

Vulnerability Analyzer

This is a GitHub Actions Reusable 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
1  name: Vulnerability Analyzer
2  env:
3    REPO_USER: AlphaArchangel
4    REPO_NAME: vulnerability_analyzer_v2
5    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.](#)

Save

- 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**

Save

- After these steps the Reusable Repe setup is complete.

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 already 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.

Secrets

Variables

Repository secrets

New repository secret

Name	Last updated
<code>OPENAI_API_KEY</code>	42 minutes ago
<code>PAT</code>	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 History

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.

```

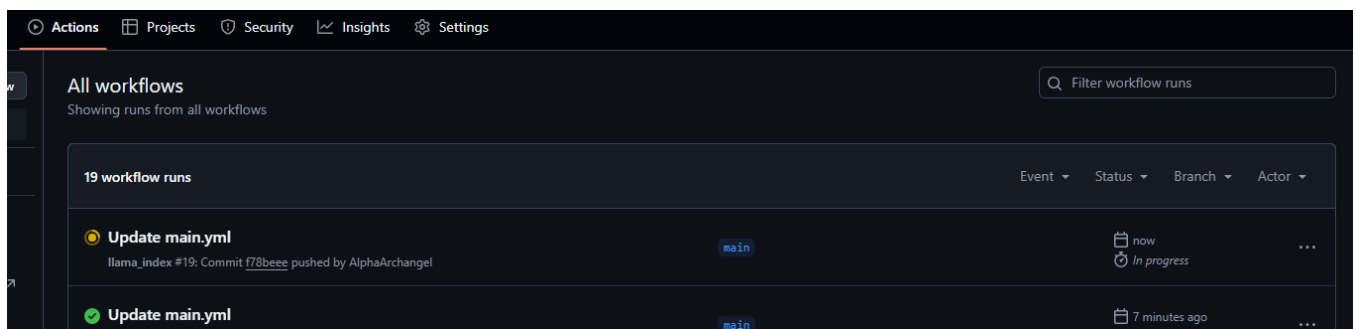
name: llama_index

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

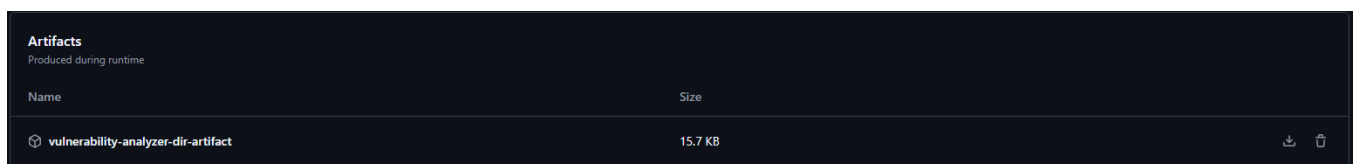
jobs:
  vulnerability-scan:
    permissions:
      contents: read
      security-events: write
    uses: AlphaArchangel/vulnerability_analyzer_v2/.github/workflows/vulnerability-analyzer.yml@main
    with:
      repo_path: "." # Path to scan
      cvss_lower_bound: "HIGH" # Optional: default is "high"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

```

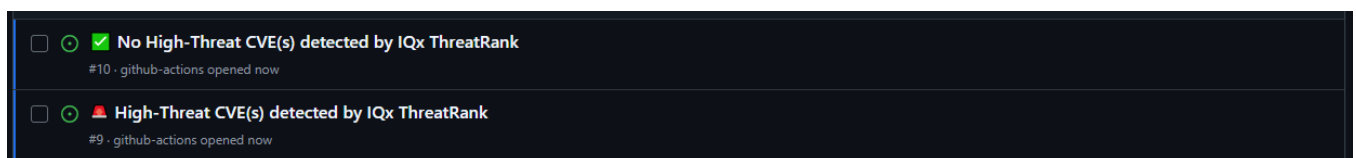
- Now commit the changes to the file.
- The GitHub actions workflow should be triggered automatically and do the vulnerability analysis.



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



- 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.



Please refer the provided demo video for more details.