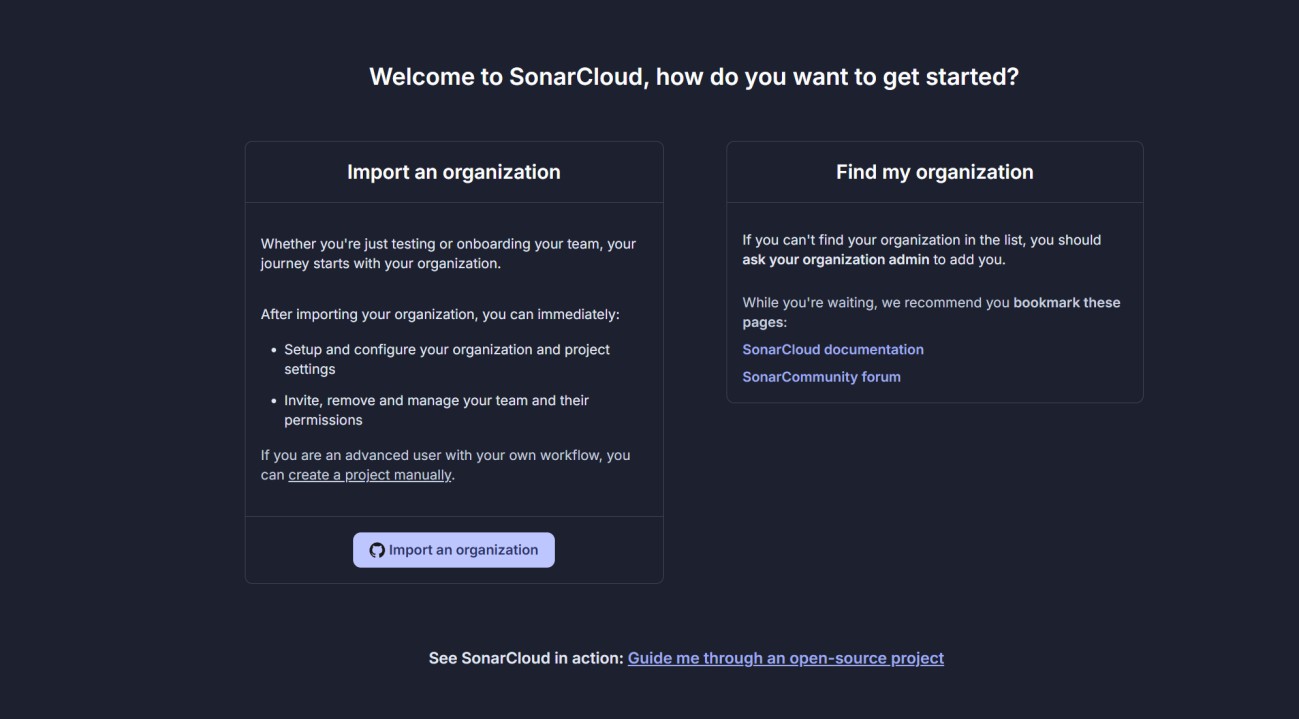
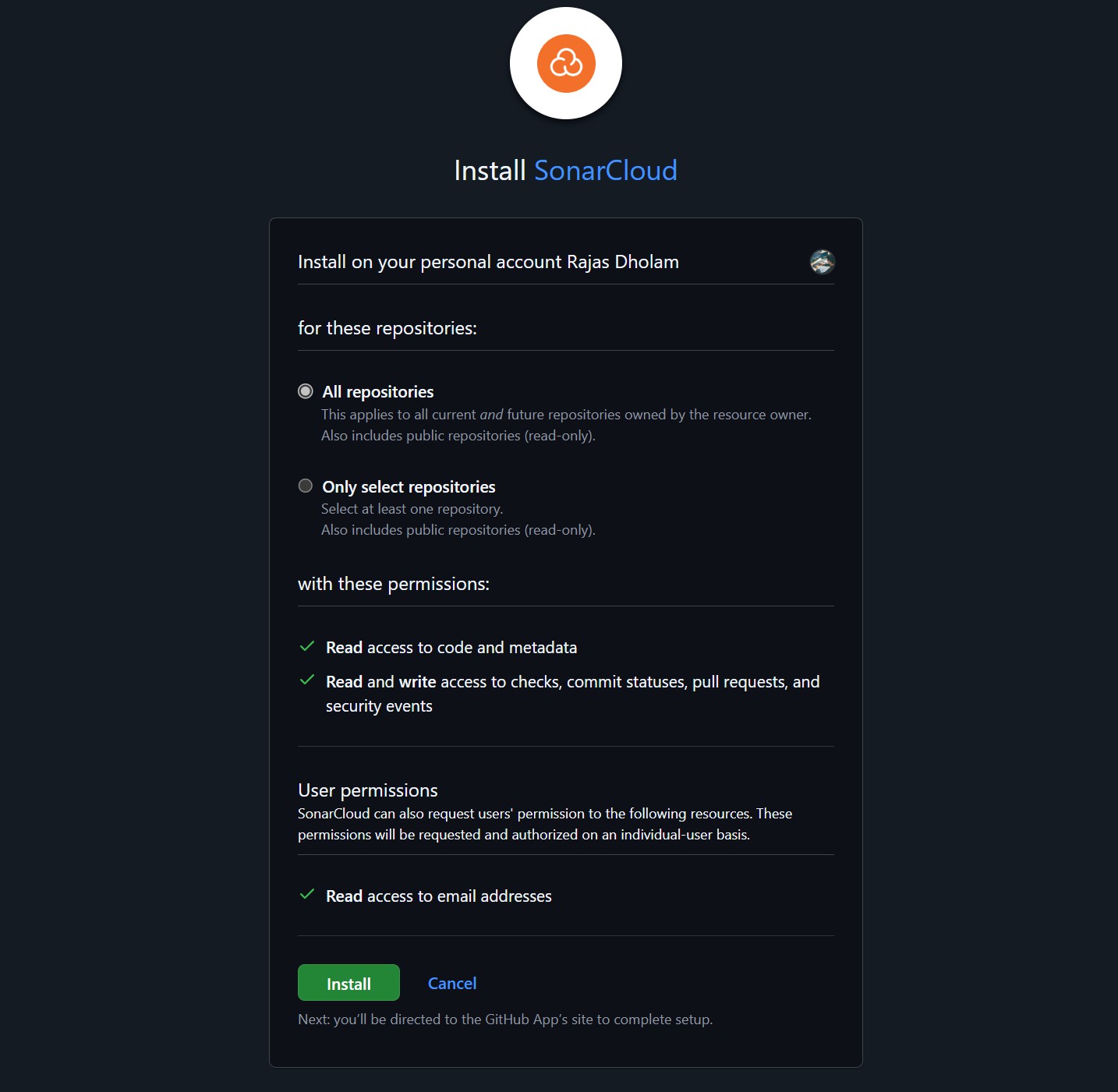
Name: Rajas Dholam Roll No:A013

