

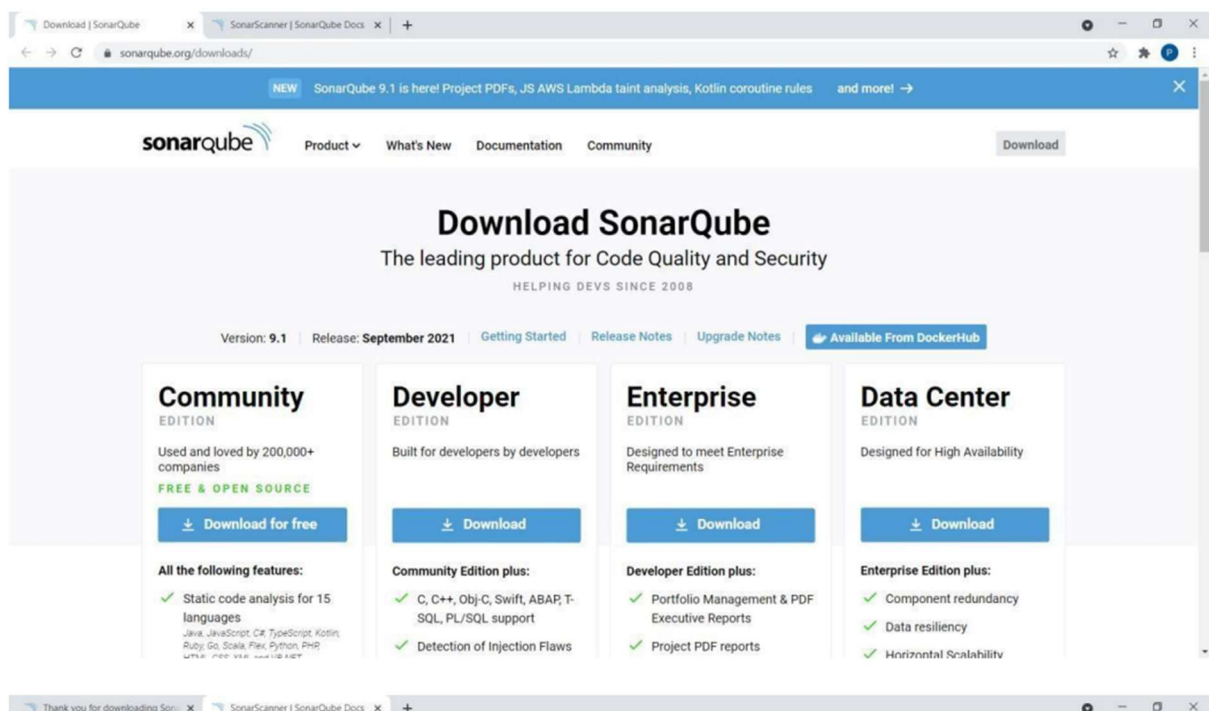
Assignment 7

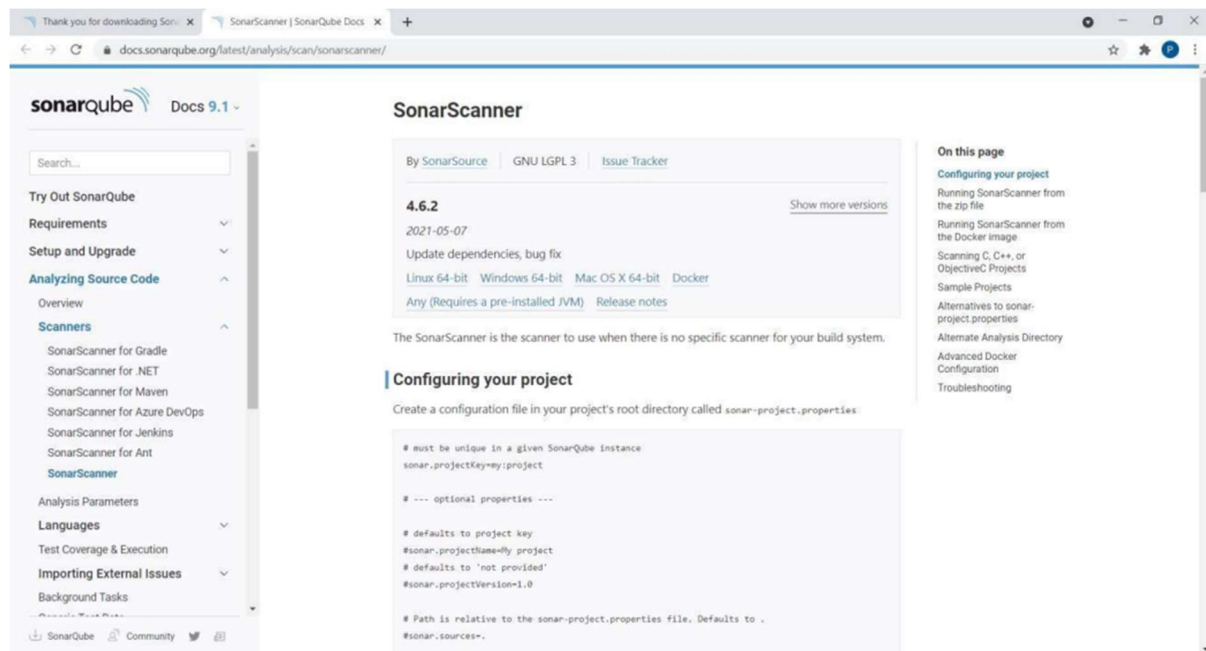
Aim: TO perform static analysis on python programs using SonarCube SAST processes

