Vulnerability Analyzer

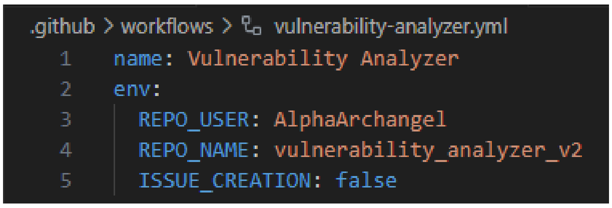
> This is a GitHub Actions Resuable Workflow. You will need to first set this repo up in your own repository and use it in other repos.

Setup Reusable Repo

- First setup your own repo called `vulnerability_analyzer`. Make sure to create the repo with private visibility.

- Then add the files of this repo to the newly created repository.

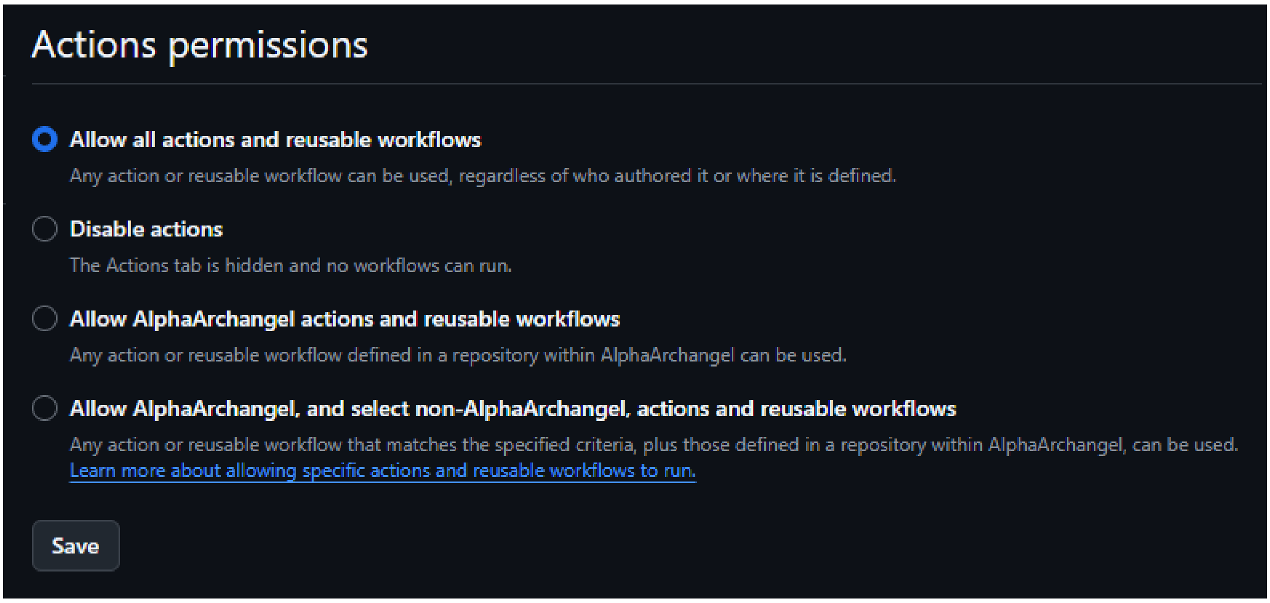
- Then update these values in `.github/workflows/vulnerability-analyzer.yml`. Set `REPO_USER` and `REPO_NAME` as your newly created repo's name and your user name. Also set `ISSUE_CREATION` to `true` or `false` according to your preference.



.github > workflows > vulnerability-analyzer.yml

```
name: Vulnerability Analyzer
env:
  REPO_USER: AlphaArchangel
  REPO_NAME: vulnerability_analyzer_v2
  ISSUE_CREATION: false
```

- Then Go to the settings page of the repo and set `Actions permissions` to `Allow all actions and reusable workflows` and hit save.



Actions permissions

● **Allow all actions and reusable workflows**

Any action or reusable workflow can be used, regardless of who authored it or where it is defined.

○ **Disable actions**

The Actions tab is hidden and no workflows can run.

