

## EXPERIMENT 7

Aim: To understand Static Analysis SAST process and learn to integrate Jenkins SAST to SonarQube/GitLab.

Step 1: Open Windows PowerShell and run the following command –

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

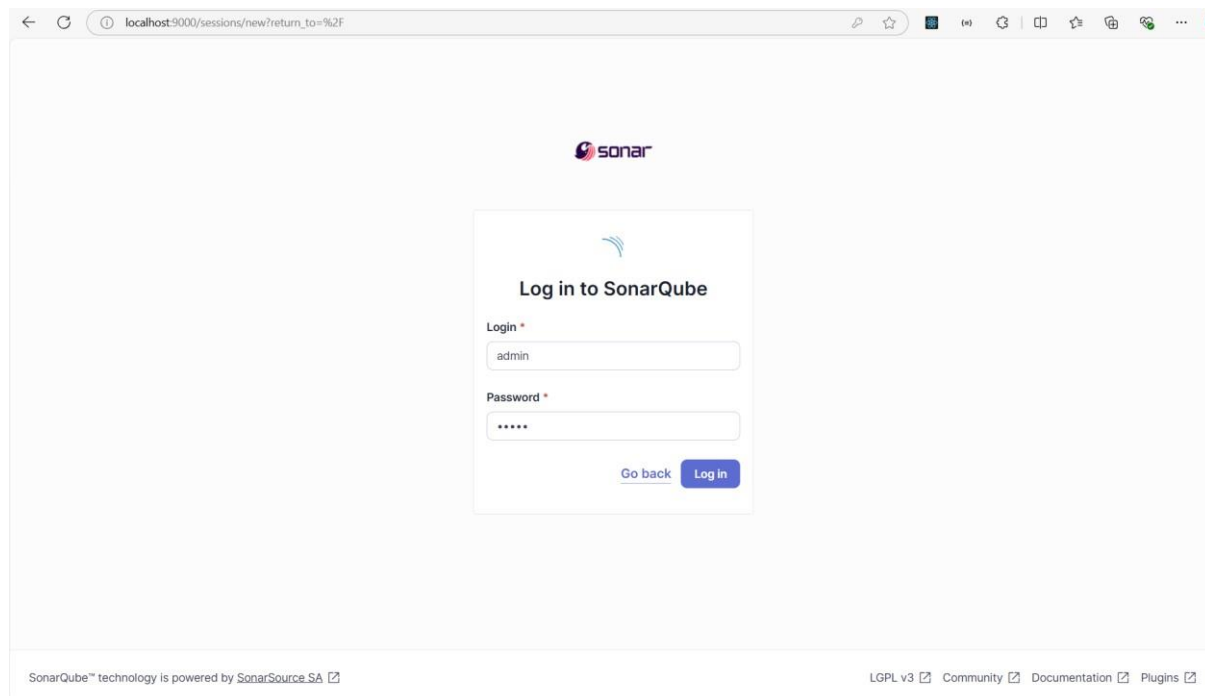
WARNING: Run the following command only once

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\User> docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
Unable to find image 'sonarqube:latest' locally
latest: Pulling from library/sonarqube
7478e0ac0f23: Pull complete
90a925ab929a: Pull complete
7d9a34308537: Pull complete
80338217a4ab: Pull complete
1a5fd5c7e184: Pull complete
7b87d6fa783d: Pull complete
bd819c9b5ead: Pull complete
4f4fb700ef54: Pull complete
Digest: sha256:72e9feec71242af83faf65f95a40d5e3bb2822a6c3b2cda8568790f3d31aecde
Status: Downloaded newer image for sonarqube:latest
006052311e5b87fb720cdca68c48b3d4dc391232a27d69e62dcd946bf75eb824
PS C:\Users\User>
```

Step 2: Visit <http://localhost:9000/> to open SonarQube. Login with username: admin and password: admin.



Step 3: Click on create a local project and name the project as sonarqube-test and key as sonarqube-test and click on the next button. In the next step select the “Use the global setting” option and click on create project.

←↻🔍localhost:9000/projects/create

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore🔍

🔔A

## 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.

🔗 Import from Azure DevOps

Setup

🔗 Import from Bitbucket Cloud

Setup

🔗 Import from Bitbucket Server

Setup

🔗 Import from GitHub

Setup

🔗 Import from GitLab

Setup

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

Create a local 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.