LO Mapped: L04

Theory:

Download and Sonar Scanner

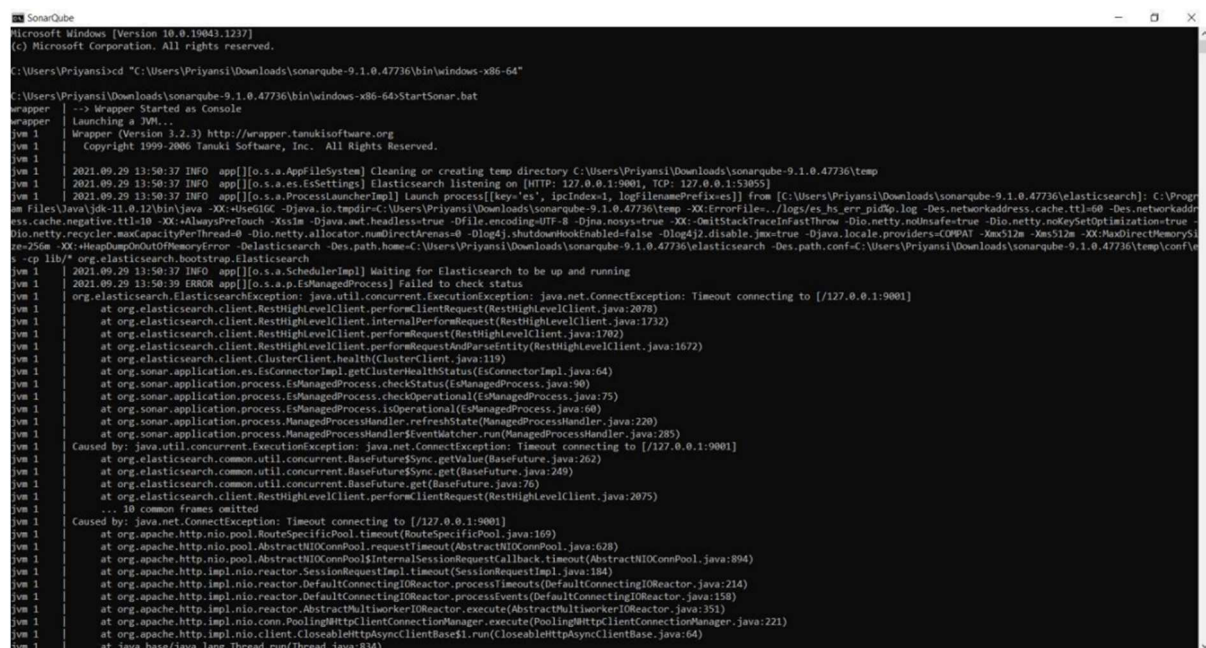


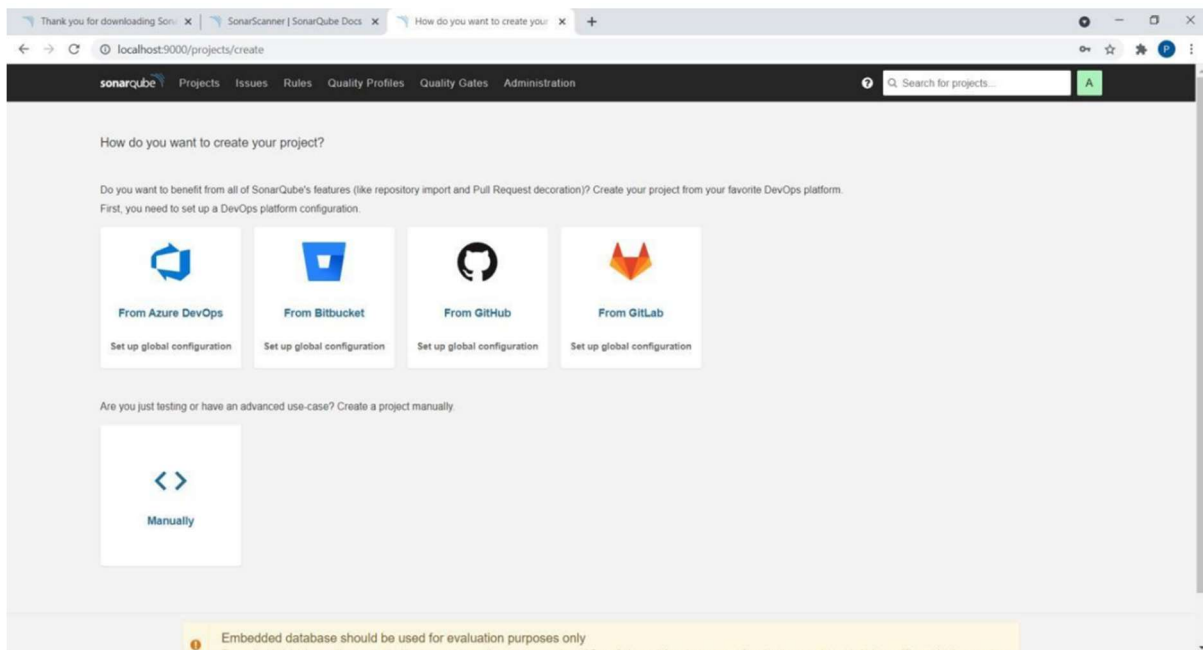
