

ASSIGNMENT-7

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

LO MAPPED: LO4

THEORY:

SonarQube is a universal tool for static code analysis that has become more or less the industry standard. Keeping code clean, simple, and easy to read is also a lot easier with SonarQube.

What is SonarQube?

SonarQube is an open-source platform developed by SonarSource for continuous inspection of code quality. Sonar does static code analysis, which provides a detailed report of bugs, code smells, vulnerabilities, code duplications. It supports 25+ major programming languages through built-in rulesets and can also be extended with various plugins.

Benefits of SonarQube

Sustainability - Reduces complexity, possible vulnerabilities, and code duplications, optimising the life of applications. Increase productivity - Reduces the scale, cost of maintenance, and risk of the application; as such, it removes the need to spend more time changing the code

☐ Quality code - Code quality control is an inseparable part of the process of software development.

☐ Detect Errors - Detects errors in the code and alerts developers to fix them automatically before submitting them for output.

☐ Increase consistency - Determines where the code criteria are breached and enhances the quality

☐ Business scaling - No restriction on the number of projects to be evaluated

☐ Enhance developer skills - Regular feedback on quality problems helps developers to improve their coding skills

Why SonarQube?

Developers working with hard deadlines to deliver the required functionality to the customer. It is so important for developers that many times they compromise with the code quality, potential bugs, code duplications, and bad distribution of complexity.

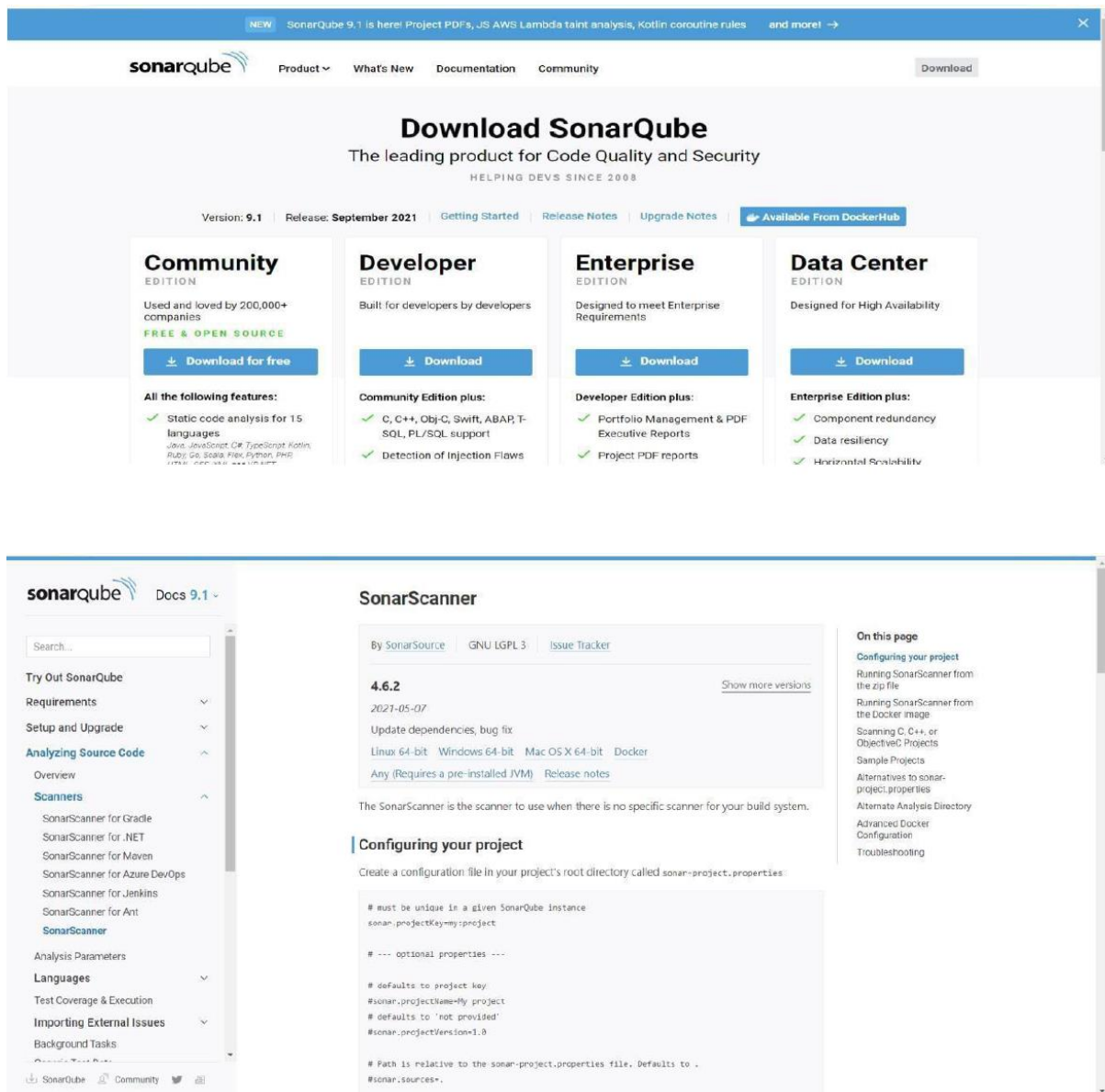
Additionally, they tend to leave unused variables, methods, etc. In this scenario, the code would work in the desired way.

