

Lab Assignment 6

AIM: To perform static analysis on Python programs using SonarQube SAST process.

LO4: To identify and remediate application vulnerabilities earlier and help integrate security in the development process using SAST Techniques.

THEORY:

SonarQube:

Overview: SonarQube is an open-source platform for continuous inspection of code quality. It is used to analyze and measure code quality and security issues in a codebase.

Features:

Static Code Analysis: SonarQube scans source code to identify bugs, code smells, and security vulnerabilities.

Continuous Integration: It integrates seamlessly with CI/CD pipelines, providing automated code analysis during the development process.

Security Analysis: While it primarily focuses on code quality, it also has some security rules to catch common security issues.

Maintainability Metrics: SonarQube provides maintainability metrics and helps teams understand code complexity and maintainability.

Dashboard and Reporting: It offers dashboards and reports for tracking code quality and issues over time.

Use Case: SonarQube is used for improving code quality, maintainability, and to catch some common code security issues. It's more about general code quality and development best practices.

SAST (Static Application Security Testing):

Overview: SAST is a security testing method that analyzes source code, bytecode, or binary code for vulnerabilities without executing the application. It is primarily focused on identifying security issues and vulnerabilities in the code.

Features:

Code Scanning: SAST tools examine the source code or compiled code to identify potential security vulnerabilities, such as SQL injection, cross-site scripting, and more.

Early Detection: SAST is used early in the development process to find security issues before they can be exploited.

Language Support: SAST tools support various programming languages and frameworks.

Integration: They can be integrated into CI/CD pipelines to automatically scan code before deployment.

Use Case: SAST is used for finding and fixing security vulnerabilities in code. It helps secure applications by identifying potential security threats early in the development lifecycle.

1. INSTALL sonarqube (docker images) and sonarscanner zip file from <https://docs.sonarsource.com/sonarqube/latest/analyzing-sourcecode/scanners/sonarscanner/> and set up config file as given in docs.

```
Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Pratik Arrote>docker pull sonarqube
Using default tag: latest
latest: Pulling from library/sonarqube
43f89b94cd7d: Pull complete
50431c77a77b: Pull complete
dfd8e860e672: Pull complete
637e2db99ae6: Pull complete
7de1c2853278: Pull complete
d2152ffce821: Pull complete
519cf218564f: Pull complete
Digest: sha256:c6c8096375002d4cb2ef64b89a2736ad572812a87a2917d92e7e59384b9f6f65
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

C:\Users\Pratik Arrote>docker pull sonarsource/sonar-scanner-cli
Using default tag: latest
latest: Pulling from sonarsource/sonar-scanner-cli
9398808236ff: Pull complete
4f4fb700ef54: Pull complete
3cd77fb28e46: Pull complete
f78b288abc31: Pull complete
Digest: sha256:494ecc3b5b1ee1625bd377b3905c4284e4f0cc155cff397805a244dee1c7d575
Status: Downloaded newer image for sonarsource/sonar-scanner-cli:latest
docker.io/sonarsource/sonar-scanner-cli:latest

What's Next?
View a summary of image vulnerabilities and recommendations → docker scout quickview sonarsource/sonar-scanner-cli
```