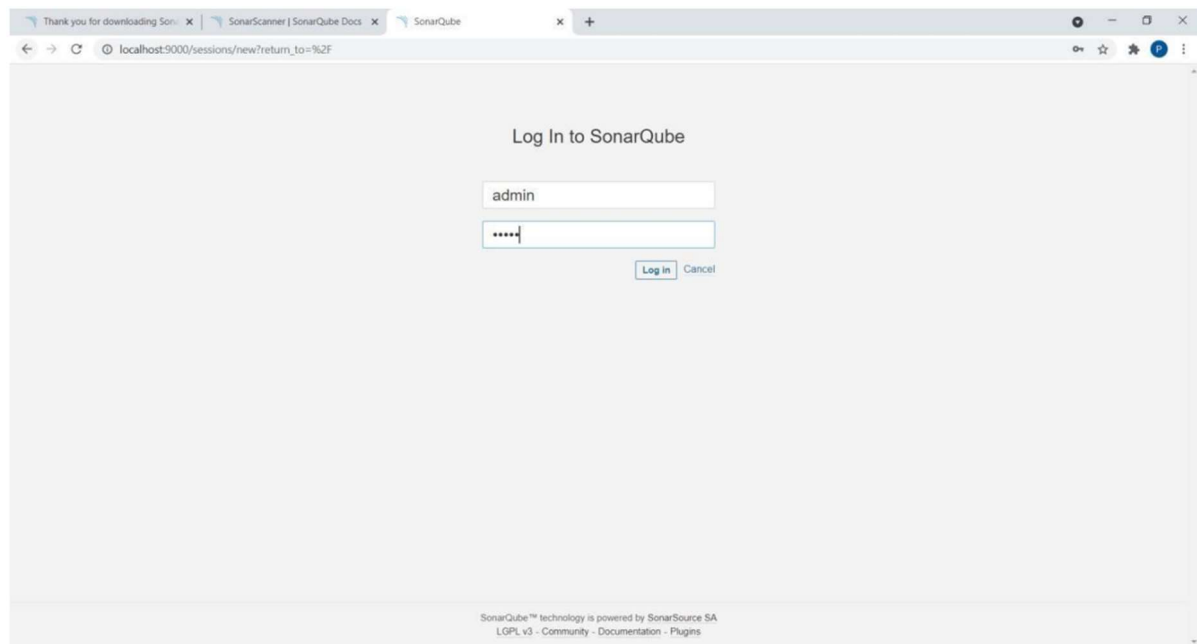


After downloading, set Environment Variables. Add "sonarqube-9.1.0.47736\bin" to Path.