SonarQube™ technology is powered by [SonarSource SA](#) [🔗](#)Community Edition v10.6 (92116) [ACTIVE](#) [🔗](#) [LGPL v3](#) [🔗](#) [Community](#) [🔗](#) [Documentation](#) [🔗](#) [Plugins](#) [🔗](#) [Web API](#)

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore🔍

🔔A

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](#) [🔗](#)

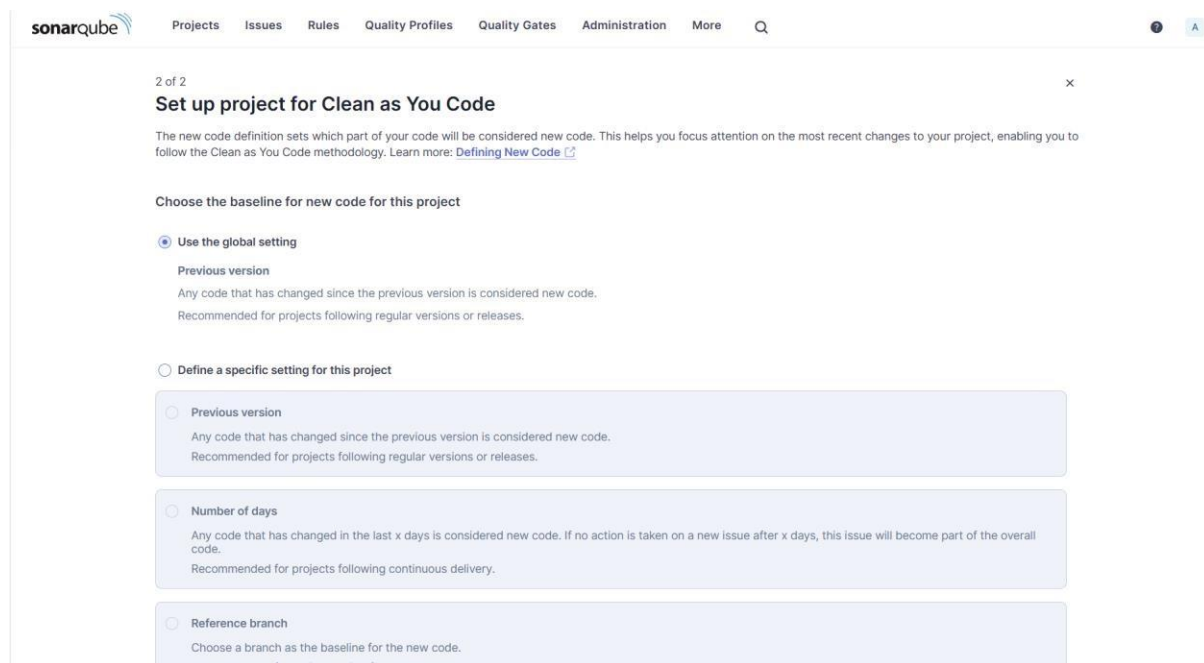
Cancel

Next

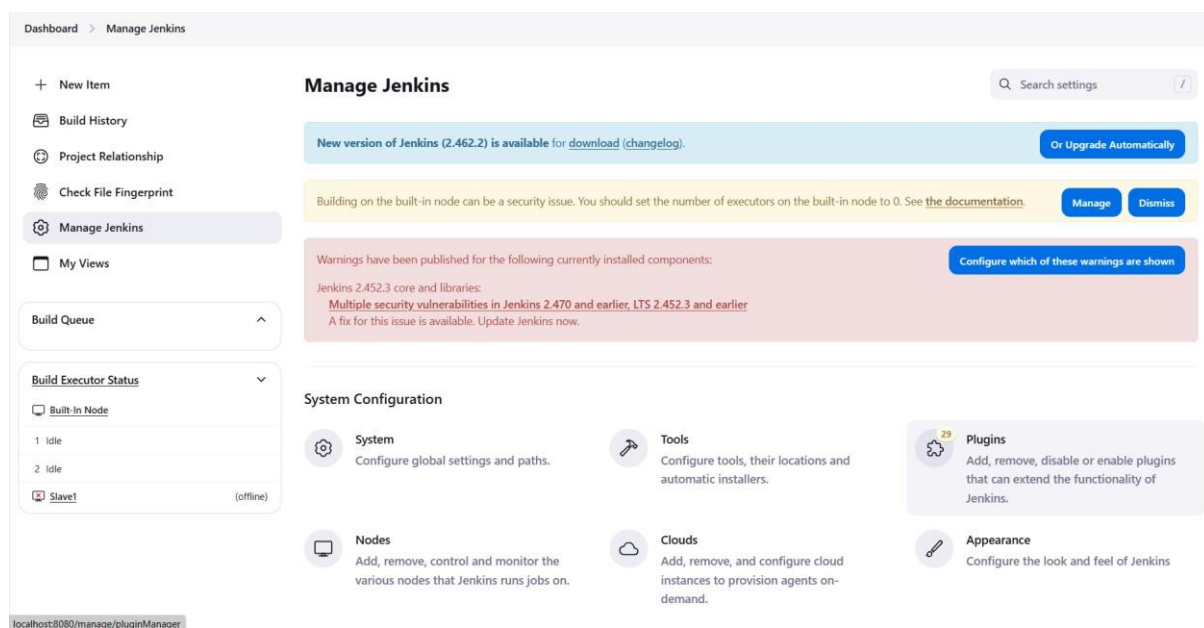
⚠️ Embedded database should be used for evaluation purposes only

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](#)



Step 4: Open Jenkins using <http://localhost:8080/> and select Manage Jenkins, then select the Plugins and select available plugins from sidebar and search for SonarQube Scanner and install it. Once installed you can view the installed plugin in installed plugins section in sidebar.