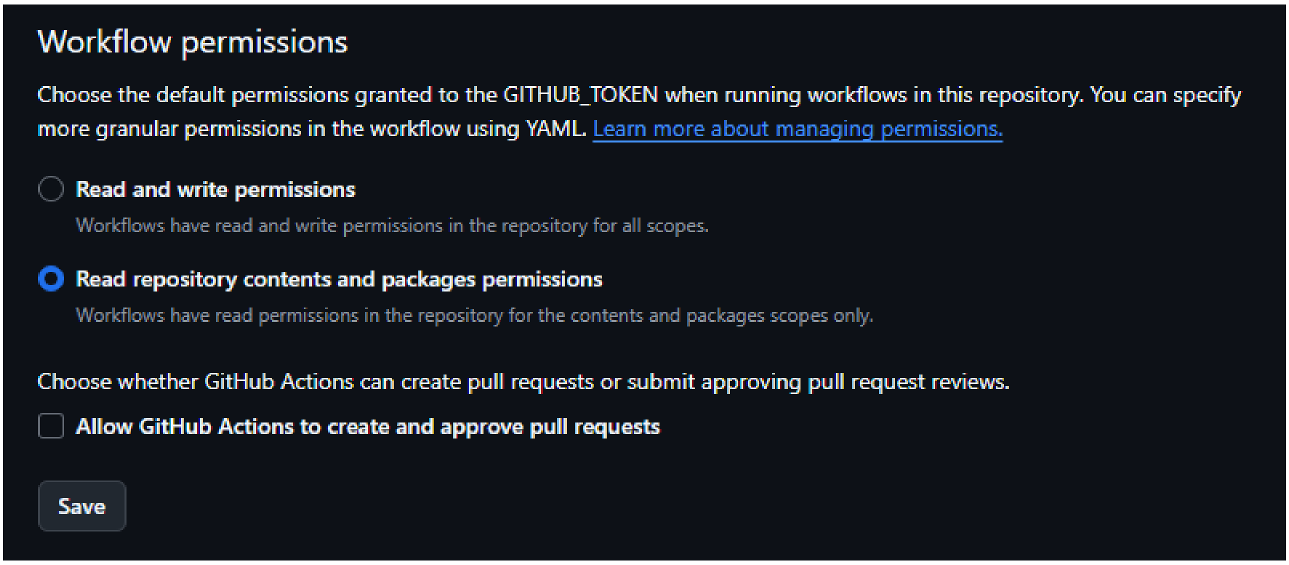
○ **Allow AlphaArchangel actions and reusable workflows**

Any action or reusable workflow defined in a repository within AlphaArchangel can be used.

○ **Allow AlphaArchangel, and select non-AlphaArchangel, actions and reusable workflows**

Any action or reusable workflow that matches the specified criteria, plus those defined in a repository within AlphaArchangel, can be used. Learn more about allowing specific actions and reusable workflows to run.

- Then Scroll down and set `Workflow permissions` to `Read repository contents and packages permissions`.



Workflow permissions

Choose the default permissions granted to the GITHUB_TOKEN when running workflows in this repository. You can specify more granular permissions in the workflow using YAML. Learn more about managing permissions.

○ **Read and write permissions**

Workflows have read and write permissions in the repository for all scopes.

● **Read repository contents and packages permissions**

Workflows have read permissions in the repository for the contents and packages scopes only.

Choose whether GitHub Actions can create pull requests or submit approving pull request reviews.

□ **Allow GitHub Actions to create and approve pull requests**

- After these steps the Reusable Repe setup is complete.

How to build python script after changes

- First you need to be in a Linux environment

- After that make sure to all the python dependencies are installed, run `pip install -r requirements.txt` after locating where your requirements.txt file is location. in the repo the file is located in `.github/workflows/vulnerability-analyzer` change directory into that location and do the pip install.

- Then, open up a terminal and `cd` change directory to the location that your `vulnerability_analyzer.py` is located. `cd .github/workflows/vulnerability-analyzer/utils` from the root of the repo.