Open command prompt. Run commands:

- `cd "sonarqube-9.1.0.47736\bin\windows-x86-64"`
- `StartSonar.bat`





Click on Create a project Manually.

Thank you for downloading SonarScanner | SonarQube Docs | How do you want to create your project | +

localhost:9000/projects/create?mode=manual

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

Search for projects...

Create a project

All fields marked with * are required

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.

Set Up

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 - Version 9.1 (build 47736) - LGPL v3 - Community - Documentation - Plugins - Web API - About

Give any Project display name.

Thank you for downloading SonarScanner | SonarQube Docs | sonarPythonProgram1 | +

localhost:9000/dashboard?id=sonarPythonProgram1

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

Search for projects...

sonarPythonProgram1 master

Overview Issues Security Hotspots Measures Code Activity

Project Settings Project information

How do you want to analyze your repository?

Do you want to integrate with your favorite CI? Choose one of the following tutorials.

With Jenkins With GitHub Actions With Bitbucket Pipelines With GitLab CI With Azure Pipelines Other CI

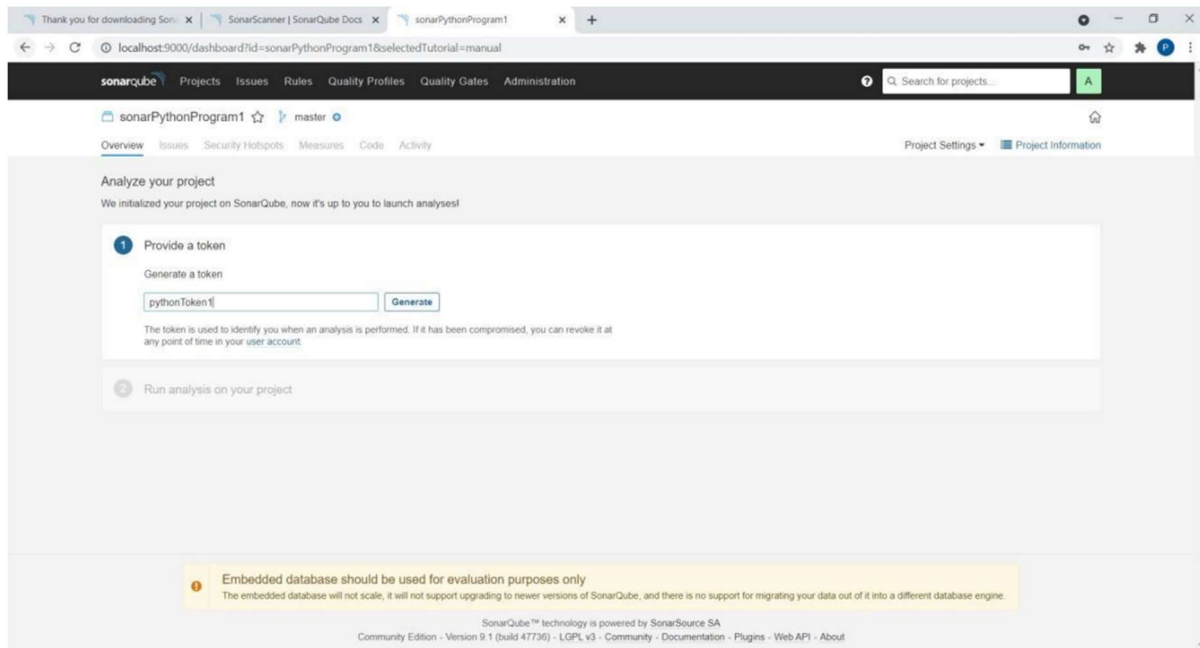
Are you just testing or have an advanced use-case? Analyze your project locally

