Setting up workflow secret

Objective: You wanted to configure sensitive information used in your workflow, within your secrets to ensure those does not get exposed into execution logs.

Tools required: GitHub Actions

Prerequisites: None

Steps to be followed:

1. Login to GitHub.com.
2. Create new secret in your repository
3. Create workflow to implement secrets

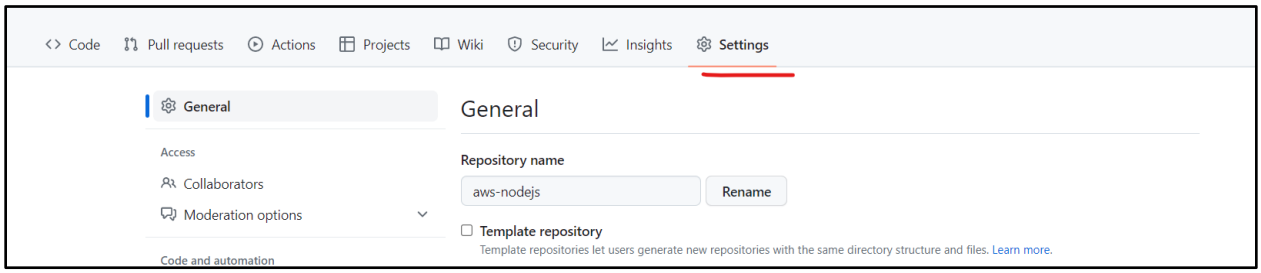
Step 1: Login to GitHub.com

1.1 Sign in to the GitHub portal at https://github.com

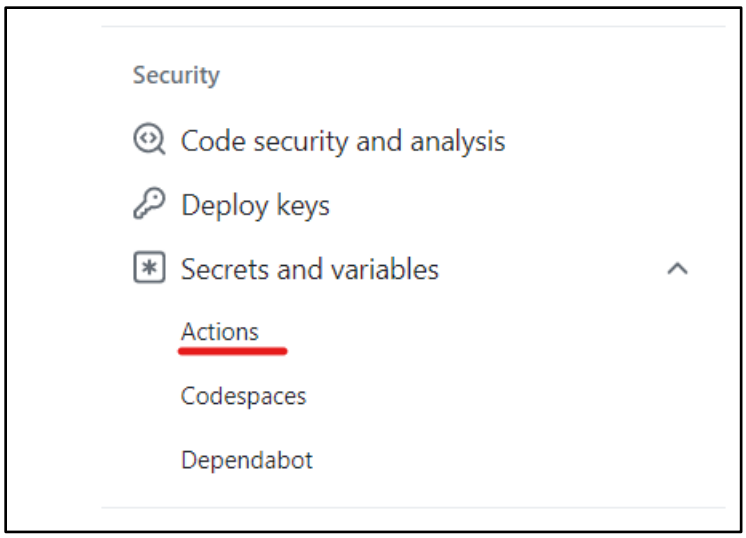
1.2 Navigate to your repository main page where we are going to create a workflow file.