Dashboard > Manage Jenkins > Plugins

Plugins

Updates

Available plugins

Installed plugins

Advanced settings

sonar

Name	Enabled
<div>SonarQube Scanner for Jenkins 2.17.2</div> <div>This plugin allows an easy integration of SonarQube, the open source platform for Continuous Inspection of code quality.</div> <div>Report an issue with this plugin</div>	<div> <div></div> <div></div> </div>

REST API Jenkins 2.452.3

Step 5: Select Manage Jenkins, then select the System and then scroll down to SonarQube Server. Name the server as sonarqube and set the server url as <http://localhost:9000/> then click on save.

Dashboard > Manage Jenkins

New Item

Build History

Project Relationship

Check File Fingerprint

Manage Jenkins

My Views

Build Queue

Build Executor Status

Built-In Node

1 idle

2 idle

Slave! (offline)

Manage Jenkins

New version of Jenkins (2.462.2) is available for download (changelog).

Or Upgrade Automatically

Building on the built-in node can be a security issue. You should set the number of executors on the built-in node to 0. See the documentation.

Manage Dismiss

Warnings have been published for the following currently installed components:

Jenkins 2.452.3 core and libraries:

Multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier

A fix for this issue is available. Update Jenkins now.

Configure which of these warnings are shown

System Configuration

System

Configure global settings and paths.

Tools

Configure tools, their locations and automatic installers.

29 Plugins

Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Nodes

Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Clouds

Add, remove, and configure cloud instances to provision agents on-demand.

Appearance

Configure the look and feel of Jenkins

localhost:8080/manage/configure

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 ▾

Save

Apply

Step 6: Go to Jenkins Dashboard and select Manage Jenkins, then select the Tools and then scroll down to SonarQube Scanner installations. Name the sonarqube scanner as sonarqubescanner and select install automatically then click on save.

Dashboard > Manage Jenkins

+ New Item

Build History

Project Relationship

Check File Fingerprint

Manage Jenkins

My Views

Build Queue

Build Executor Status

Built-In Node

1 Idle

2 Idle

Slave1 (offline)

## Manage Jenkins

New version of Jenkins (2.462.2) is available for [download](#) ([changelog](#)).

Or Upgrade Automatically

Building on the built-in node can be a security issue. You should set the number of executors on the built-in node to 0. See [the documentation](#).

Manage

Dismiss

Warnings have been published for the following currently installed components:  
Jenkins 2.452.3 core and libraries:  
**Multiple security vulnerabilities in Jenkins 2.470 and earlier, LTS 2.452.3 and earlier**  
A fix for this issue is available. Update Jenkins now.

Configure which of these warnings are shown

### System Configuration

System

Configure global settings and paths.

Tools

Configure tools, their locations and automatic installers.

29 Plugins

Add, remove, disable or enable plugins that can extend the functionality of Jenkins.

Nodes

Add, remove, control and monitor the various nodes that Jenkins runs jobs on.

Clouds

Add, remove, and configure cloud instances to provision agents on-demand.

Appearance

Configure the look and feel of Jenkins

localhost:8080/manage/configureTools

Dashboard > Manage Jenkins > Tools

### SonarScanner for MSBuild installations

Add SonarScanner for MSBuild

---

### SonarQube Scanner installations

Add SonarQube Scanner

SonarQube Scanner

Name

sonarqubescanner

☒ Install automatically ?

Install from Maven Central

Version

SonarQube Scanner 6.2.0.4584

Add Installer

Save Apply

Step 7: Go to Jenkins dashboard and click on New Item and select Freestyle project and name it as SonarQube and then click on ok.