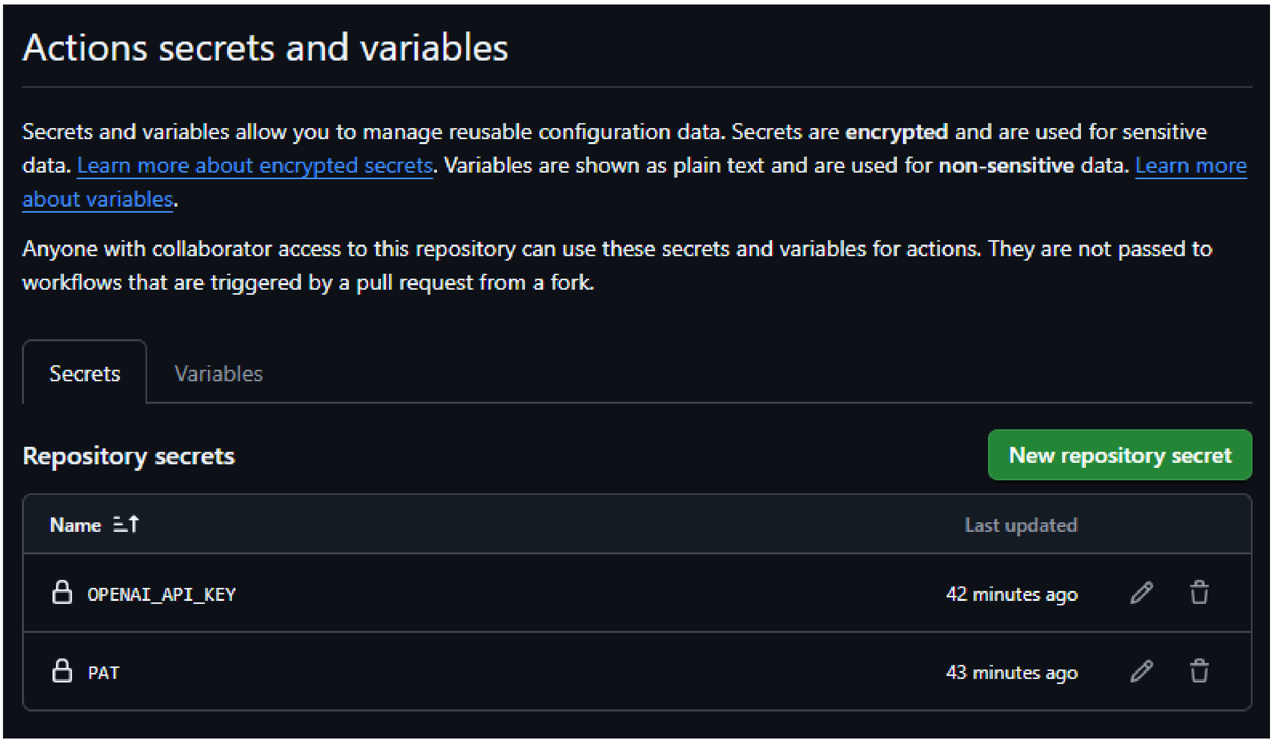
- Then run this command to build the python script. `pyinstaller --onefile --hidden-import=tiktoken_ext.openai_public --hidden-import=tiktoken_ext .github/workflows/vulnerability-analyzer/utils/vulnerability_analyzer.py` . This command should create two folders and one file. goto `dist` folder and copy the build file into the `utils` folder in the repo. then delete the `dist`, `build` and `vulnerability_analyzer.spec` folders and files.

- Finally push the changes.

Setup other repo's to use the reusable repo

- As shown in the demo video, First you will need to create a new repository. This can be done in your alredy available repo also.

- Then you will need to setup the required credentials in the repo. Just go to repo Settings -> Secrets and variables -> Actions and setup the `OPENAI_API_KEY` and `PAT` .



Actions secrets and variables

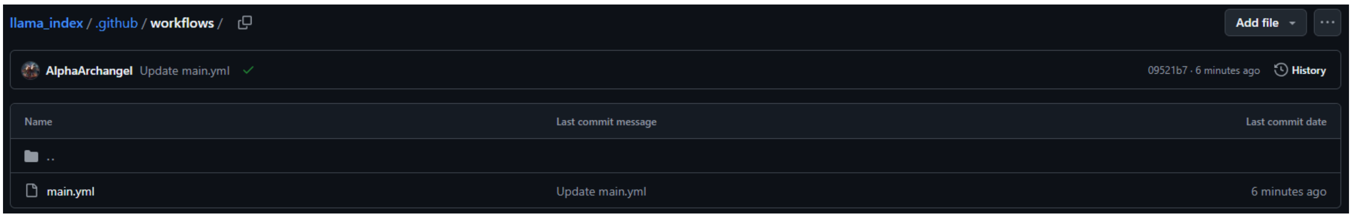
Secrets and variables allow you to manage reusable configuration data. Secrets are **encrypted** and are used for sensitive data. Learn more about encrypted secrets. Variables are shown as plain text and are used for **non-sensitive** data. Learn more about variables.

Anyone with collaborator access to this repository can use these secrets and variables for actions. They are not passed to workflows that are triggered by a pull request from a fork.