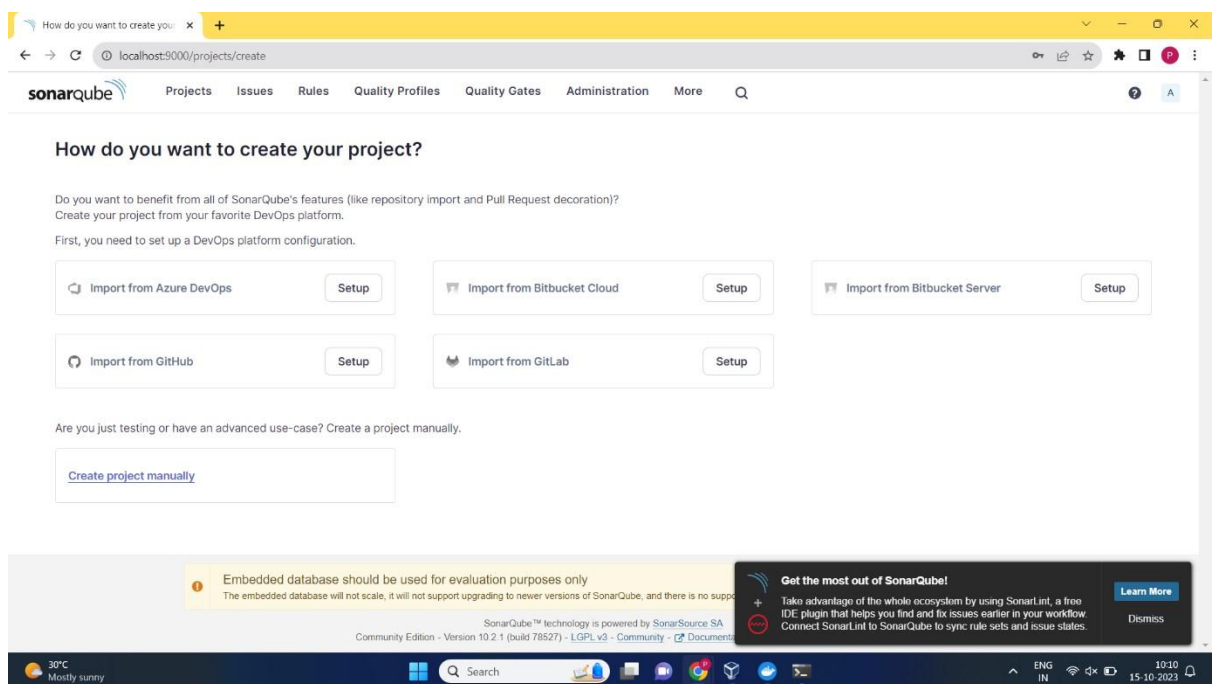
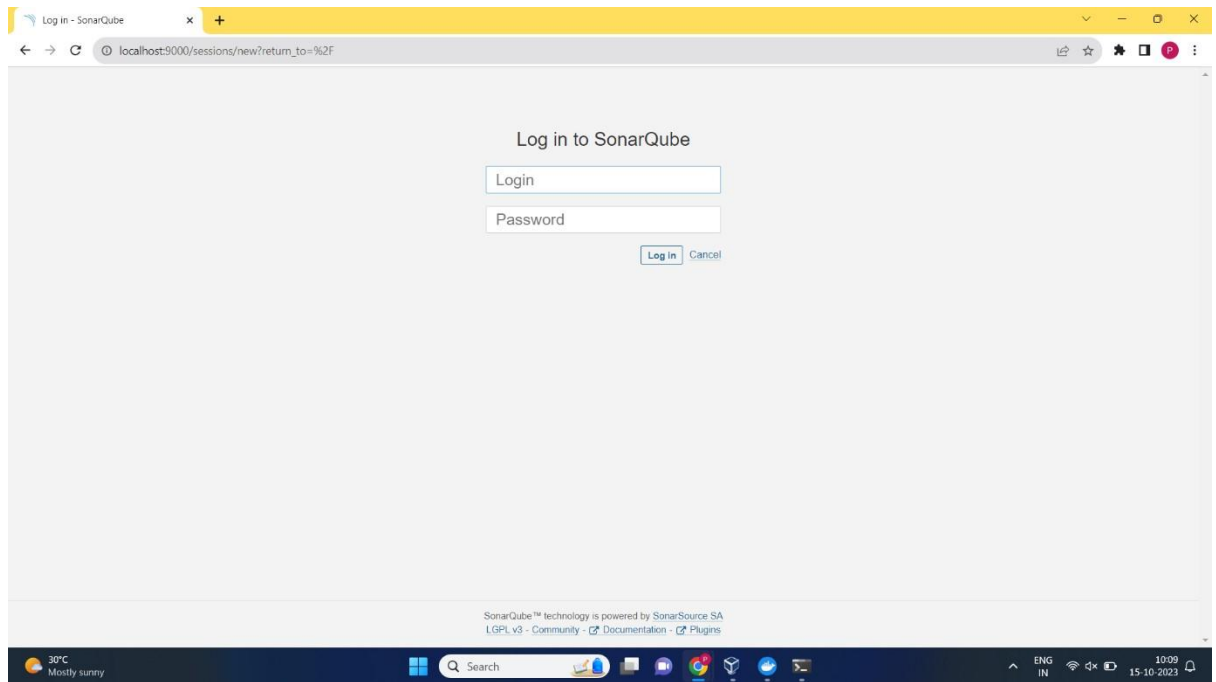
2. Spin up the container

```
C:\Users\Pratik Arrote>docker run -d --name sonarqube -e SONAR_ES_BOOTSTRAP_CHECKS_DISABLE=true -p 9000:9000 sonarqube:latest
f3630dbc2ffa6e5598ad922085026400a1f9f1564416b0606b5348000f6d1377

C:\Users\Pratik Arrote>docker images
REPOSITORY          TAG          IMAGE ID      CREATED        SIZE
sonarqube            latest       3183d6818c6e  42 hours ago  716MB
sample-web-app       latest       713c7cdaaf78  2 weeks ago   42.7MB
myimage              latest       438bb56a50a3  2 weeks ago   122MB
sonarsource/sonar-scanner-cli latest       2f384fb1bbd5  5 weeks ago   358MB
ubuntu               latest       c6b84b685f35  8 weeks ago   77.8MB
hello-world          latest       9c7a54a9a43c  5 months ago  13.3kB

C:\Users\Pratik Arrote>docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED        STATUS        PORTS                    NAMES
f3630dbc2ffa   sonarqube:latest "/opt/sonarqube/dock..." 27 minutes ago Up 27 minutes 0.0.0.0:9000->9000/tcp   sonarqube
```