Q1. Integrate a basic Python project into SonarCloud and analyze its code quality. Configure the project to show issues like code smells, bugs, and security vulnerabilities.

Step 1) I Go to sonar cloud Sign up using your GitHub

Authorize SonarCloud to access your repositories.

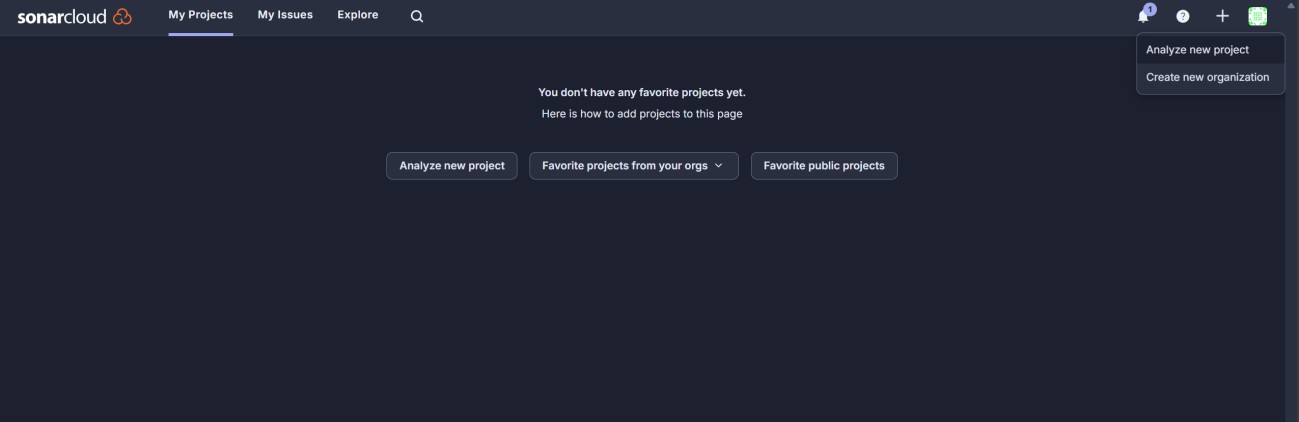


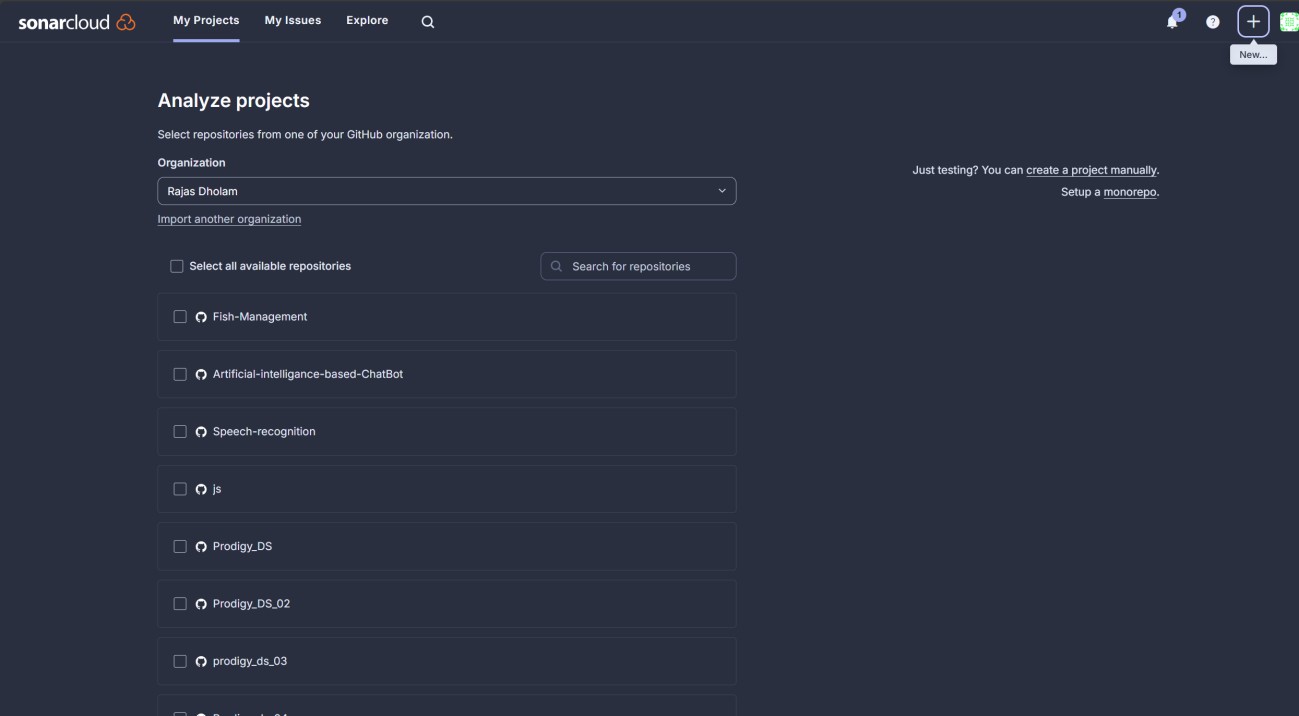


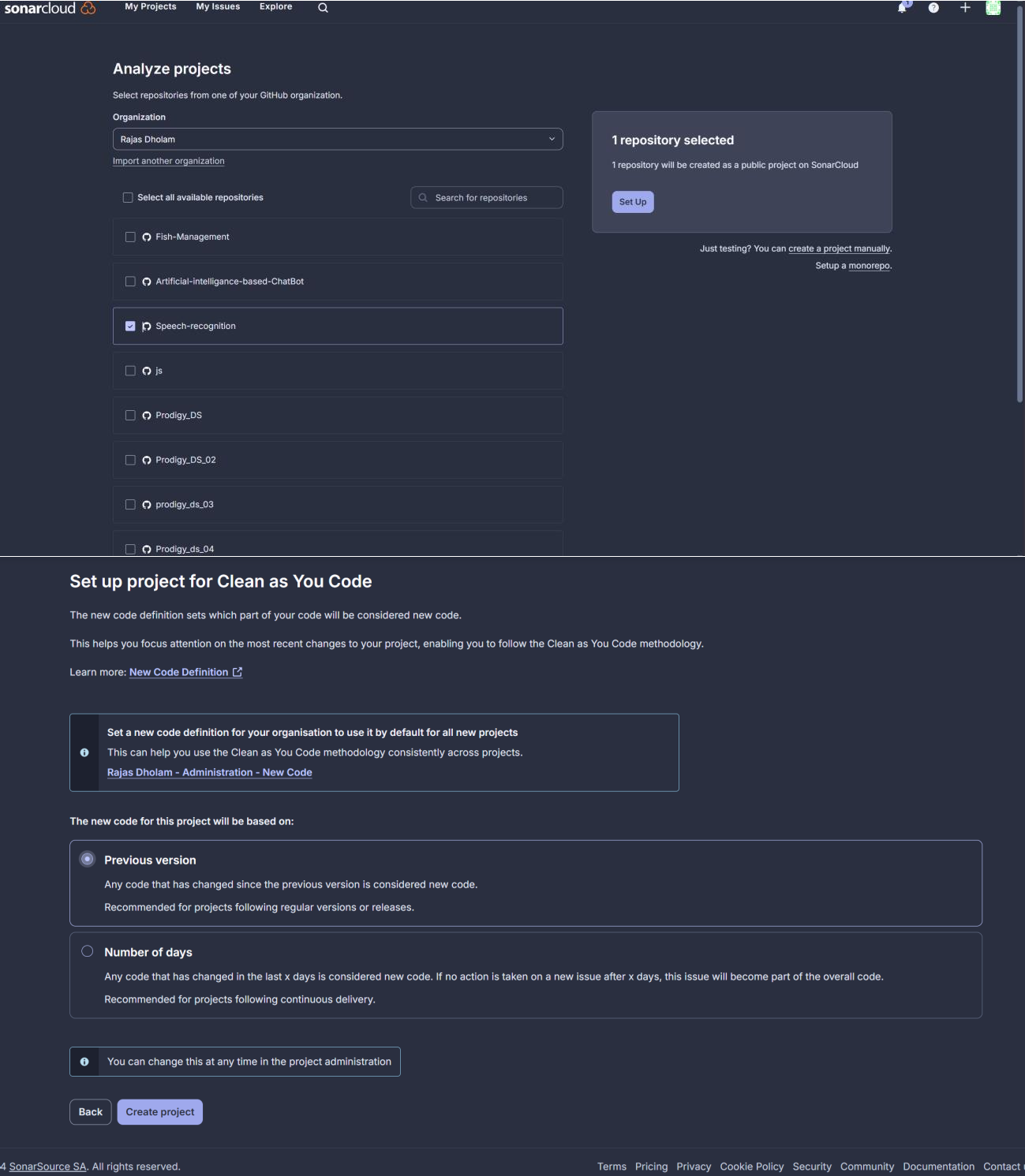
# Step 2) Create a Project on SonarCloud