Locally

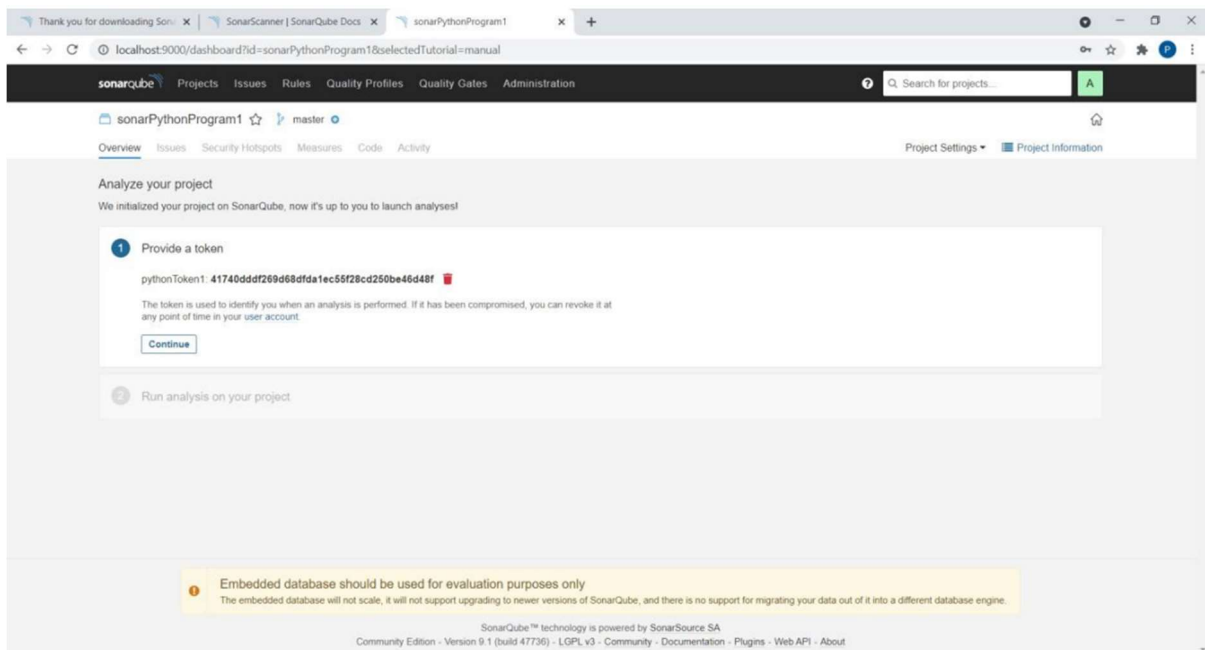
Embedded database should be used for evaluation purposes only
The embedded database will not scale, it will not support upgrading to newer versions of SonarQube, and there is no support for migrating your data out of it into a different database engine.

SonarQube™ technology is powered by SonarSource SA
Community Edition - Version 9.1 (build 47736)

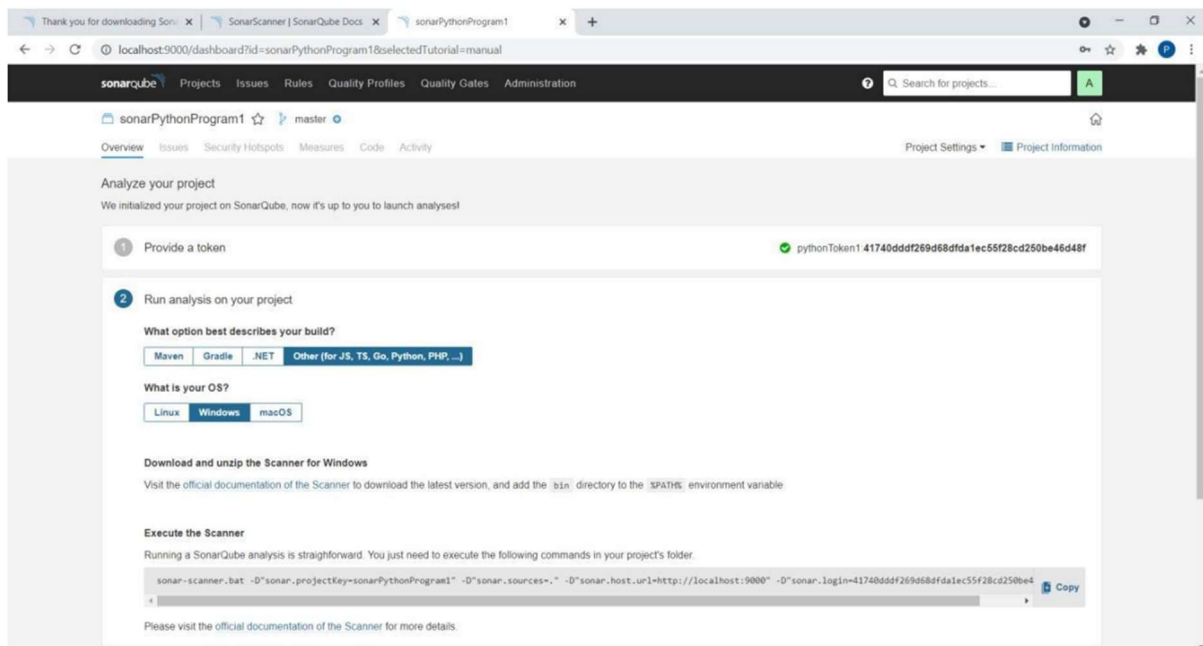
Click on Locally.



