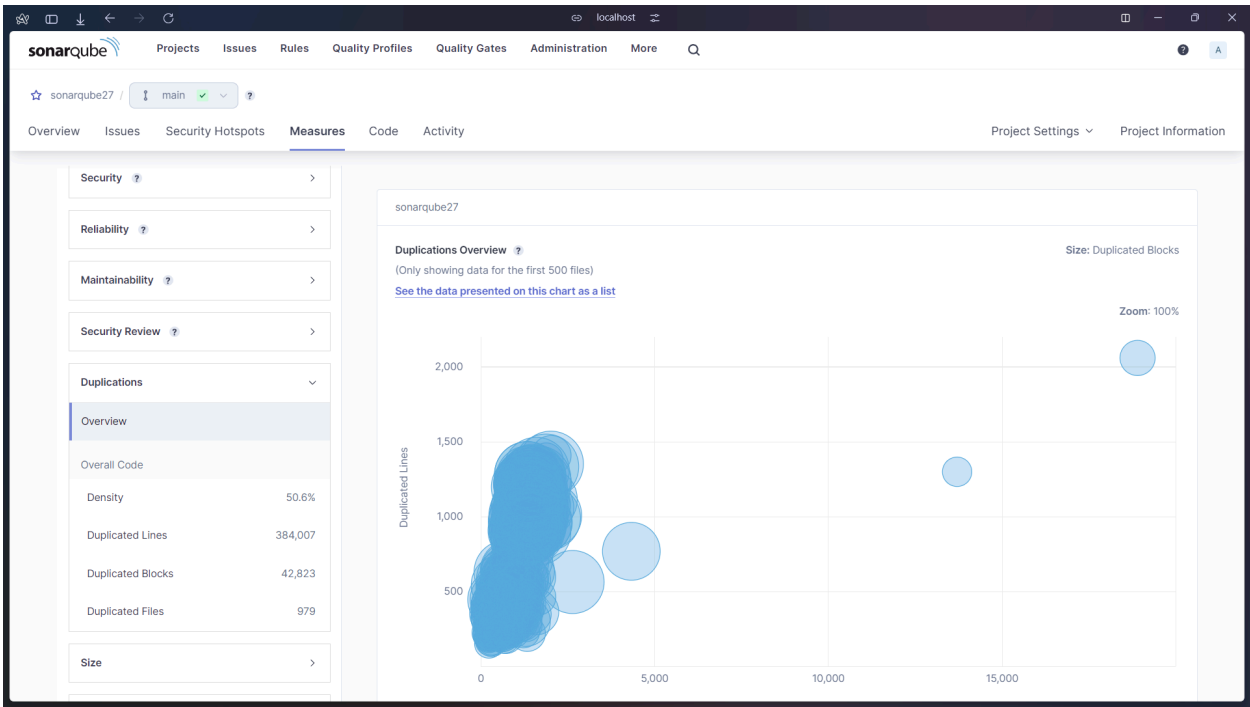
Maintainability

No tags

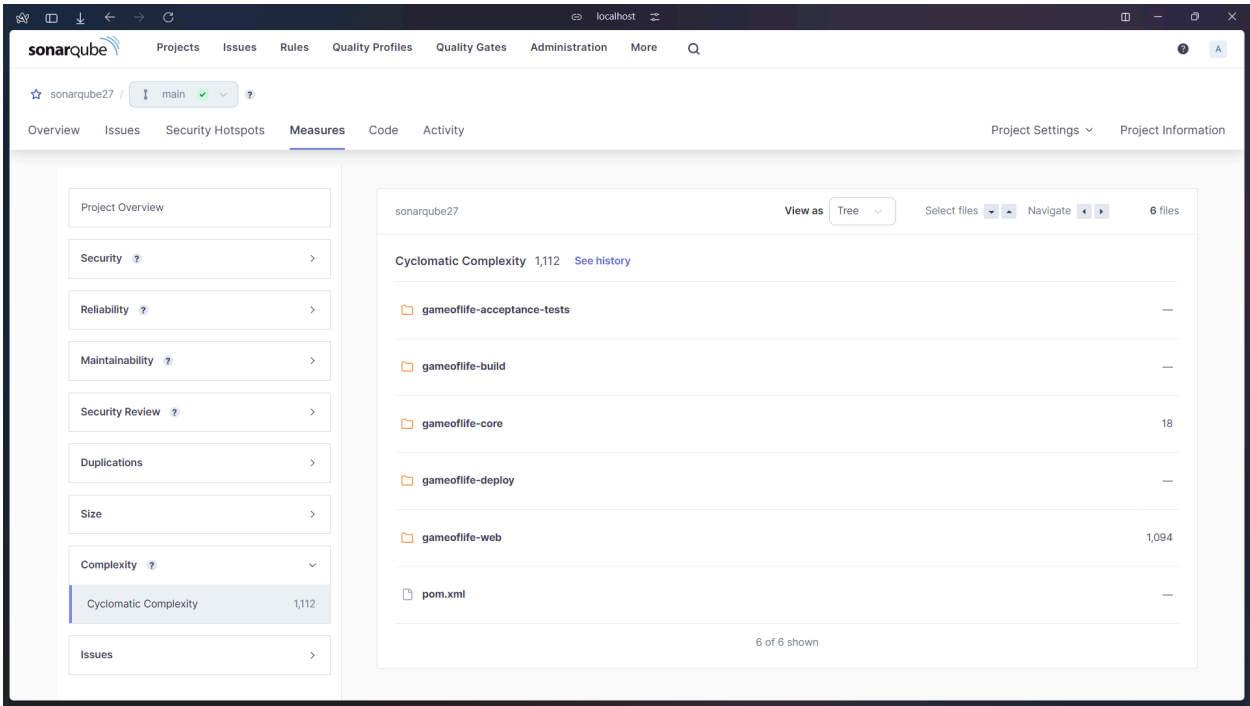
for evaluation purposes only

ill 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.

- Duplications



- Cyclomatic Complexities



Conclusion: In this experiment, we have learned how to perform static analysis of a code using Jenkins CI/CD Pipeline with SonarQune analysis. A pipeline project is to be created which is given a pipeline script. This script contains all the information needed for the project to run the SonarQube analysis. After the necessary configurations are made on jenkins, the Jenkins project is built. The code provided in this experiment contains lots of error, bugs, duplications which can be checked on the SonarQube project linked with this build.