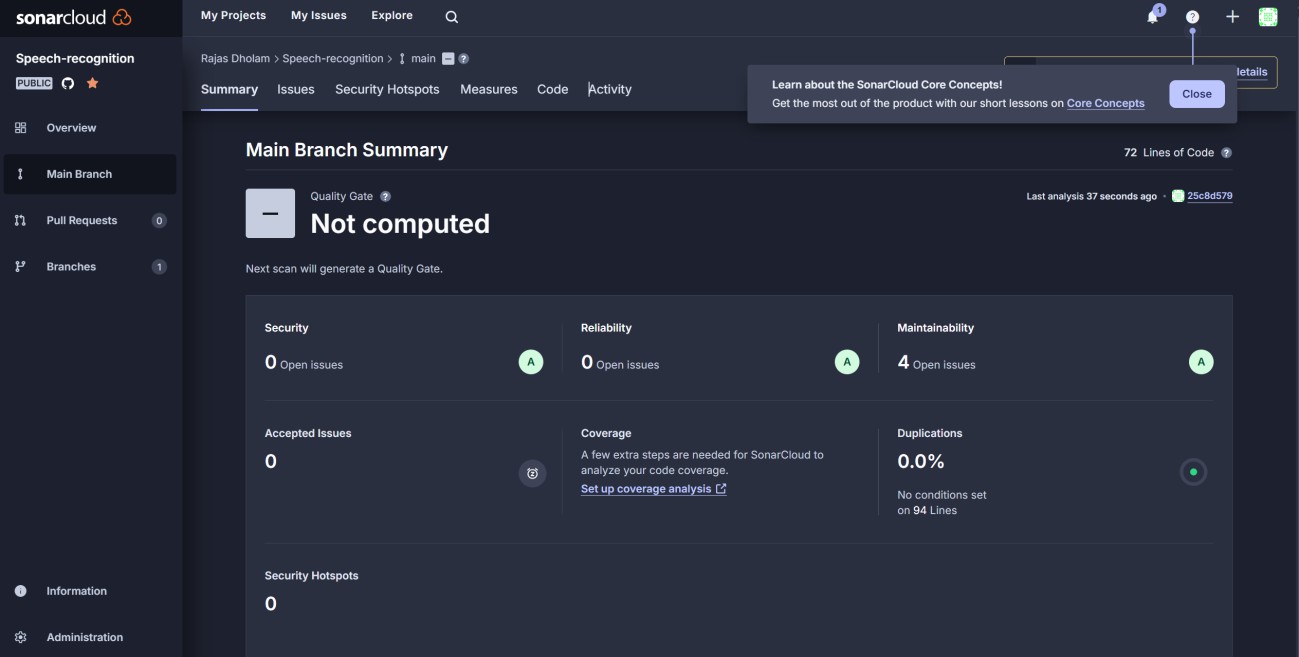
After logging into SonarCloud, go to the **Projects** section. Click on **Analyze new project**.

Choose the repository where your Python project is hosted. Select the repository and click **Set Up** to analyze the project.