Give any name to token and click on Generate.



Click on Continue.



Save a Python program in a folder.

```
class Solution(object):
```

```
def romanToInt(self, s):
```

```
    roman =
```

```
    num =
```

```
    while i < len(s):
```

```
        if i+1<len(s) and s[i:i+2] in roman:
```

```
            num+=roman[s[i:i+2]]
```

```
        else:
```

```
            #print(i)
```

```
            num+=roman[s[i]]
```

```
    return num
```

```
obl = Solution()
```

```
print(obl.l")
```

```
print(obl . l")
```

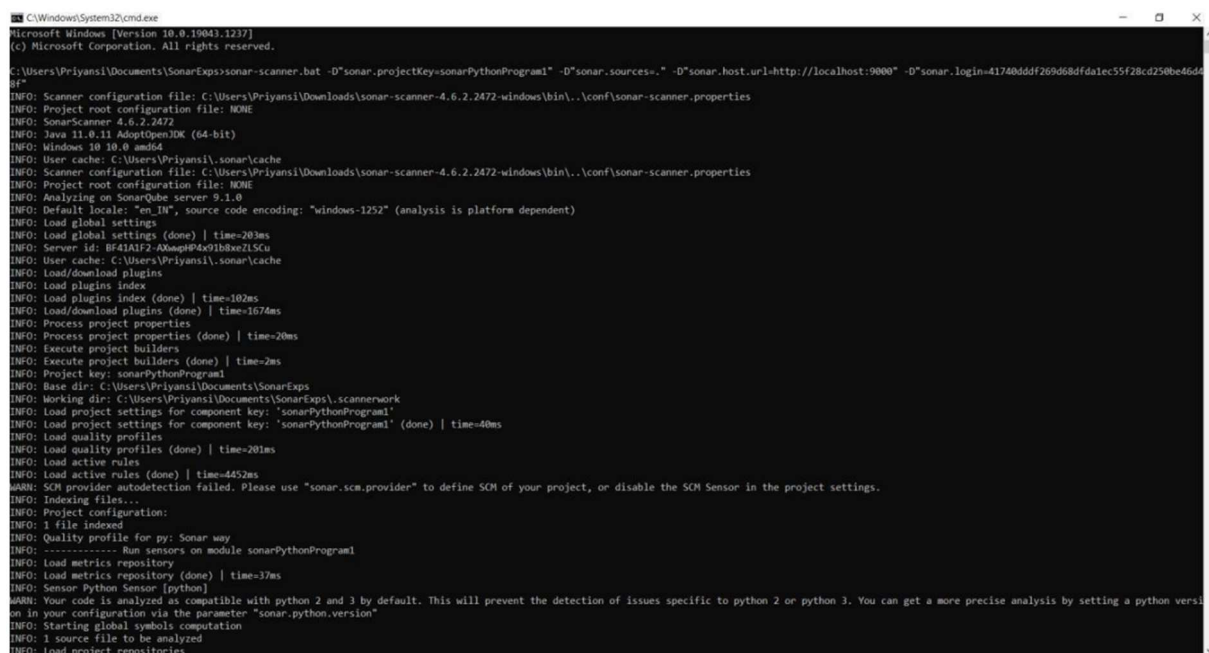
Open command prompt in this folder and Run program using copied command.

```
sonar-scanner.bat -D"sonar.projectKey=<YourDisplayName>"
```

```
-
```

```
D"sonar.sources=." -D"sonar.host.url=http://localhost:9000" -
```

```
D"sonar.login=<YourTokenGeneratedID>'
```



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.1237]
(c) Microsoft Corporation. All rights reserved.