Repository secrets

Name	Last updated
OPENAI_API_KEY	42 minutes ago
PAT	43 minutes ago

- Then inside the repo, create a folder called `.github`, then inside that create a folder called `workflows` .



llama_index / .github / workflows /

AlphaArchangel Update main.yml ✓ 09521b7 · 6 minutes ago

Name	Last commit message	Last commit date
..		
main.yml	Update main.yml	6 minutes ago

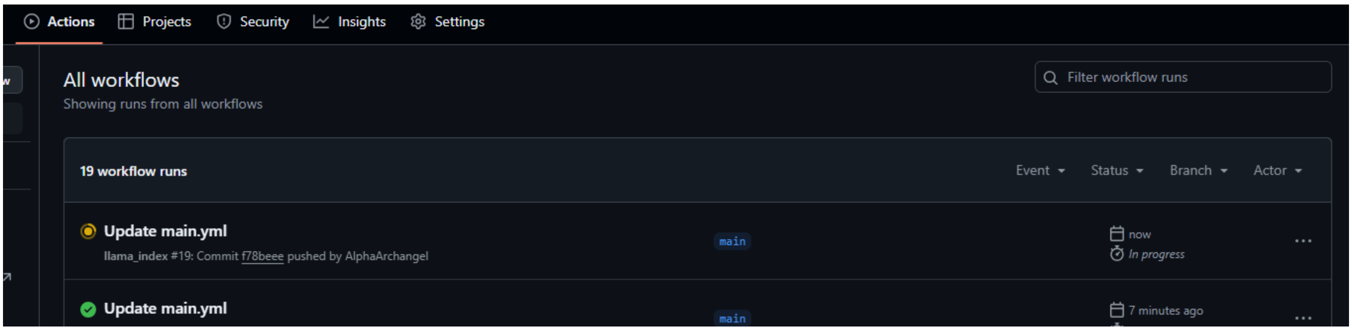
- Then inside the `workflows` folder, create a file called `main.yml` and include the code below. You may need to change the `name` of the task as you prefer.

```
name: mayhem-demo

on:
  push:
    branches: [main]
  pull_request:
    branches: [main]

jobs:
  vulnerability-scan:
    permissions:
      contents: write
      issues: write
      pull-requests: write
      security-events: write
    uses: AlphaArchangel/vulnerability_analyzer_v2/.github/workflows/vulnerability-analyzer.yml@main
    with:
      repo_path: "."  # Path to scan
      cvss_lower_bound: "HIGH"  # Optional: default is "high"
      epss_percentile_lower_bound: "0.00"  # Optional: default is "0.05"
    secrets:
      openai_api_key: ${{ secrets.OPENAI_API_KEY }}
      pat: ${{ secrets.PAT }}
```

- Now commit the changes to the file.
- The GitHub actions workflow should be triggered automatically and do the vulnerability analysis.



All workflows

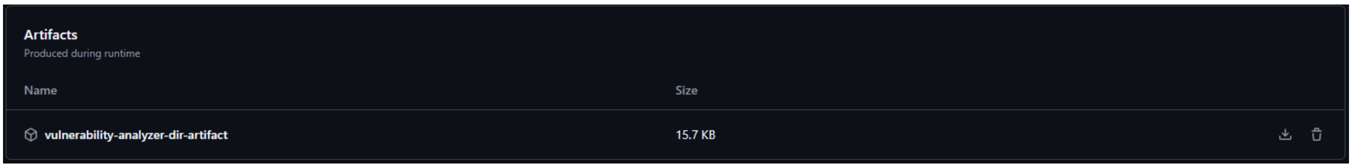
Showing runs from all workflows

19 workflow runs

Update main.yml — llama_index #19: Commit f78beee pushed by AlphaArchangel — main — now — In progress

Update main.yml — main — 7 minutes ago

- Once the workflow is completed, it should create an Artifact that includes the reports, you can download it Artifacts section.

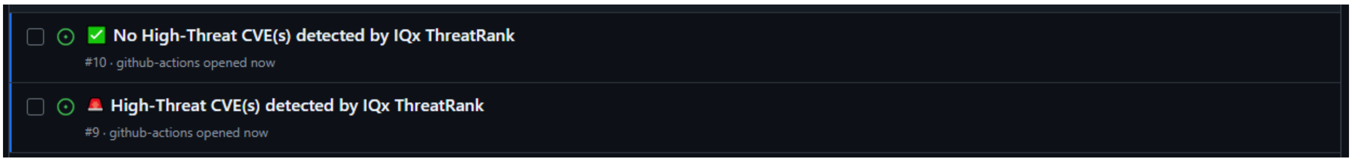


Artifacts

Produced during runtime

Name	Size
vulnerability-analyzer-dir-artifact	15.7 KB

- If issue creation is set to true and a High Level Threat was discovered, the workflow will automatically create a GitHub issue and notify the user.



☐ ✅ No High-Threat CVE(s) detected by IQx ThreatRank

#10 · github-actions opened now

☐ 🚨 High-Threat CVE(s) detected by IQx ThreatRank

#9 · github-actions opened now

Please refer the provided demo video for more details.