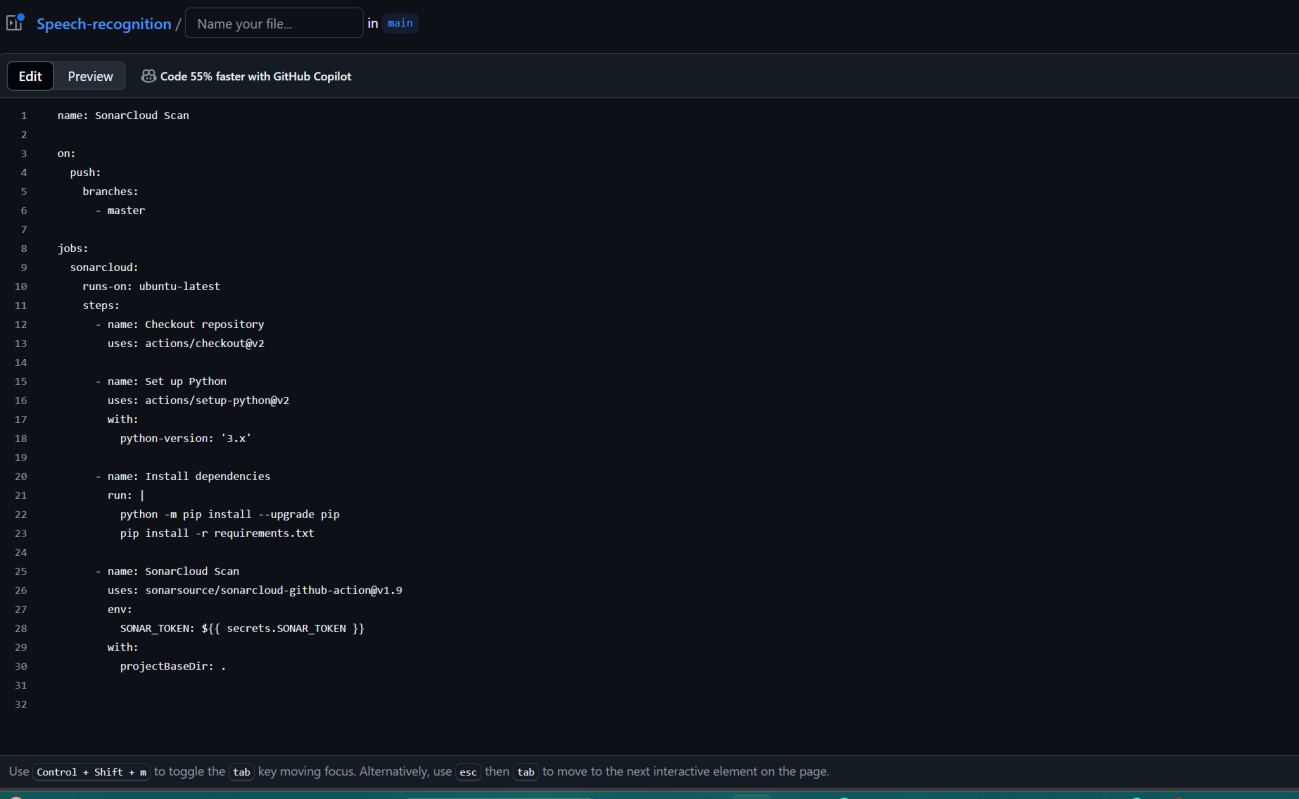


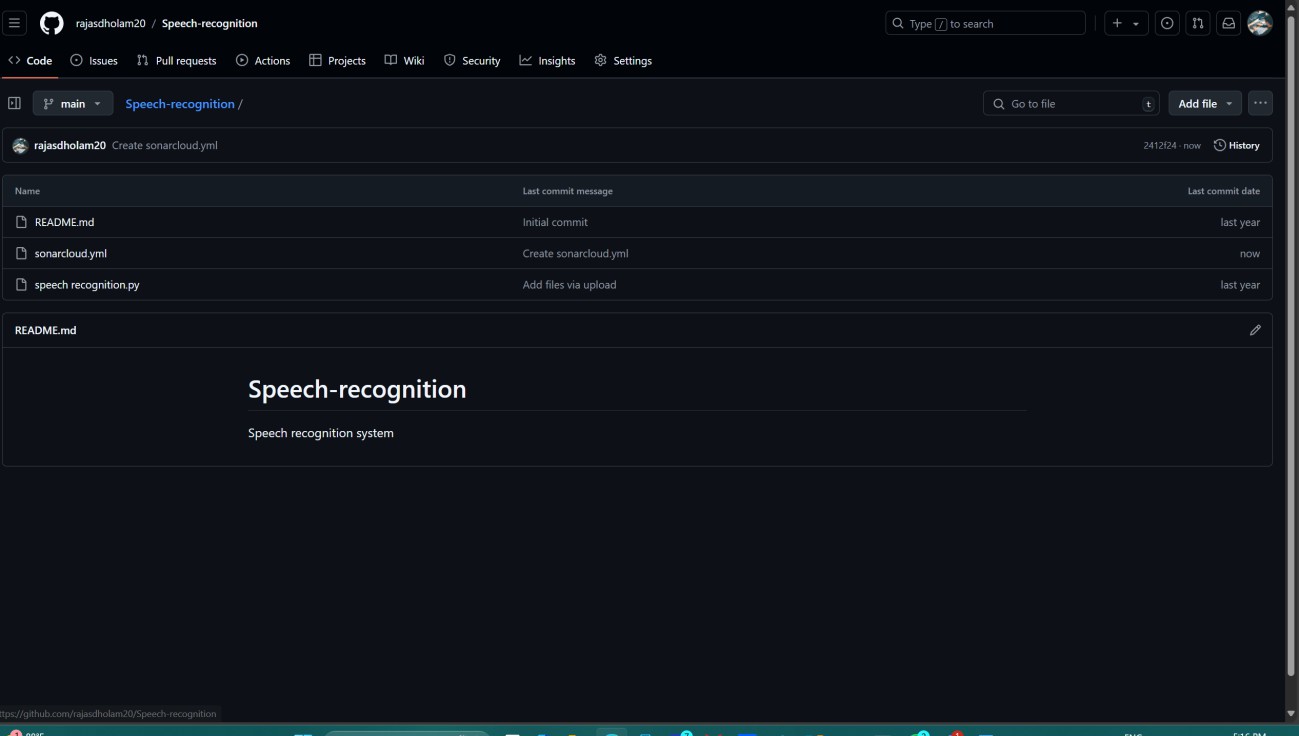
Step 3 ) To analyze your Python project, you need to set up the SonarScanner in your project repository.

# Option 1: Using SonarCloud GitHub Actions (Recommended for GitHub Projects)

1. **Add SonarCloud Configuration:**

In your repository, create a file .github/workflows/sonarcloud.yml with the following content This yaml cloud add in the project