Enter an item name

SonarQube

» Required field

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.

Multi-branch Pipeline

OK

Step 8: For configuration, Select git and paste the following git repository in the repository url.

[https://github.com/shazforiot/MSBuild\\_firstproject](https://github.com/shazforiot/MSBuild_firstproject)

This is a simple Hello world project

Dashboard > SonarQube > Configuration

### Configure

- General
- Source Code Management**
- Build Triggers
- Build Environment
- Build Steps
- Post-build Actions

#### Source Code Management

☐ None

☒ **Git** ?

Repositories ?

Repository URL ?

https://github.com/shazforiot/MSBuild\_firstproject.git

Credentials ?

- none -

+ Add

Advanced

Add Repository

Branches to build ?

Branch Specifier (blank for 'any') ?

\*/master

Save Apply

Step 9: Under the Build steps select “Execute SonarQube Scanner” option and under Analysis Properties write the following -

sonar.projectKey=sonarqube-test

sonar.login=admin

sonar.password=sonarqube

sonar.hosturl=http://sonarqube:9000

Then click on the save button.

Dashboard > SonarQube > Configuration

### Configure

- General
- Source Code Management
- Build Triggers
- Build Environment
- Build Steps**
- Post-build Actions

#### Build Steps

**Execute SonarQube Scanner**

JDK ?

JDK to be used for this SonarQube analysis

(Inherit From Job)

Path to project properties ?

Analysis properties ?

sonar.projectKey=sonarqube-test  
sonar.login=admin  
sonar.password=sonarqube  
sonar.hosturl=http://sonarqube:9000

Additional arguments ?

JVM Options ?

Save Apply

Dashboard > SonarQube >

Status

Changes

Workspace

Build Now

Configure

Delete Project

SonarQube

Rename

SonarQube

Permalinks

Add description

Disable Project

Build History

trend

No builds

Atom feed for all

Atom feed for failures

REST API Jenkins 2.452.3

Step 10: Visit <http://localhost:9000/admin/permissions> and select the Users tab and for Administrator select the checkbox Execute Analysis.

sonarqube

Projects Issues Rules Quality Profiles Quality Gates Administration More

Administration

Configuration Security Projects System Marketplace

Global Permissions

Grant and revoke permissions to make changes at the global level. These permissions include editing Quality Profiles, executing analysis, and performing global system administration.

All Users Groups Search for users or groups...

	Administer System ?	Administer ?	Execute Analysis ?	Create ?
A Administrator admin	<input type="checkbox"/>	<input type="checkbox"/> Quality Gates <input type="checkbox"/> Quality Profiles	<input checked="" type="checkbox"/>	<input type="checkbox"/> Projects

1 of 1 shown

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 LGPL v3 Community Documentation Plugins Web API

Step 11: Now, come back to Jenkins and click on Build Now. The build is success.



Status

Changes

Console Output

View as plain text

Edit Build Information

Delete build '#4'

Timings

Git Build Data

Previous Build

Console Output

Started by user Anuprita Mhapankar

Running as SYSTEM

Building on the built-in node in workspace C:\ProgramData\Jenkins\jenkins\workspace\SonarQube

The recommended git tool is: NONE

No credentials specified

> git.exe rev-parse --resolve-git-dir C:\ProgramData\Jenkins\jenkins\workspace\SonarQube\.git # timeout=10

Fetching changes from the remote Git repository

> git.exe config remote.origin.url https://github.com/shazforiot/MSBuild\_firstproject.git # timeout=10

Fetching upstream changes from https://github.com/shazforiot/MSBuild\_firstproject.git

> git.exe --version # timeout=10

> git --version # 'git version 2.41.0.windows.3'

> git.exe fetch --tags --force --progress -- https://github.com/shazforiot/MSBuild\_firstproject.git +refs/heads/\*:refs/remotes/origin/\* # timeout=10

> git.exe rev-parse "refs/remotes/origin/master^{commit}" # timeout=10

Checking out Revision f2bc042c04c6e72427c380bcae6d6fee7b49adf (refs/remotes/origin/master)