3. Open <http://localhost:9000> on the browser. Enter login and password both as “admin” and then set up new password.



4. Create a project

Create a project

localhost:5000/projects/create?mode=manual

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

Create a project

Project display name *

sonarPythonProgram1

Up to 255 characters. Some scanners might override the value you provide.

Project key *

sonarPythonProgram1

The project key is a unique identifier for your project. It may contain up to 400 characters. Allowed characters are alphanumeric, '-' (dash), '_' (underscore), ':' (period) and ':' (colon), with at least one non-digit.

Main branch name *

main

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

Next

Embedded database should be used for evaluation purposes only

Get the most out of SonarQube!

Create a project

localhost:5000/projects/create?mode=manual&setncd=true

sonarqube

ProjectsIssuesRulesQuality ProfilesQuality GatesAdministrationMore

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.

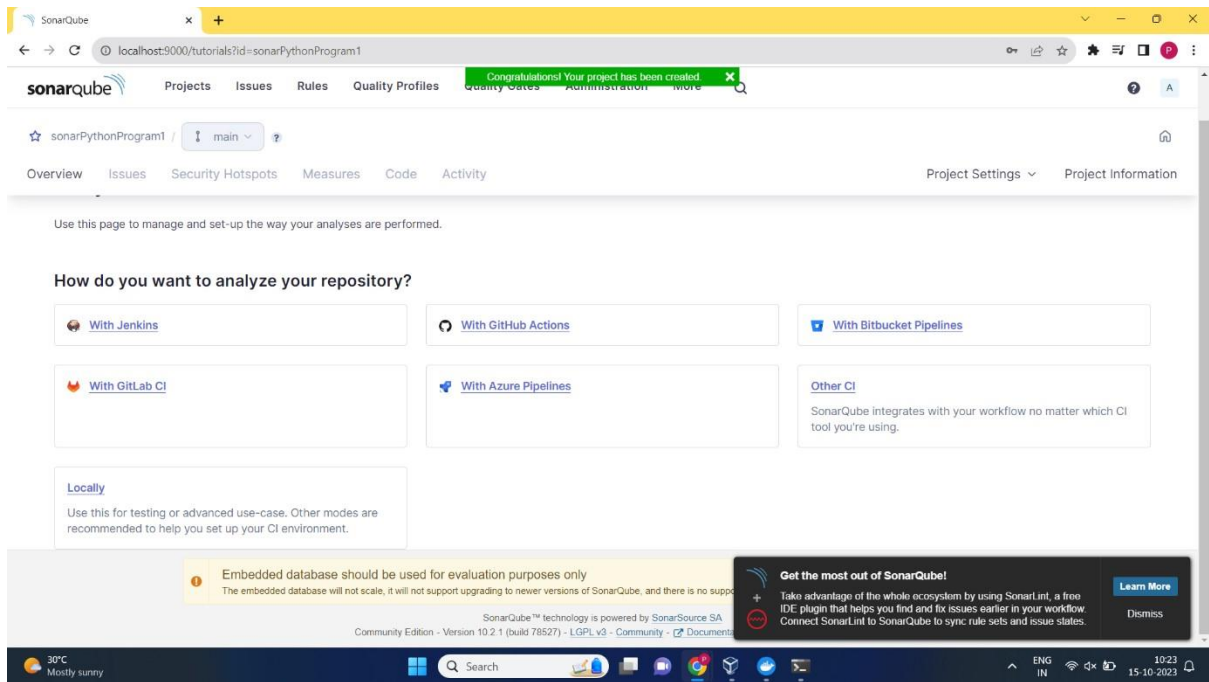
Recommended for projects following regular versions or releases.

☐ Number of days

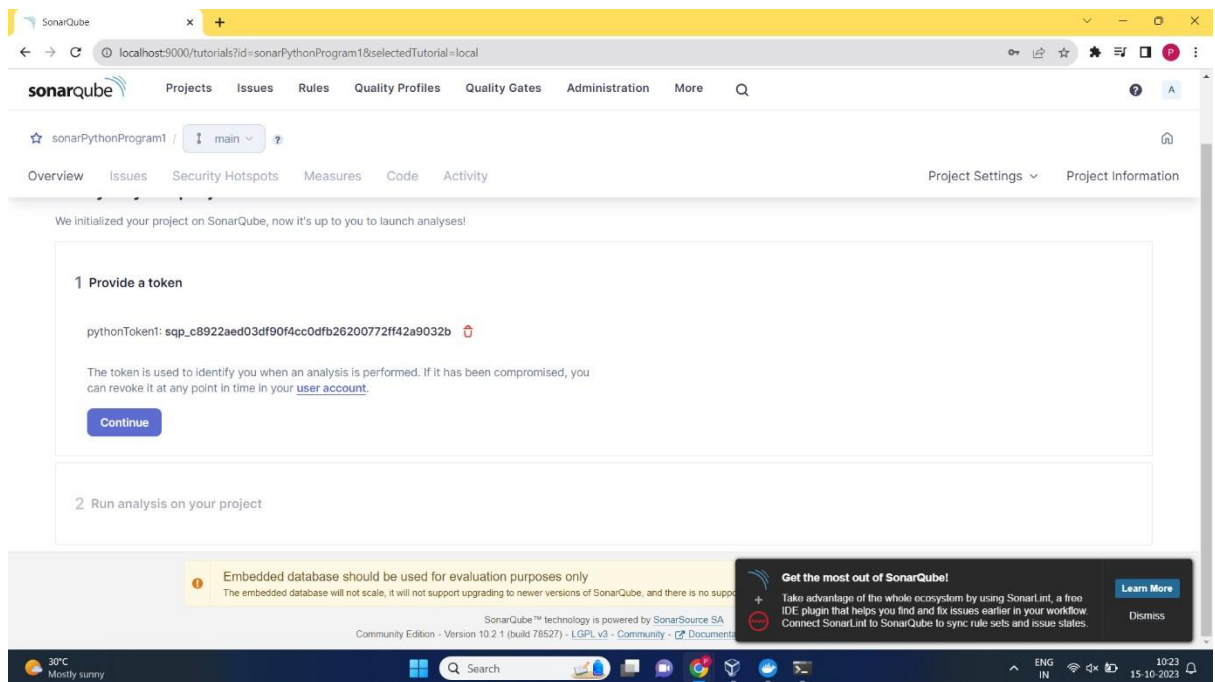
Any code that has changed in the last x days is considered new code. If no action is taken on a new issue code.

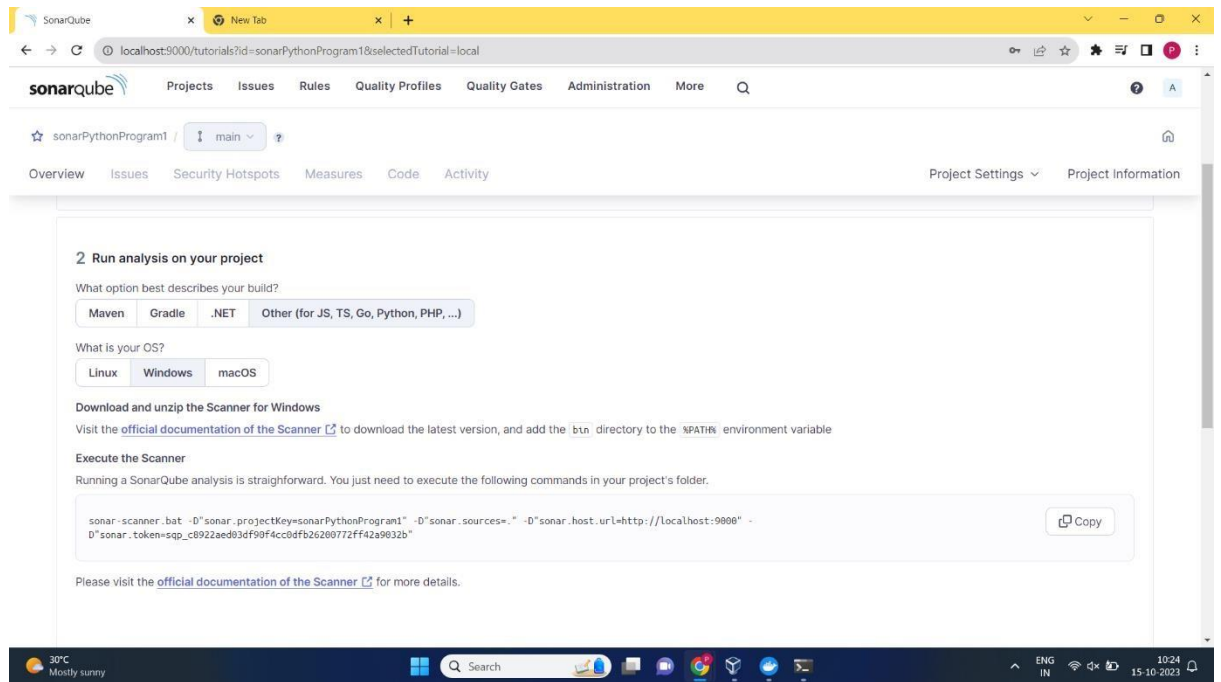
Recommended for projects following continuous delivery.

Get the most out of SonarQube!



5. Provide token





6. Enter the following command

```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22621.2428]
(c) Microsoft Corporation. All rights reserved.

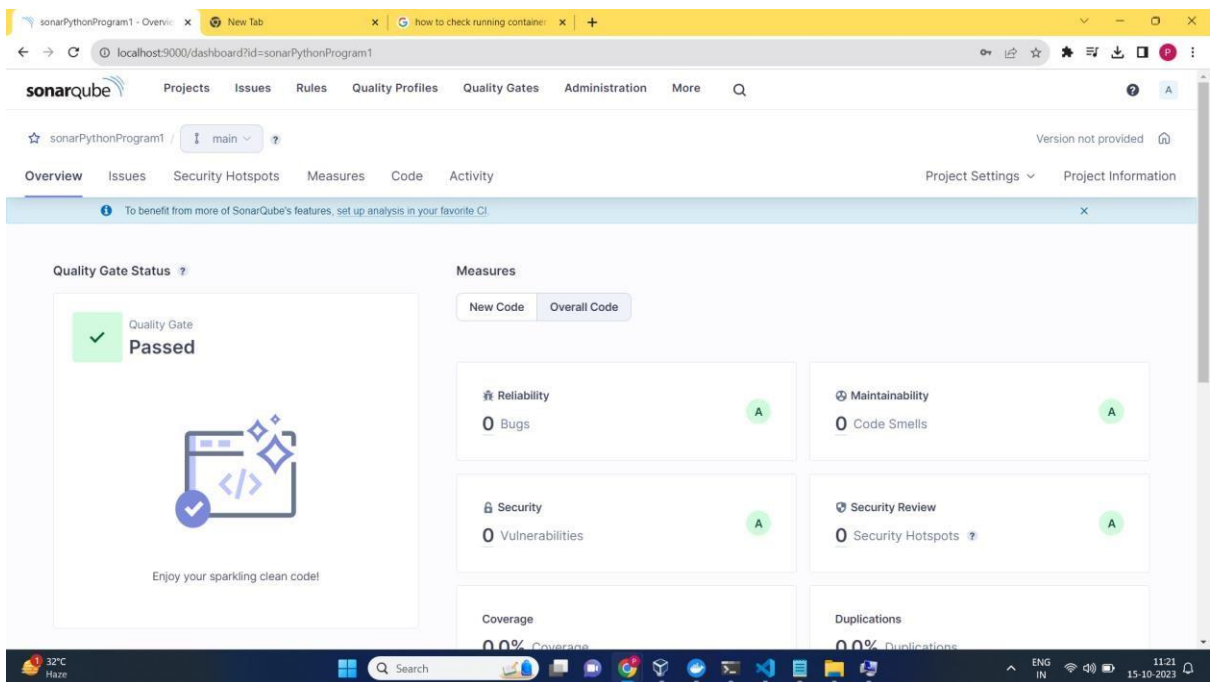
C:\Program Files\sonar-scanner-5.0.1.3006-windows\bin>sonar-scanner.bat -D"sonar.projectKey=sonarPythonProgram1" -D"sonar.sources=C:\Users\Pratik Arote\Desktop\sastPython" -D"sonar.host.url=http://localhost:9000" -D"sonar.token=sqp_c8922aed03df90f4cc0dfb26208772ff42a9032b" -D"sonar.projectBaseDir=C:\Users\Pratik Arote\Desktop\sastPython"
INFO: Scanner configuration file: C:\Program Files\sonar-scanner-5.0.1.3006-windows\bin\..conf\sonar-scanner.propertiesINFO: Project root configuration file: NONE
INFO: SonarScanner 5.0.1.3006
INFO: Java 17.0.7 Eclipse Adoptium (64-bit)
INFO: Windows 11 10.0 amd64
INFO: User cache: C:\Users\Pratik Arote\.sonar\cache
INFO: Analyzing on SonarQube server 10.2.1.78527
INFO: Default locale: "en_IN", source code encoding: "windows-1252" (analysis is platform dependent)
INFO: Load global settings
INFO: Load global settings (done) | time=588ms
INFO: Server id: 1d7b11e-AVxofDZoQL--ruFd2_S5
INFO: User cache: C:\Users\Pratik Arote\.sonar\cache
INFO: Load/download plugins
INFO: Load plugins index
INFO: Load plugins index (done) | time=338ms
INFO: Load/download plugins (done) | time=8251ms
INFO: Process project properties
INFO: Process project properties (done) | time=40ms
INFO: Execute project builders
INFO: Execute project builders (done) | time=7ms
INFO: Project key: sonarPythonProgram1
INFO: Base dir: C:\Users\Pratik Arote\Desktop\sastPython
INFO: Working dir: C:\Users\Pratik Arote\Desktop\sastPython\.scannerwork
INFO: Load project settings for component key: 'sonarPythonProgram1'
INFO: Load project settings for component key: 'sonarPythonProgram1' (done) | time=122ms
WARN: SCM provider autodetection failed. Please use "sonar.scm.provider" to define SCM of your project, or disable the SCM Sensor in the project settings.
INFO: Load quality profiles
INFO: Load quality profiles (done) | time=597ms
INFO: Load active rules
INFO: Load active rules (done) | time=7984ms
INFO: Load analysis cache
INFO: Load analysis cache (404) | time=60ms
INFO: Load project repositories
INFO: Load project repositories (done) | time=295ms
  
```



```
C:\Windows\System32\cmd.exe x + v
INFO: Sensor VB.NET Properties [vbnet] (done) | time=2ms
INFO: Sensor IaC Docker Sensor [iac]
INFO: 0 source files to be analyzed
INFO: 0/0 source files have been analyzed
INFO: Sensor IaC Docker Sensor [iac] (done) | time=206ms
INFO: ----- Run sensors on project
INFO: Sensor Analysis Warnings import [csharp]
INFO: Sensor Analysis Warnings import [csharp] (done) | time=7ms
INFO: Sensor Zero Coverage Sensor
INFO: Sensor Zero Coverage Sensor (done) | time=47ms
INFO: SCM Publisher No SCM system was detected. You can use the 'sonar.scm.provider' property to explicitly specify it.
INFO: CPD Executor 1 file had no CPD blocks
INFO: CPD Executor Calculating CPD for 0 files
INFO: CPD Executor CPD calculation finished (done) | time=0ms
INFO: Analysis report generated in 253ms, dir size=136.5 kB
INFO: Analysis report compressed in 48ms, zip size=17.5 kB
INFO: Analysis report uploaded in 201ms
INFO: ANALYSIS SUCCESSFUL, you can find the results at: http://localhost:9000/dashboard?id=sonarPythonProgram1
INFO: Note that you will be able to access the updated dashboard once the server has processed the submitted analysis report
INFO: More about the report processing at http://localhost:9000/api/ce/task?id=AYSx47EpoQL-ruFd3M3Y
INFO: Analysis total time: 22.756 s
INFO: More about the report processing at http://localhost:9000/api/ce/task?id=AYSx47EpoQL-ruFd3M3Y
INFO: EXECUTION SUCCESS
INFO: -----
INFO: Total time: 35.565s
INFO: Final Memory: 23M/77M
INFO: -----

C:\Program Files\sonar-scanner-5.0.1.3006-windows\bin>
```

7. See the result of the test



CONCLUSION:

Here we have successfully performed static analysis of python programs.