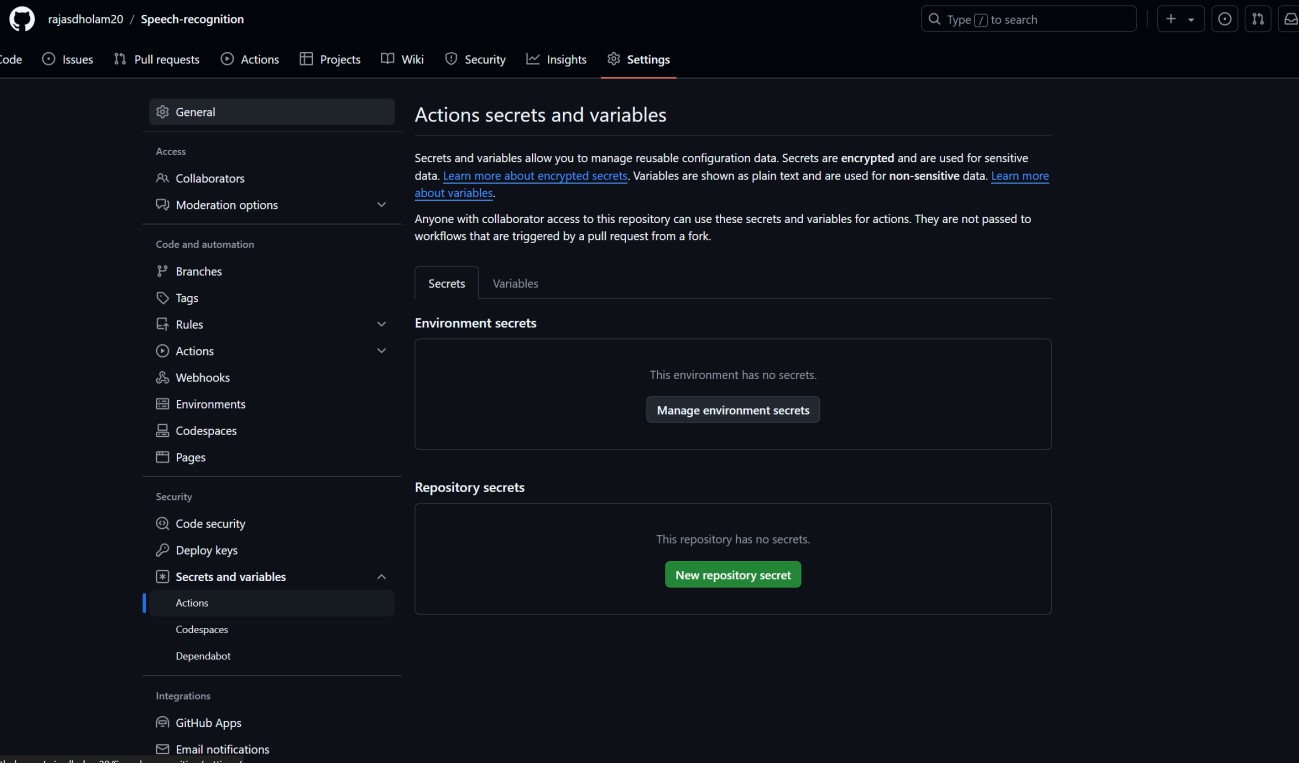
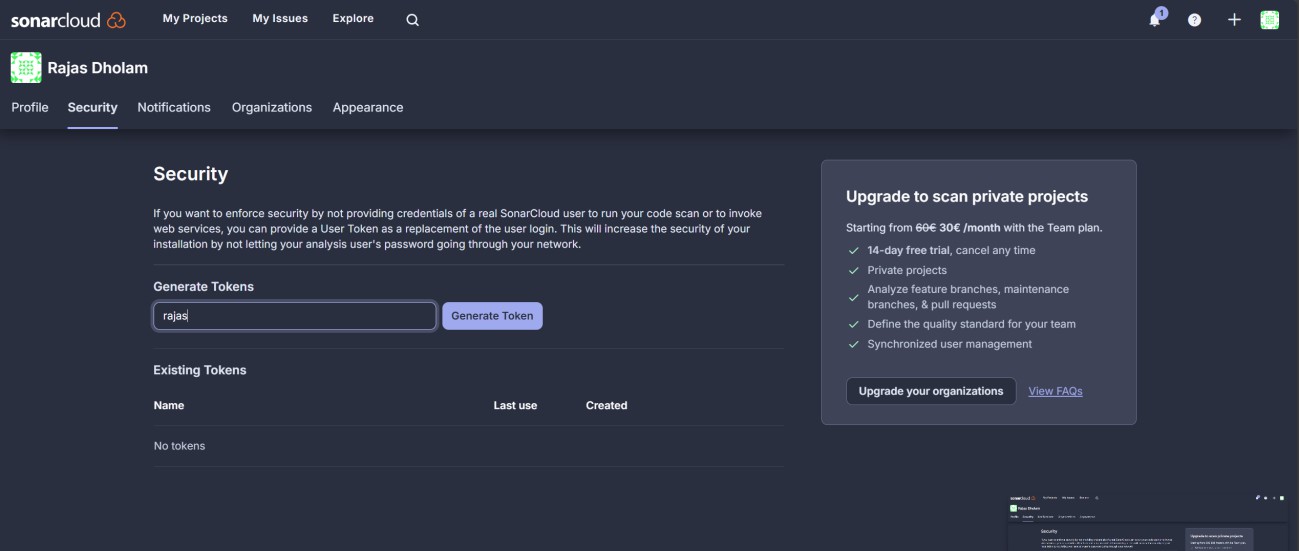