Step 2: Create new secret in your repository

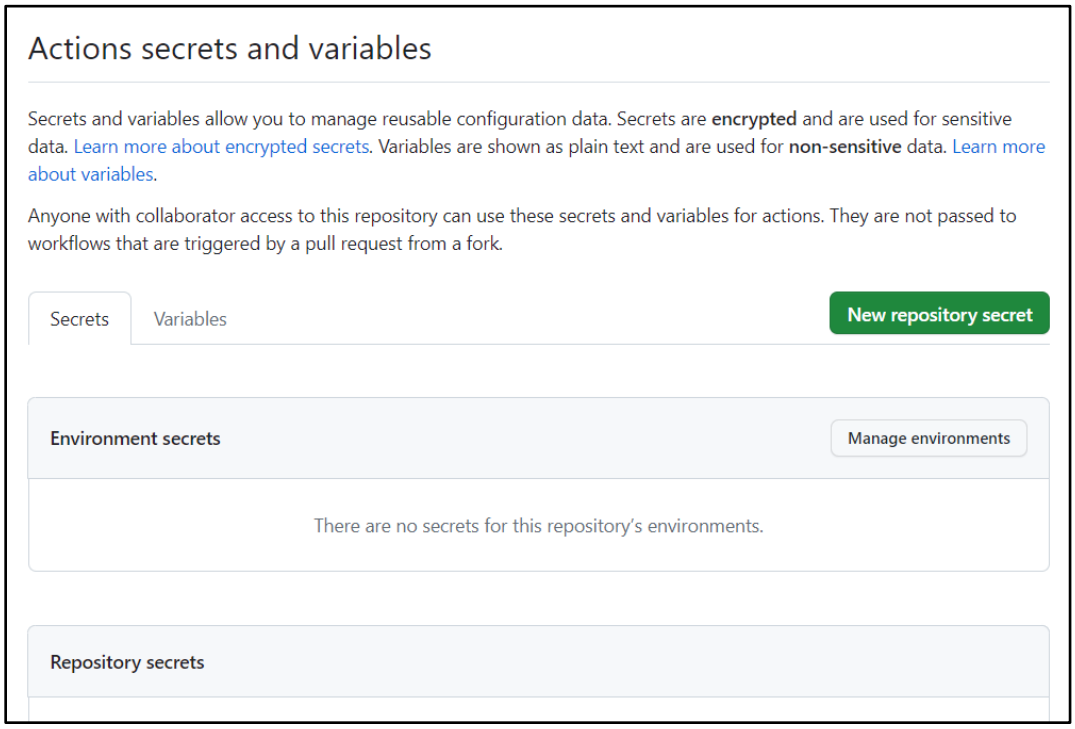
2.1 Navigate to your repository main page and click on settings tab to create new secret in your repository.



2.2 Navigate to security section to left sidebar and choose Secrets and variable dropdown and then click on Actions to create new secrets and variables.



2.3 Next, we have to create new secrets or variable, Click on New repository secret to store sensitive information.



Step 3: Create workflow to implement secrets in your workflow.

3.1 Next, we have to create Docker workflow file to automate CI process for building custom Docker image.

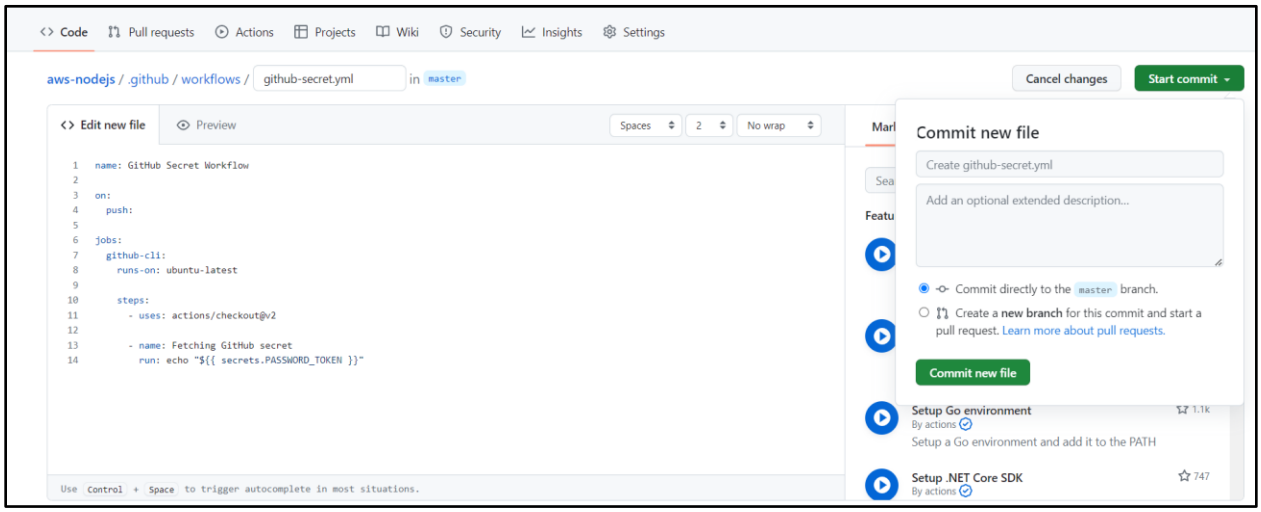
3.2 Create a .github/workflows directory in your repository in case directory does not exists.