> git.exe config core.sparsecheckout # timeout=10

> git.exe checkout -f f2bc042c04c6e72427c380bcae6d6fee7b49adf # timeout=10

Commit message: "updated"

> git.exe rev-list --no-walk f2bc042c04c6e72427c380bcae6d6fee7b49adf # timeout=10

[SonarQube] \$ C:\ProgramData\Jenkins\jenkins\tools\udson.plugins.sonar.SonarRunnerInstallation\sonarqubes scanner\bin\sonar-scanner.bat -Dsonar.host.url=http://localhost:9000 -Dsonar.projectKey=sonarqube-test -Dsonar.login=admin -Dsonar.hosturl=http://sonarqube:9000 -Dsonar.password=sonarqube -Dsonar.projectBaseDir=C:\ProgramData\Jenkins\jenkins\workspace\SonarQube

18:40:04.147 INFO Scanner configuration file:

C:\ProgramData\Jenkins\jenkins\tools\udson.plugins.sonar.SonarRunnerInstallation\sonarqubes scanner\bin\..\conf\sonar-scanner.properties

18:40:04.152 INFO Project root configuration file: NONE

18:40:04.175 INFO SonarScanner CLI 6.2.0.4584

18:40:04.177 INFO Java 21.0.4 Eclipse Adoptium (64-bit)

18:40:04.184 INFO Windows 11 10.0 amd64

Dashboard > SonarQube > #4 > Console Output

18:40:41.286 INFO ----- Run sensors on project

18:40:41.484 INFO Sensor C# [csharp]

18:40:41.485 WARN Your project contains C# files which cannot be analyzed with the scanner you are using. To analyze C# or VB.NET, you must use the SonarScanner for .NET 5.x or higher, see <https://redirect.sonarsource.com/doc/install-configure-scanner-msbuild.html>

18:40:41.485 INFO Sensor C# [csharp] (done) | time=2ms

18:40:41.486 INFO Sensor Analysis Warnings import [csharp]

18:40:41.488 INFO Sensor Analysis Warnings import [csharp] (done) | time=2ms

18:40:41.488 INFO Sensor C# File Caching Sensor [csharp]

18:40:41.489 WARN Incremental PR analysis: Could not determine common base path, cache will not be computed. Consider setting 'sonar.projectBaseDir' property.

18:40:41.490 INFO Sensor C# File Caching Sensor [csharp] (done) | time=1ms

18:40:41.491 INFO Sensor Zero Coverage Sensor

18:40:41.508 INFO Sensor Zero Coverage Sensor (done) | time=19ms

18:40:41.514 INFO SCM Publisher SCM provider for this project is: git

18:40:41.517 INFO SCM Publisher 4 source files to be analyzed

18:40:42.309 INFO SCM Publisher 4/4 source files have been analyzed (done) | time=791ms

18:40:42.317 INFO CPD Executor Calculating CPD for 0 files

18:40:42.318 INFO CPD Executor CPD calculation finished (done) | time=0ms

18:40:42.326 INFO SCM revision ID 'f2bc042c04c6e72427c380bcae6d6fee7b49adf'

18:40:42.522 INFO Analysis report generated in 181ms, dir size=201.1 kB

18:40:42.588 INFO Analysis report compressed in 63ms, zip size=22.3 kB

18:40:42.876 INFO Analysis report uploaded in 283ms

18:40:42.880 INFO ANALYSIS SUCCESSFUL, you can find the results at: <http://localhost:9000/dashboard?id=sonarqube-test>

18:40:42.881 INFO Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report

18:40:42.882 INFO More about the report processing at <http://localhost:9000/api/ce/task?id=d10eb30d-ebdd-4bb2-b564-0aa4ea71b0f2>

18:40:42.916 INFO Analysis total time: 25.189 s

18:40:42.926 INFO SonarScanner Engine completed successfully

18:40:43.027 INFO EXECUTION SUCCESS

18:40:43.029 INFO Total time: 38.885s

Finished: SUCCESS

REST API Jenkins 2.452.3

Step 12: Visit the following URL to see the result - <http://localhost:9000/dashboard?id=sonarqube-test&codeScope=overall>

localhost:9000/dashboard?id=sonarqube-test&codeScope=overall

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

sonarqube-test

main

OverviewIssuesSecurity HotspotsMeasuresCodeActivityProject SettingsProject Information

main

Version not providedSet as homepage

Quality Gate

Passed

Last analysis 14 minutes ago

The last analysis has warnings. See details

New Code

Overall Code

Security

0 Open issues

0 H0 M0 L

A

Reliability

0 Open issues

0 H0 M0 L

A

Maintainability

0 Open issues

0 H0 M0 L

A

Accepted issues

0

Valid issues that were not fixed

Coverage

On 0 lines to cover.

Duplications

0.0%

On 86 lines.

Security Hotspots