To avoid these issues in code, developers should always follow the good coding practice, but sometimes it is not possible to follow the rules and maintain the good quality as there may be many reasons.

In order to achieve continuous code integration and deployment, developers need a tool that not only works once to check and tell them the problems in the code but also to track and control the code to check continuous code quality. To satisfy all these requirements, here comes SonarQube in the picture.

STEPS:

Download SonarQube and Sonar Scanner



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

Open command prompt. Run commands:

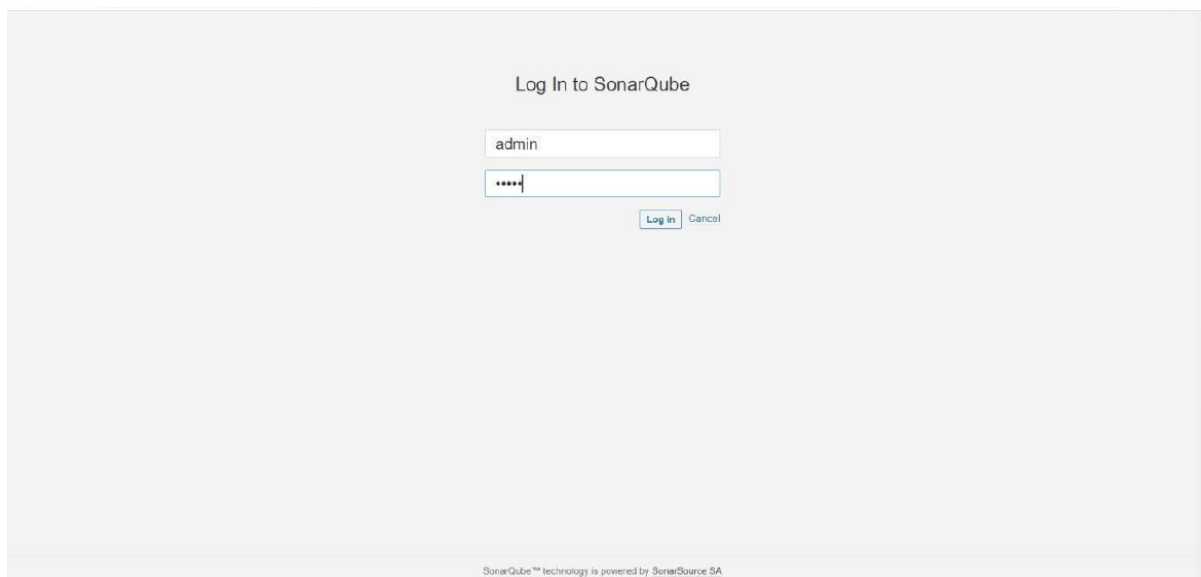
- cd "sonarqube-9.1.0.47736\bin\windows-x86-64"
- StartSonar.bat


```
Command Prompt
C:\Users\Priyansi\Downloads\sonar-scanner-4.6.2.2472-windows\bin>sonar-scanner
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: -----
INFO: EXECUTION FAILURE
INFO: -----
INFO: Total time: 3.958s
INFO: Final Memory: 5M/20M
INFO: -----
ERROR: Error during SonarScanner execution
ERROR: Not authorized. Analyzing this project requires authentication. Please provide a user token in sonar.login or other credentials in sonar.login and sonar.password.
ERROR:
ERROR: Re-run SonarScanner using the -X switch to enable full debug logging.

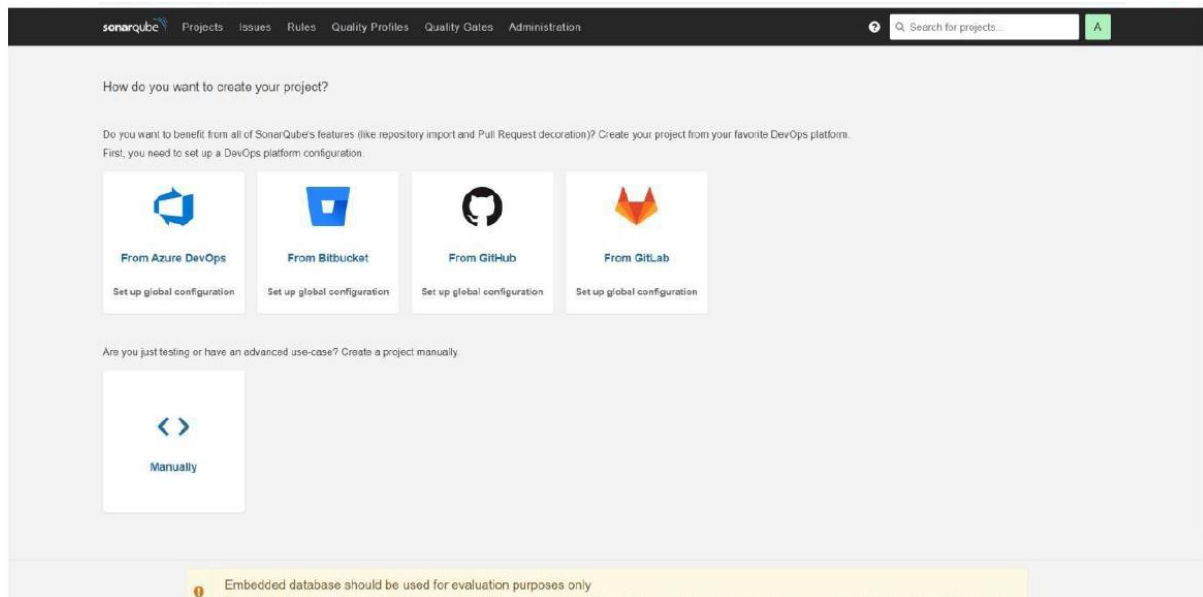
C:\Users\Priyansi\Downloads\sonar-scanner-4.6.2.2472-windows\bin>
```

Server up and running on **localhost:9000**

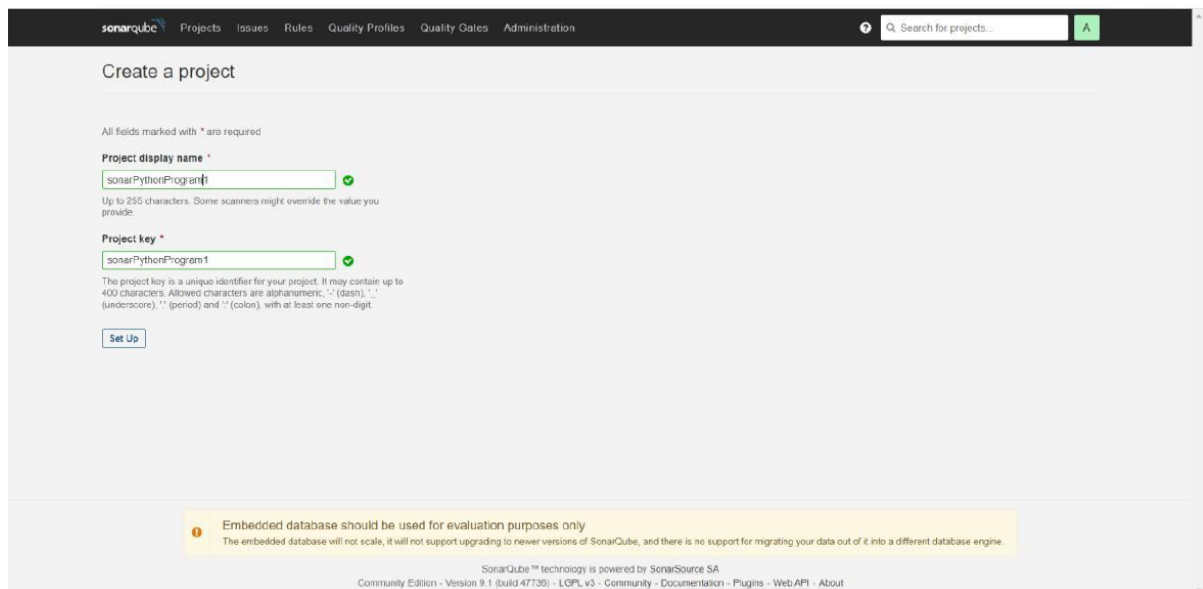
Login using credentials as User: admin and Password: admin and Set a new password



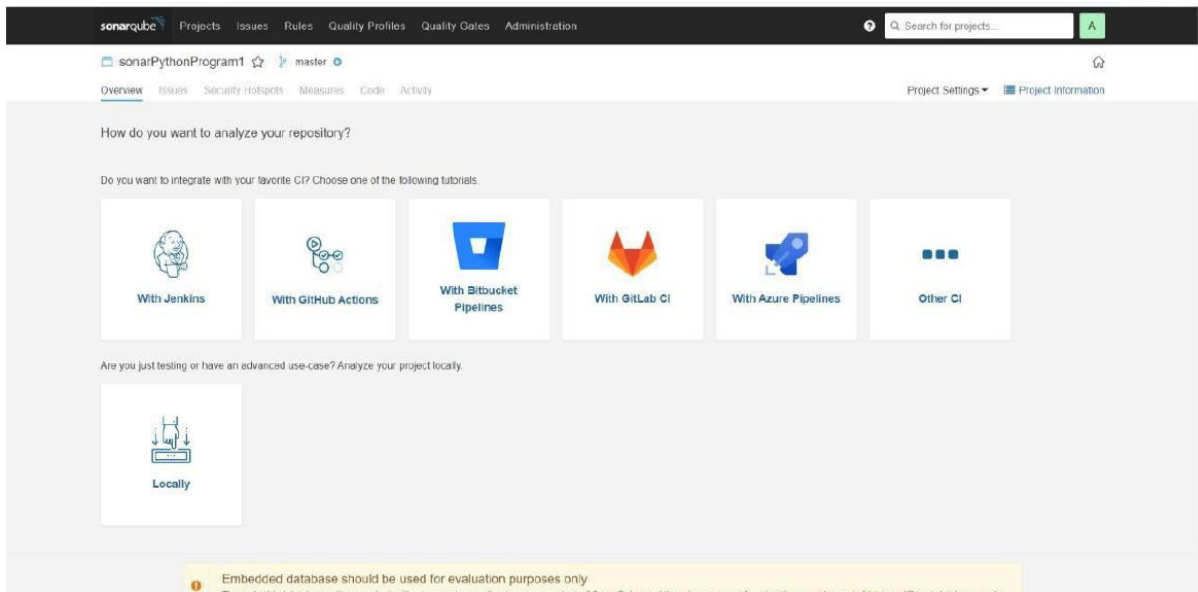
The image shows a 'Log In to SonarQube' dialog box. It has a title bar with the text 'Log In to SonarQube'. Below the title bar, there are two input fields. The first field contains the text 'admin'. The second field contains a series of dots, indicating a password. Below the input fields, there are two buttons: 'Log In' and 'Cancel'. At the bottom of the dialog box, there is a small line of text that reads 'SonarQube™ technology is powered by SonarSource SA'.



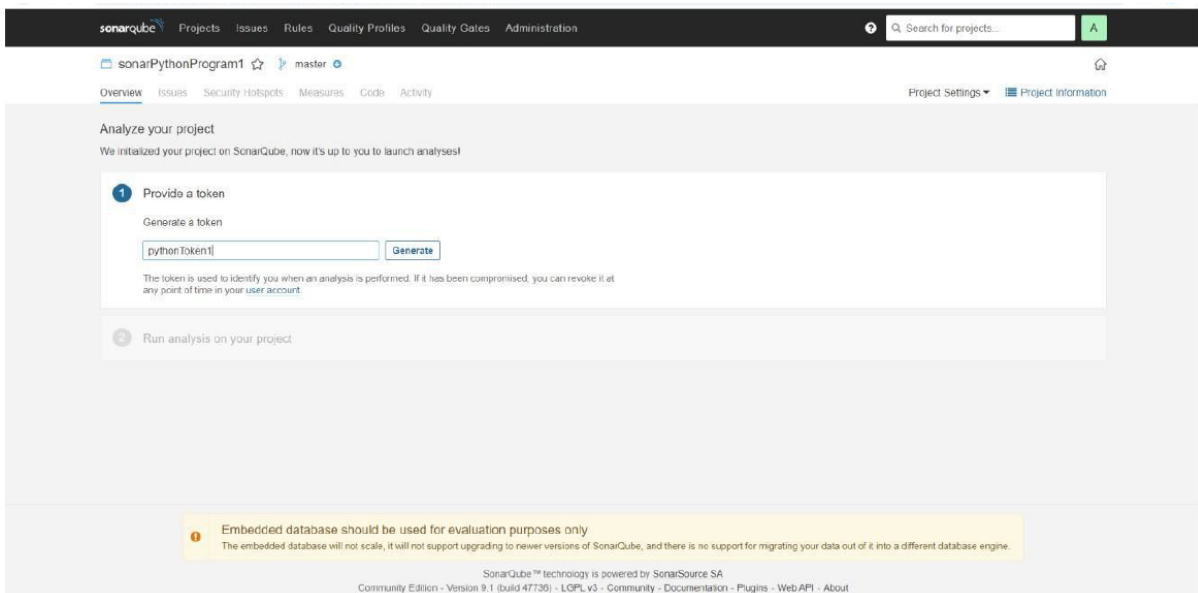
Click on Create a project **Manually**.



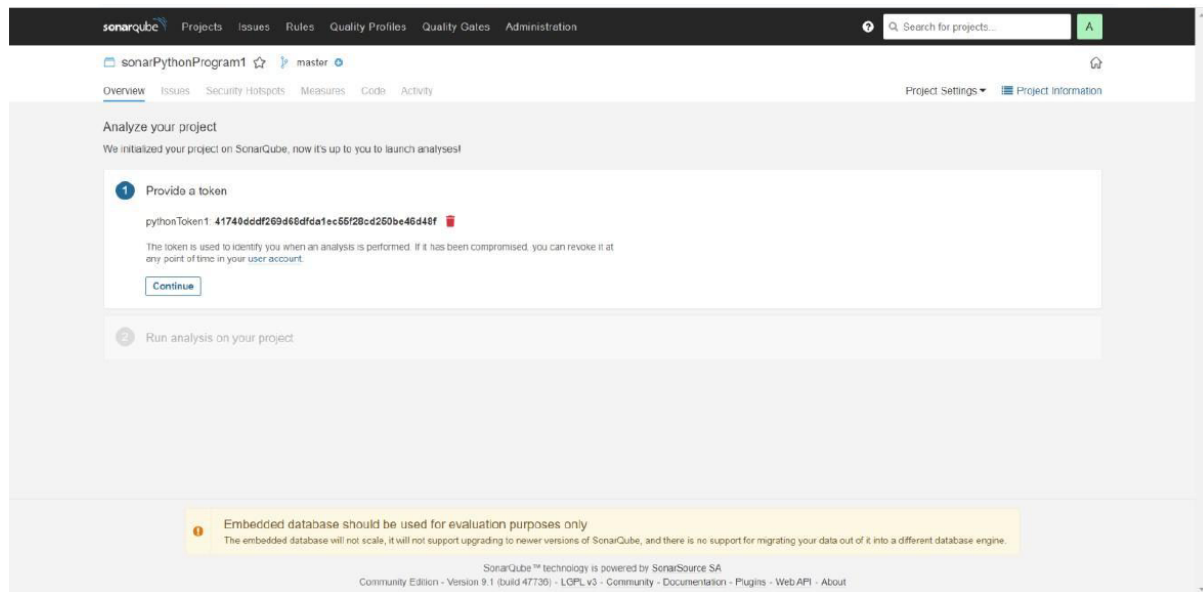
Give any Project display name.



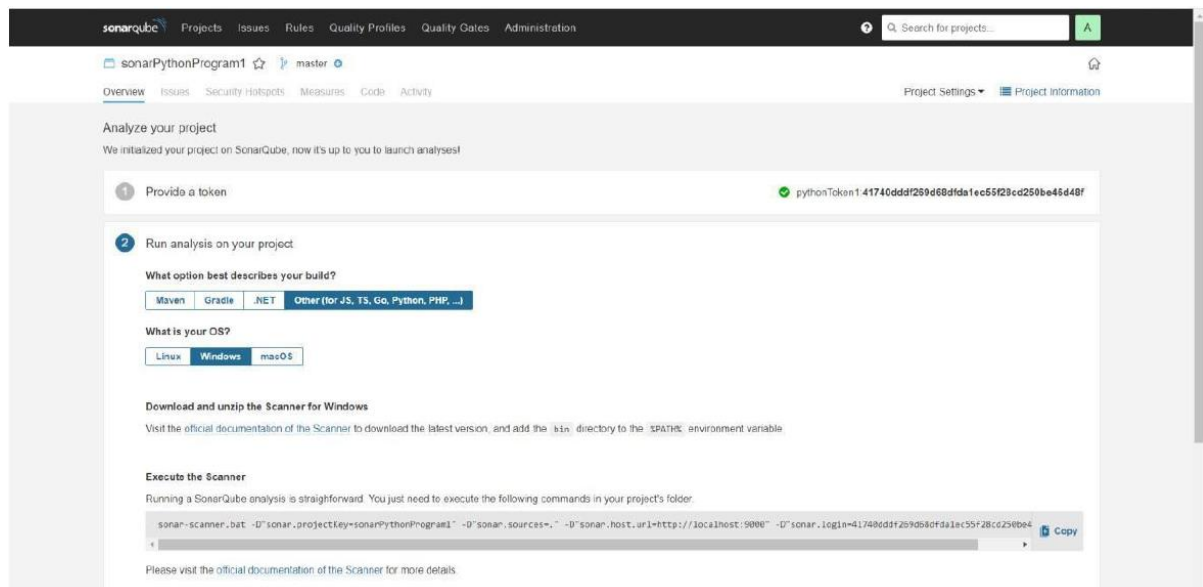
Click on **Locally**



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 =
{'I':1,'V':5,'X':10,'L':50,'C':100,'D':500,'M':1000,'IV':4,'IX':9,'XL':40,'XC':
90,'CD':400,'CM':900}

i = 0 num = " "
while i < len(s):
if i+1<len(s) and s[i:i+2] in roman:
num+=roman[s[i:i+2]] i+=2
else:
#print(i) num+=roman[s[i]] i+=1
return num ob1 = Solution()
print(ob1.romanToInt("III")) print(ob1.romanToInt("CDXLIII"))
```

Open command prompt in this folder and Run program using copied command. "sonar-scanner.bat -
D"sonar.projectKey=sonarPythonProgram1" -D"sonar.sources=." -
D"sonar.host.url=http://localhost:9000" -
D"sonar.login=41740dddf269d68dfda1ec55f28cd250be46d48f"

```
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=41740dddf269d68dfda1ec55f28cd250be46d48f"

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_US", source code encoding: "windows-1252" (analysis is platform dependent)
INFO: Load global settings
INFO: Load global settings (done) | time=20ms
INFO: Server id: bf41a1f2-4b0a0f4e3b8e2L5Cu
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=1674ms
INFO: Process project properties
INFO: Process project properties (done) | time=30ms
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=20ms
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: Indexing files...
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]
INFO: Sensor VB.NET Project Type Information [vbnet] (done) | time=1ms
INFO: Sensor VB.NET Analysis Log [vbnet]
INFO: Sensor VB.NET Analysis Log [vbnet] (done) | time=12ms
INFO: Sensor VB.NET Properties [vbnet]
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 19ms, dir size=103.9 KB
INFO: Analysis report compressed in 19ms, zip size=14.7 KB
INFO: Analysis report uploaded in 76ms
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/ci/task?id=Xwwv7hw91b8xe2L5X01
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\Priyansi\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.

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

sonarPythonProgram1 master

Overview Issues Security Hotspots Measures Code Activity

Quality Gate Status: **Passed**
All conditions passed.