3.3 In workflow directory, create a new workflow file with name github-secret.yml.

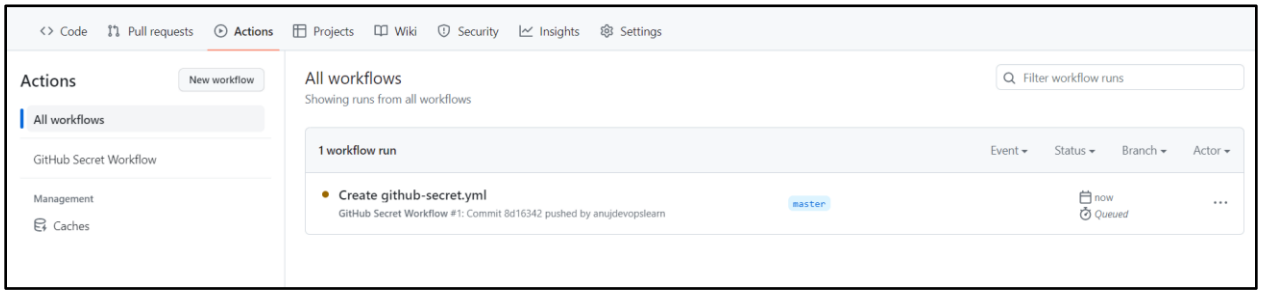
```
name: GitHub Secret Workflow

on:
  push:

jobs:
  github-cli:
    runs-on: ubuntu-latest

    steps:
      - uses: actions/checkout@v2

      - name: Fetching GitHub secret
```

run: echo "${{ secrets.PASSWORD_TOKEN }}"

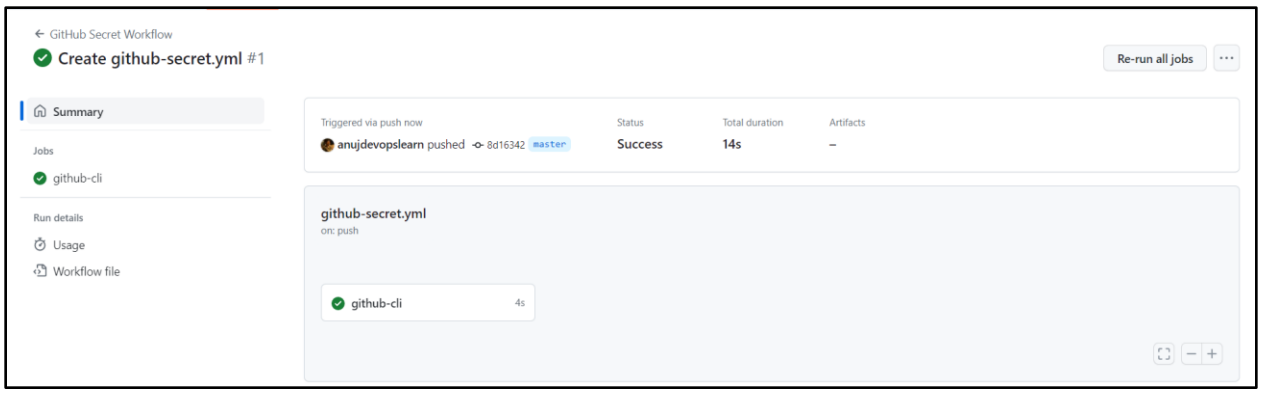
2.3 Once file is created, click on Commit new file to save workflow file in your code repository.



2.4 Next navigate to Actions tab on your repository to access workflow execution page as below:



2.5 Select latest execution logs from GitHub actions and look for detailed execution logs as below:



You can expand secrets to see secrets gets redacted, which means sensitive information would not be displayed in execution logs: