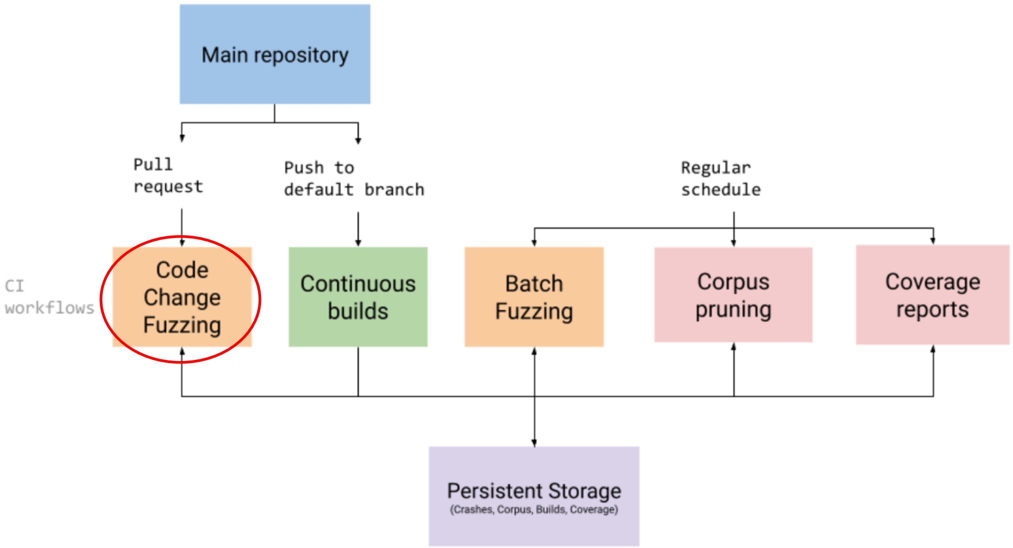
Lab6 (Part 2)： Fuzz Test and CI/CD: GitHub Actions

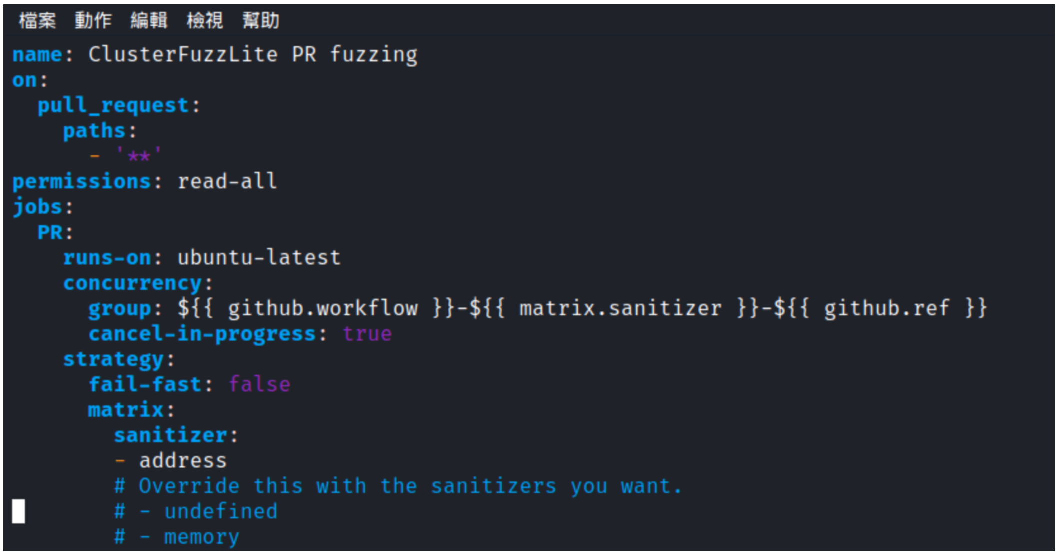
I. Fuzz Test and CI/CD

1. Use the google **culsterfuzzlite** as the example (https://google.github.io/clusterfuzzlite/)

Overview



2. We just test PR fuzzing (Code Change!)
   (1) Create a new repository fuzzexample2 in your GitHub, and create a first file named README.md
   (2) Clone your repository to your local machine
   git colone git@github.com:wangch64/fuzzexample2.git
   cd fuzzexample2
   (3) Create workflow file for GitHub Actions
   mkdir .github
   cd .github
   mkdir workflows
   cd workflows
   vi clite.yml
3. The yml example can be copied from https://google.github.io/clusterfuzzlite/running-clusterfuzzlite/github-actions/



```
name: ClusterFuzzLite PR fuzzing
on:
  pull_request:
    paths:
      - '**'
permissions: read-all
jobs:
  PR:
    runs-on: ubuntu-latest
    concurrency:
      group: ${{ github.workflow }}-${{ matrix.sanitizer }}-${{ github.ref }}
      cancel-in-progress: true
    strategy:
      fail-fast: false
      matrix:
        sanitizer:
        - address
        # Override this with the sanitizers you want.
        # - undefined
        # - memory
```

4. In ~/fuzzexample2

   Create .clusterfuzzlite folder

   mkdir .clusterfuzzlite

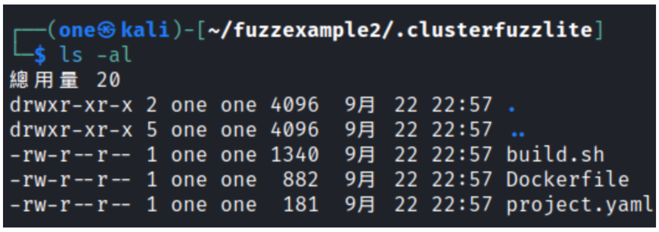
   cd .clusterfuzzlite

5. Copy three files from the example project (https://github.com/google/oss-fuzz/tree/master/projects/example) into **.clusterfuzzlite** folder

   Dockerfile

   build.sh

   project.yaml

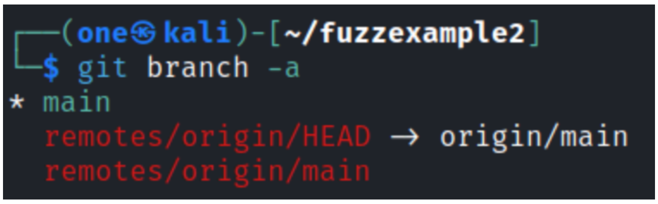


```
┌──(one㉿kali)-[~/fuzzexample2/.clusterfuzzlite]
└─$ ls -al
總用量 20
drwxr-xr-x 2 one one 4096  9月  22 22:57 .
drwxr-xr-x 5 one one 4096  9月  22 22:57 ..
-rw-r--r-- 1 one one 1340  9月  22 22:57 build.sh
-rw-r--r-- 1 one one  882  9月  22 22:57 Dockerfile
-rw-r--r-- 1 one one  181  9月  22 22:57 project.yaml
```

6. Modify the Dockerfile as in the following:

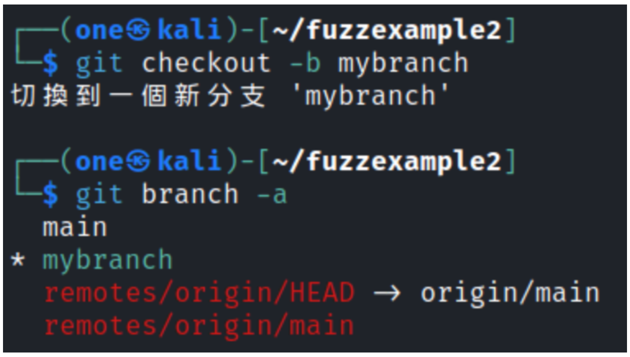
```
FROM gcr.io/oss-fuzz-base/base-builder
RUN apt-get update && apt-get install -y make

# Get *your* source code here.
RUN git clone https://github.com/google/oss-fuzz.git my-git-repo
WORKDIR my-git-repo
COPY ./.clusterfuzzlite/build.sh $SRC/
```

7. You should create **a new branch** in your local repository
   git branch -a



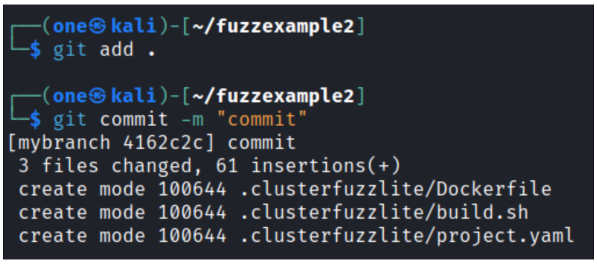
```
┌──(one㉿kali)-[~/fuzzexample2]
└─$ git branch -a
* main
  remotes/origin/HEAD → origin/main
  remotes/origin/main
```

   git checkout -b mybranch
   git branch -a



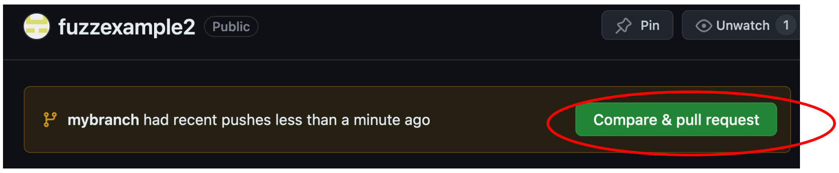
```
┌──(one㉿kali)-[~/fuzzexample2]
└─$ git checkout -b mybranch
切換到一個新分支 'mybranch'

┌──(one㉿kali)-[~/fuzzexample2]
└─$ git branch -a
  main
* mybranch
  remotes/origin/HEAD → origin/main
  remotes/origin/main
```

8. Do pull request:
   git add .
   git commit -m "commit"
   git push -u origin **mybranch**

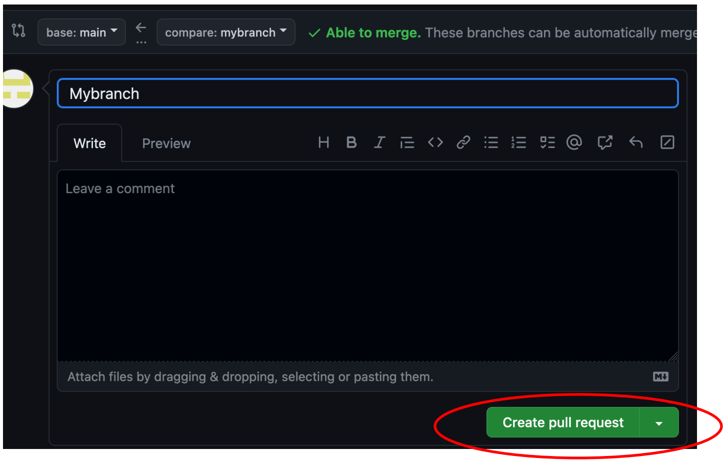


```
┌──(one㉿kali)-[~/fuzzexample2]
└─$ git add .

┌──(one㉿kali)-[~/fuzzexample2]
└─$ git commit -m "commit"
[mybranch 4162c2c] commit
 3 files changed, 61 insertions(+)
 create mode 100644 .clusterfuzzlite/Dockerfile
 create mode 100644 .clusterfuzzlite/build.sh
 create mode 100644 .clusterfuzzlite/project.yaml
```

9. In your GitHub, you can see mybranch a pull request



mybranch had recent pushes less than a minute ago



base: main ← compare: mybranch ✓ Able to merge. These branches can be automatically merge

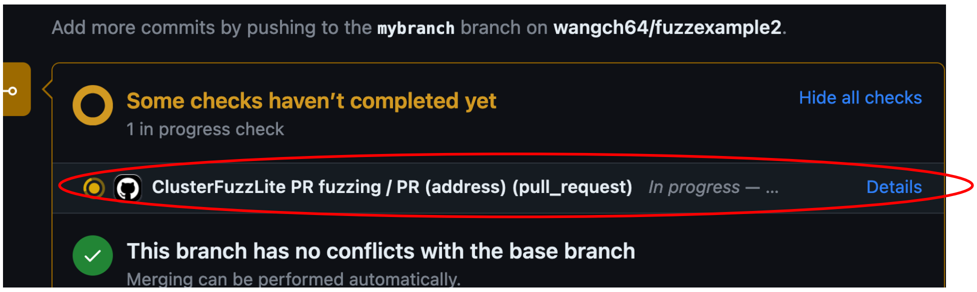
Mybranch

Write Preview

Leave a comment

Attach files by dragging & dropping, selecting or pasting them.

