

Running static code analysis using Sonar Cloud in CI pipeline

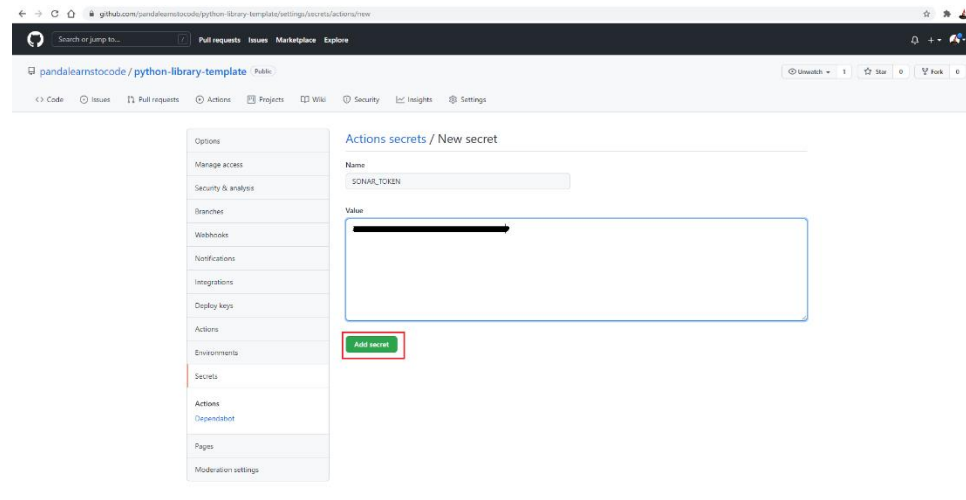
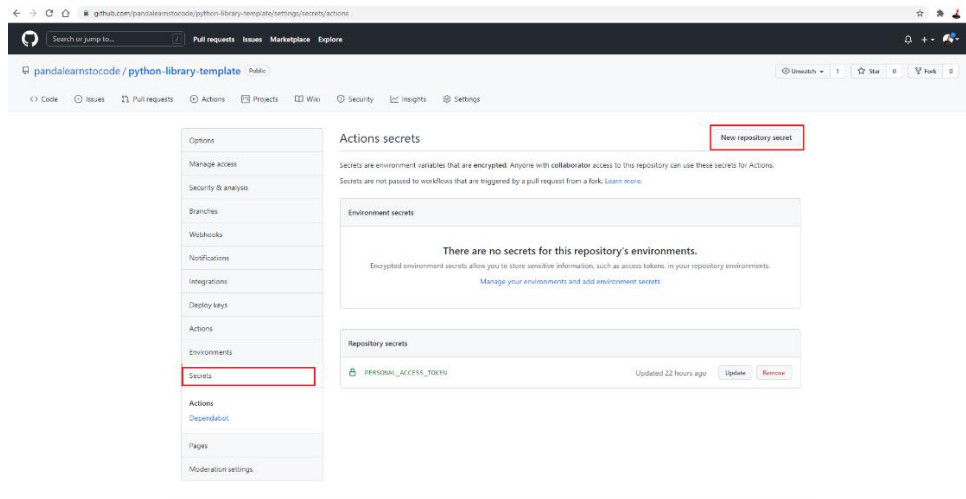
Step 1: Importing project to sonar cloud: login to sonarcloud.io → import GitHub organization → select a repository in which you want to run sonar cloud static code analysis → sonar cloud will import the repository → copy paste the project key and organization key from the landing page → these values has to be updated in sonar-project.properties in project root directory.

The screenshot shows the SonarCloud project landing page for 'python-library-template'. The page displays various quality metrics: Quality Gate (Not computed), Reliability Measures (0 bugs), Security Measures (0 vulnerabilities, 0 security hotspots), Maintainability Measures (0 code smells), and Duplications Measures (0.0% duplications, 0 duplicated blocks). On the right, the 'About This Project' section shows 303 lines of code, 237 Python lines, and 95 C# lines. The 'Last analysis' was performed on October 7, 2021, at 2:21 AM. A red annotation points to the 'Project Key' and 'Organization Key' fields, stating: 'These two values has to be updated in sonar-project.properties in the project root directory'. The Project Key is 'pandalearnetocode_python-library' and the Organization Key is 'pandalearnetocode'.

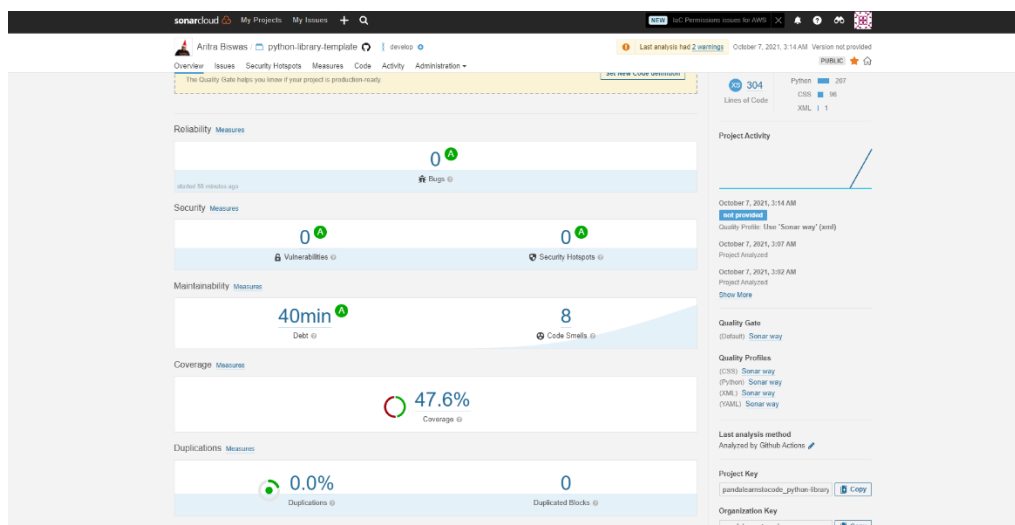
Step 2: Get SONAR_TOKEN from sonarcloud.io. Log into SonarCloud → Click on your profile → 'My Account' → 'Security' → Generate your access token for SonarCloud here → Go to your repository settings in GitHub → 'Secrets' → add a new secret with name SONAR_TOKEN and use the generated SonarCloud access token as value.

The screenshot shows the 'Tokens' page in SonarCloud. It explains that User Tokens can be used as a replacement for user login. A new token 'python-library-template' has been created. A red annotation points to the 'Generate' button, stating: '2. When you click on generate a token will be generate, copy and keep this, it will be used as SONAR_TOKEN in github actions'. Below the token list, there is a table with the following data:

Name	Last use	Created	Revoke
Analyze "streamlit boilerplate..."	2 months ago	July 24, 2021	Revoke
python-library-template	Never	October 7, 2021	Revoke



Step 4: Add pytest, flake8 and pylint related command in action → add SonarCloud action in GitHub action → From sonar cloud project → administrative → switch off automatic integration with github repository → trigger CI pipeline → Validate all the required things are getting reflected in sonar cloud dashboard or not.



TODO:

- Quality gate
- PR decorator
- Adding status badge
- Notification if the merge fails
- Enabling things based on PR, not by push

Reference:

1. <https://dev.to/remast/go-for-sonarcloud-with-github-actions-3pmn>
2. <https://github.com/pandalearnstocode/python-library-template/blob/develop/.github/workflows/python-app.yml>
3. <https://github.com/pandalearnstocode/python-library-template/blob/develop/sonar-project.properties>
4. https://sonarcloud.io/dashboard?id=pandalearnstocode_python-library-template