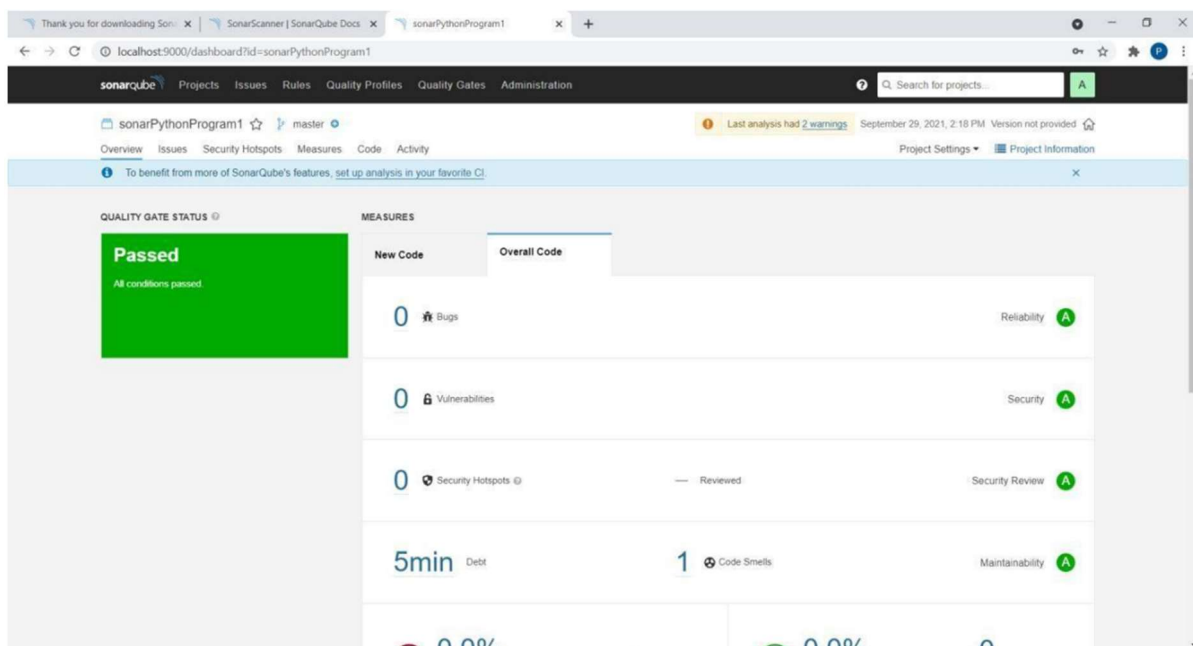
C:\Users\Priyansi\Documents\SonarExps>sonar-scanner.bat -D"sonar.projectKey=sonarPythonProgram1" -D"sonar.sources=." -D"sonar.host.url=http://localhost:9000" -D"sonar.login=41740dddf269d68dfdalec55f28cd250be46da4bf"