MEASURES

New Code	Overall Code
0 Bugs	Reliability A
0 Vulnerabilities	Security A
0 Security Hotspots	Reviewed Security Review A
5min Debt	1 Code Smells Maintainability A

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

sonarPythonProgram1 master

Overview Issues Security Hotspots Measures Code Activity

MEASURES

0 Vulnerabilities	Security A
0 Security Hotspots	Reviewed Security Review A
5min Debt	1 Code Smells Maintainability A
0.0% Coverage on 15 Lines to cover	Unit Tests
0.0% Duplications on 16 Lines	Duplicated Blocks

ACTIVITY

ISSUES

September 29, 2021, 2:18 PM not provided

sonarqube Projects Issues Rules Quality Profiles Quality Gates Administration

sonarPythonProgram1 master

Overview Issues Security Hotspots Measures Code Activity

My Issues All

Filters

- Type
 - Bug 0
 - Vulnerability 0
 - Code Smell 1
- Severity
 - Blocker 0
 - Critical 0
 - Major 0
 - Minor 1
 - Info 0
- Scope
- Resolution
- Status
- Security Category
- Creation Date
- Language
- Rule
- Tag
- Directory

1 / 1 issues 5min effort

Solution.py

Rename method "romanToInt" to match the regular expression "[a-z][a-z0-9_]*". Why is this an issue? 4 minutes ago L2 convention