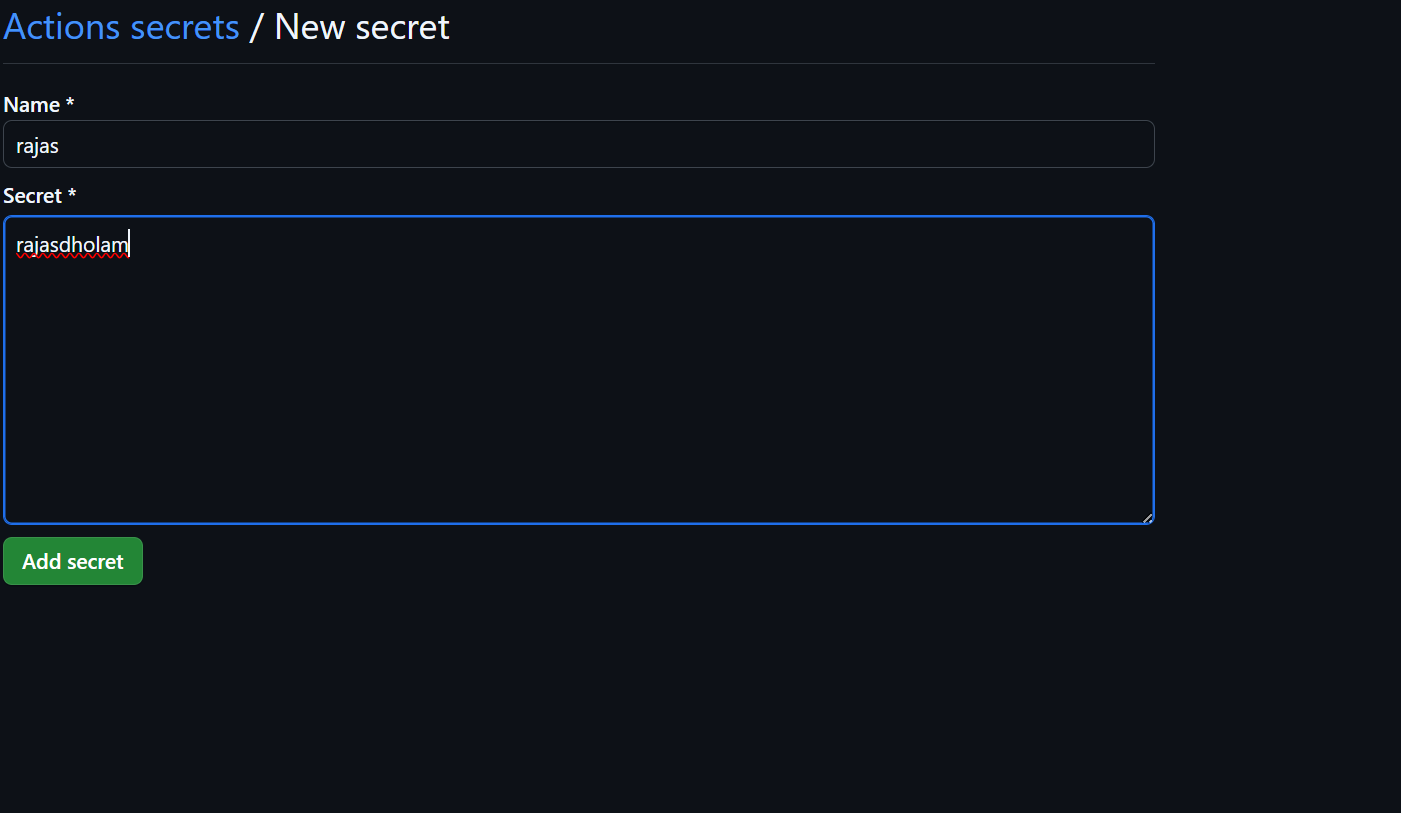
# Step 4) Generate a SonarCloud Token:

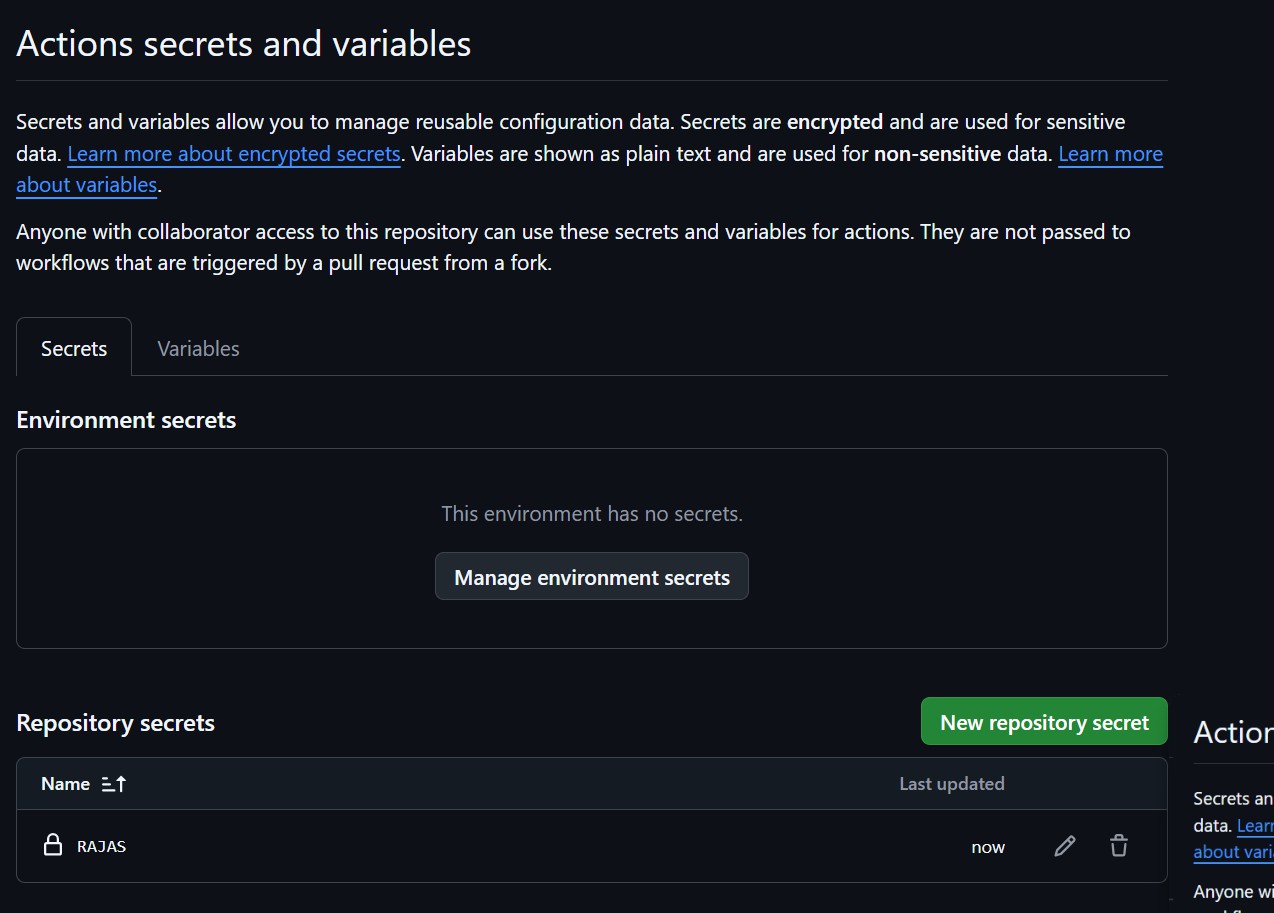
* + Go to **SonarCloud > My Account > Security**.
  + Click **Generate Token** and copy the token.
  + Add this token as a secret in your GitHub repository:

# Go to Repository > Settings > Secrets > Actions > New repository secret.

* + - Name the secret SONAR\_TOKEN and paste the token.

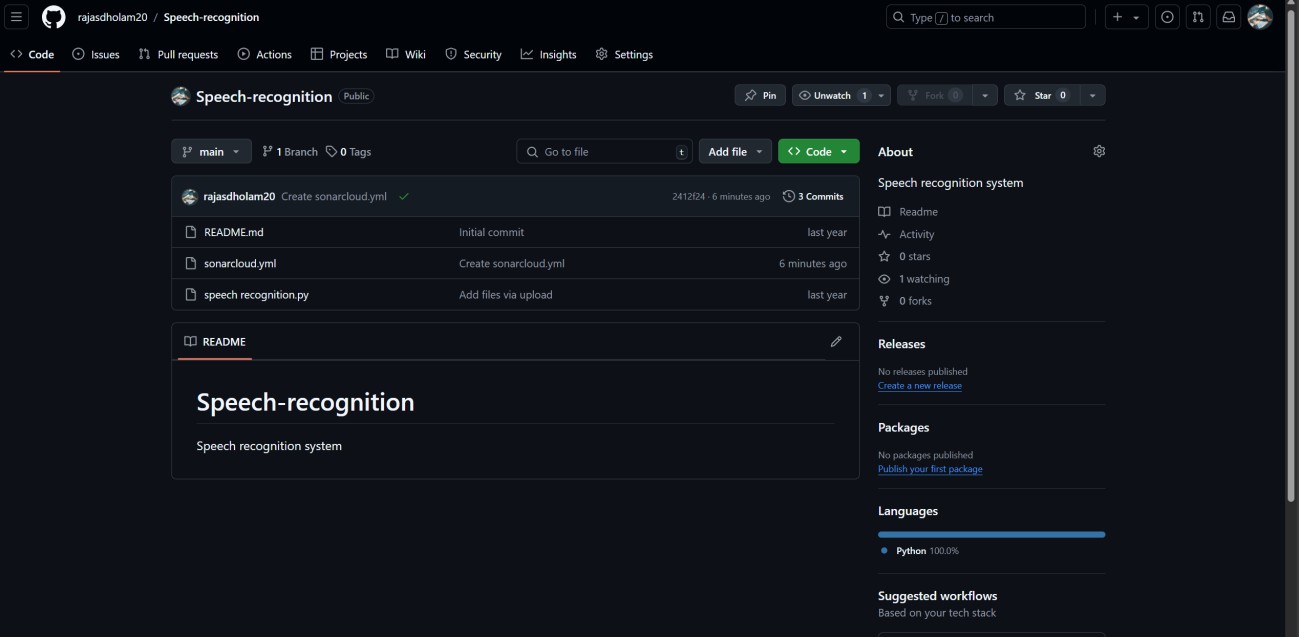






Step 5) **Push Your Changes to GitHub**:

Once you push this configuration to your repository, GitHub Actions will run and integrate SonarCloud for code quality analysis.



# Step 6) Fix Issues and Re-Analyze

1. I Review the issues SonarCloud detected code small and bugs
2. I Fix these issues in code.
3. And lastly Push the changes to your repository, and SonarCloud will automatically re-run the analysis if GitHub Actions is configured.