INFO: Scanner configuration file: C:\Users\Priyansi\Downloads\sonar-scanner-4.6.2.2472-windows\bin\..\conf\sonar-scanner.properties
INFO: Project root configuration file: NONE
INFO: SonarScanner 4.6.2.2472
INFO: Java 11.0.11 AdoptOpenJDK (64-bit)
INFO: Windows 10 10.0 amd64
INFO: User cache: C:\Users\Priyansi\sonar\cache
INFO: Scanner configuration file: C:\Users\Priyansi\Downloads\sonar-scanner-4.6.2.2472-windows\bin\..\conf\sonar-scanner.properties
INFO: Project root configuration file: NONE
INFO: Analyzing on SonarQube server 9.1.0
INFO: Default locale: "en_IN", source code encoding: "windows-1252" (analysis is platform dependent)
INFO: Load global settings
INFO: Load global settings (done) | time=203ms
INFO: Server id: BF43A1P2-A0aap84x01b8xe2L5Cu
INFO: User cache: C:\Users\Priyansi\sonar\cache
INFO: Load/download plugins
INFO: Load plugins index
INFO: Load plugins index (done) | time=102ms
INFO: Load/download plugins (done) | time=167ms
INFO: Process project properties
INFO: Process project properties (done) | time=20ms
INFO: Execute project builders
INFO: Execute project builders (done) | time=2ms
INFO: Project key: sonarPythonProgram1
INFO: Base dir: C:\Users\Priyansi\Documents\SonarExps
INFO: Working dir: C:\Users\Priyansi\Documents\SonarExps\scannerwork
INFO: Load project settings for component key: 'sonarPythonProgram1'
INFO: Load project settings for component key: 'sonarPythonProgram1' (done) | time=40ms
INFO: Load quality profiles
INFO: Load quality profiles (done) | time=201ms
INFO: Load active rules
INFO: Load active rules (done) | time=4452ms
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: Project configuration:
INFO: 1 file indexed
INFO: Quality profile for py: Sonar way
INFO: ----- Run sensors on module sonarPythonProgram1
INFO: Load metrics repository
INFO: Load metrics repository (done) | time=37ms
INFO: Sensor Python Sensor [python]
WARN: Your code is analyzed as compatible with python 2 and 3 by default. This will prevent the detection of issues specific to python 2 or python 3. You can get a more precise analysis by setting a python version in your configuration via the parameter "sonar.python.version"
INFO: Starting global symbols computation
INFO: 1 source file to be analyzed
INFO: Load project repositories
```



```
C:\Windows\System32\cmd.exe
INFO: Sensor HTML [web] (done) | time=2ms
INFO: Sensor VB.NET Project Type Information [vbnet] (done) | time=1ms
INFO: Sensor VB.NET Project Type Information [vbnet] (done) | time=1ms
INFO: Sensor VB.NET Analysis Log [vbnet] (done) | time=12ms
INFO: Sensor VB.NET Properties [vbnet] (done) | time=0ms
INFO: Sensor VB.NET Properties [vbnet] (done) | time=0ms
INFO: Run sensors on project
INFO: Sensor Zero Coverage Sensor
INFO: Sensor Zero Coverage Sensor (done) | time=12ms
INFO: SCM Publisher No SCM system was detected. You can use the 'sonar.scm.provider' property to explicitly specify it.
INFO: CPD Executor Calculating CPD for 1 file
INFO: CPD Executor CPD calculation finished (done) | time=10ms
INFO: Analysis report generated in 59ms, dir size=103.9 kB
INFO: Analysis report compressed in 19ms, zip size=14.7 kB
INFO: Analysis report uploaded in 70ms
INFO: ANALYSIS SUCCESSFUL, you can browse 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=AWawvY1hx91b8xeZLXH1
INFO: Analysis total time: 7.502 s
INFO: -----
INFO: EXECUTION SUCCESS
INFO: -----
INFO: Total time: 10.887s
INFO: Final Memory: 7M/30M
INFO: -----
C:\Users\Priyansh\Documents\SonarExps>
```

Given below is the inspection of code quality to perform automatic reviews with static analysis of code to detect bugs, code smells, and security vulnerabilities.



The top screenshot shows the SonarQube 'Overview' page for the project 'sonarPythonProgram1'. The page includes a navigation bar with tabs for Overview, Issues, Security Hotspots, Measures, Code, and Activity. The main content area displays several key metrics: 0 Vulnerabilities, 0 Security Hotspots, 5min Debt, 1 Code Smells, 0.0% Coverage (on 15 Lines to cover), 0.0% Duplications (on 16 Lines), and 0 Duplicated Blocks. The bottom section shows the 'ACTIVITY' tab with a dropdown menu and a date selector.

The bottom screenshot shows the 'Issues' page for the same project. It features a left sidebar with filters for Type (Bug, Vulnerability, Code Smell) and Severity (Blocker, Critical, Major, Minor, Info). The main area displays a list of issues, with one issue selected: 'Rename method "romanToInt" to match the regular expression "[a-z][a-z0-9_]*\$'. Why is this an issue?'. The issue is categorized as a 'Code Smell' with a 'Minor' severity and is currently 'Open' and 'Not assigned'.

Press "Ctrl + C" to stop the server.

SAST processes.