1 of 1 shown

Embedded database should be used for evaluation purposes only

SonarQube™ technology is powered by SonarSource SA

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

```

C:\Users\Priyansu>cmd

jw1 [ at org.sonar.application.process.ManagedProcess.isOperational(isManagedProcess.java:60)
jw1 [ at org.sonar.application.process.ManagedProcessHandler.refreshState(ManagedProcessHandler.java:220)
jw1 [ at org.sonar.application.process.ManagedProcessHandler.EventWatcher.run(ManagedProcessHandler.java:285)
jw1 [ Caused by: java.util.concurrent.ExecutionException: java.net.ConnectException: Timeout connecting to [/127.0.0.1:9001]
jw1 [ at org.elasticsearch.common.util.concurrent.BaseFutureSync.getValue(BaseFuture.java:202)
jw1 [ at org.elasticsearch.common.util.concurrent.BaseFutureSync.get(BaseFuture.java:249)
jw1 [ at org.elasticsearch.common.util.concurrent.BaseFuture.get(BaseFuture.java:76)
jw1 [ at org.elasticsearch.client.RestHighLevelClient.performClientRequest(RestHighLevelClient.java:2075)
jw1 [ - 10 common frames omitted
jw1 [ Caused by: java.net.ConnectException: Timeout connecting to [/127.0.0.1:9001]
jw1 [ at org.apache.http.nio.pool.RouteSpecificPool.timeout(RouteSpecificPool.java:169)
jw1 [ at org.apache.http.nio.pool.AbstractNIOConnPool.requestTimeout(AbstractNIOConnPool.java:628)
jw1 [ at org.apache.http.nio.pool.AbstractNIOConnPool.requestTimeout(AbstractNIOConnPool.java:894)
jw1 [ at org.apache.http.nio.reactor.SessionRequestImpl.timeout(SessionRequestImpl.java:184)
jw1 [ at org.apache.http.impl.nio.reactor.DefaultConnectingIOReactor.processTimeouts(DefaultConnectingIOReactor.java:214)
jw1 [ at org.apache.http.impl.nio.reactor.DefaultConnectingIOReactor.processEvents(DefaultConnectingIOReactor.java:158)
jw1 [ at org.apache.http.impl.nio.reactor.AbstractPollingIOReactor.execute(AbstractPollingIOReactor.java:351)
jw1 [ at org.apache.http.impl.nio.conn.PoolingNIOHttpClientConnectionManager.execute(PoolingNIOHttpClientConnectionManager.java:221)
jw1 [ at org.apache.http.impl.nio.client.CloseableHttpAsyncClientBase$1.run(CloseableHttpAsyncClientBase.java:64)
jw1 [ at java.base/java.lang.Thread.run(Thread.java:834)
jw1 [
jw1 [ 2021-09-29 13:50:50 INFO app[[[o.s.a.SchedulerImpl] Process(es) is up
jw1 [ 2021-09-29 13:50:50 INFO app[[[o.s.a.ProcessLauncherImpl] Launch process[key='web', ipcIndex=2, jvmName=refrindexweb]] from [C:\Users\Priyansu\Downloads\sonarqube-9.1.0.47736\; C:\Program Files\Java\jdk-11.0.12\bin\java -Djava.net.handler.class=Offile.encoding=UTF-8 -Djava.io.tmpdir=C:\Users\Priyansu\Downloads\sonarqube-9.1.0.47736\temp -XX:-OmitStackTraceInFastThrow -add-opens:java.base/java.util.all=UNWE
jw1 [ UNWE -add-opens:java.base/java.lang.ALL=UNWE -add-opens:java.base/java.io.ALL=UNWE -add-opens:java.rmi/sun.rmi.transport.all=UNWE -add-exports:java.base/jdk.internal.ref=ALL=UNWE -add-opens:java
jw1 [ .base/java.nio.all=UNWE -add-opens:java.base/sun.nio.ch.all=UNWE -add-opens:java.management/sun.management.all=UNWE -add-opens:java.management/com.sun.management.internal.all=UNWE -Xmx512m -Xms128m
jw1 [ -jar C:\Users\Priyansu\Downloads\sonarqube-9.1.0.47736\temp\sonarqube-9.1.0.47736\bin\lib\jib\ch2\h2-1.4.199.jar org.sonar.ce
jw1 [ Application-9.1.0.47736.jar; C:\Users\Priyansu\Downloads\sonarqube-9.1.0.47736\bin\lib\jib\ch2\h2-1.4.199.jar org.sonar.ce
jw1 [
jw1 [ 2021-09-29 13:51:42 INFO app[[[o.s.a.SchedulerImpl] Process(es) is up
jw1 [ 2021-09-29 13:51:42 INFO app[[[o.s.a.ProcessLauncherImpl] Launch process[key='ce', ipcIndex=3, jvmName=refrindexce]] from [C:\Users\Priyansu\Downloads\sonarqube-9.1.0.47736\; C:\Program Files\Java\jdk-11.0.12\bin\java -Djava.net.handler.class=Offile.encoding=UTF-8 -Djava.io.tmpdir=C:\Users\Priyansu\Downloads\sonarqube-9.1.0.47736\temp -XX:-OmitStackTraceInFastThrow -add-opens:java.base/java.util.all=UNWE
jw1 [ -add-exports:java.base/jdk.internal.ref=ALL=UNWE -add-opens:java.base/sun.nio.ch.all=UNWE -add-opens:java.management/sun.management.all=UNWE -add-opens:java.management/com.sun.management.internal.all=UNWE -Xmx512m -Xms128m -XX:-HeapDumpOnOutOfMemoryError -Dhttp.nonProxyHosts=localst[127.0.0.1]; C:\Users\Priyansu\Downloads\sonarqube-9.1.0.47736\bin\lib\jib\ch2\h2-1.4.199.jar org.sonar.ce
jw1 [ Application-9.1.0.47736.jar; C:\Users\Priyansu\Downloads\sonarqube-9.1.0.47736\bin\lib\jib\ch2\h2-1.4.199.jar org.sonar.ce
jw1 [
jw1 [ Properties
jw1 [ 2021-09-29 13:51:42 WARN app[[[start] #####
jw1 [ 2021-09-29 13:51:42 WARN app[[[start] Default Administrator credentials are still being used. Make sure to change the password or deactivate the account.
jw1 [ 2021-09-29 13:51:42 WARN app[[[start] #####
jw1 [ 2021-09-29 13:51:46 INFO app[[[o.s.a.SchedulerImpl] Process(es) is up
jw1 [ 2021-09-29 13:51:46 INFO app[[[o.s.a.SchedulerImpl] SonarQube is up
jw1 [ CTRL-C trapped. Shutting down.
jw1 [ 2021-09-29 14:38:57 INFO app[[[o.s.a.SchedulerImpl] Stopping SonarQube
jw1 [ 2021-09-29 14:38:58 INFO app[[[o.s.a.SchedulerImpl] Process(es) is stopped
jw1 [ 2021-09-29 14:38:58 INFO app[[[o.s.a.SchedulerImpl] Process(es) is stopped
jw1 [ 2021-09-29 14:38:58 INFO app[[[o.s.a.SchedulerImpl] Process(es) is stopped
jw1 [ 2021-09-29 14:38:58 INFO app[[[o.s.a.SchedulerImpl] SonarQube is stopped
jw1 [
jw1 [ wrapper <-- Wrapper Stopped
jw1 [
jw1 [ Terminate batch job (Y/N)? Y

```

CONCLUSION: In this assignment, we learnt analysis of using sonarqube. The goal of SonarQube is to empower developers first and to grow an open community around the quality and security of code.