Create pull request



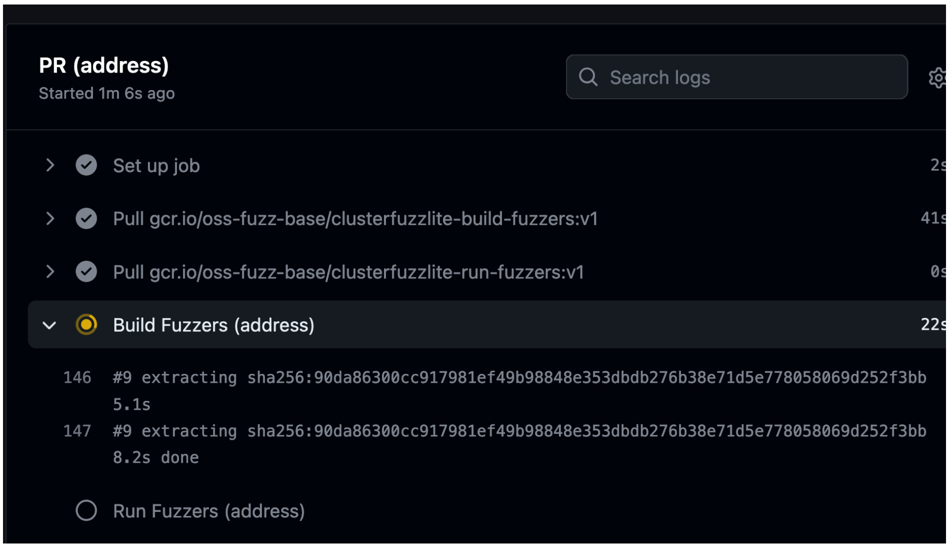
Add more commits by pushing to the **mybranch** branch on **wangch64/fuzzexample2**.

Some checks haven't completed yet
1 in progress check
Hide all checks

ClusterFuzzLite PR fuzzing / PR (address) (pull_request) *In progress — ...* Details

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

10. Build and Run Fuzzer



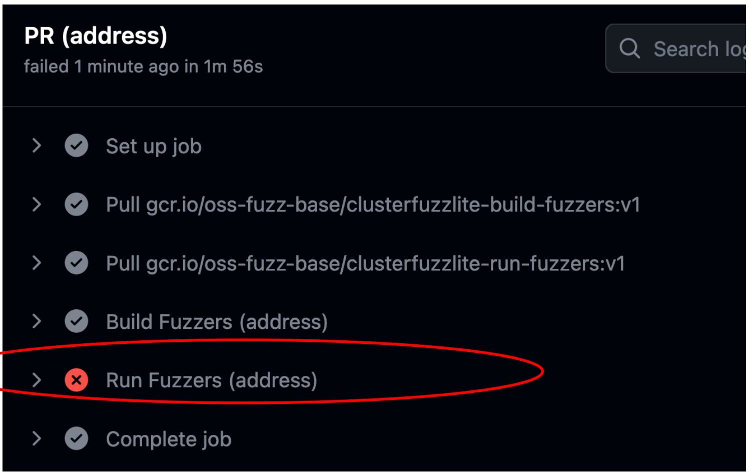
PR (address)
Started 1m 6s ago

Search logs

Set up job 2s
Pull gcr.io/oss-fuzz-base/clusterfuzzlite-build-fuzzers:v1 41s
Pull gcr.io/oss-fuzz-base/clusterfuzzlite-run-fuzzers:v1 0s
Build Fuzzers (address) 22s

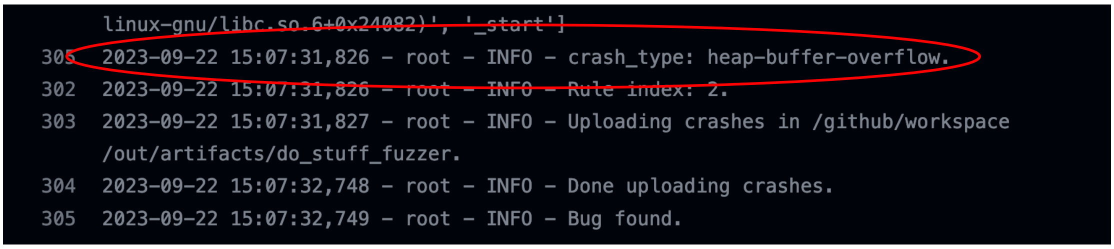
```
146  #9 extracting sha256:90da86300cc917981ef49b98848e353dbdb276b38e71d5e778058069d252f3bb
     5.1s
147  #9 extracting sha256:90da86300cc917981ef49b98848e353dbdb276b38e71d5e778058069d252f3bb
     8.2s done
```

○ Run Fuzzers (address)



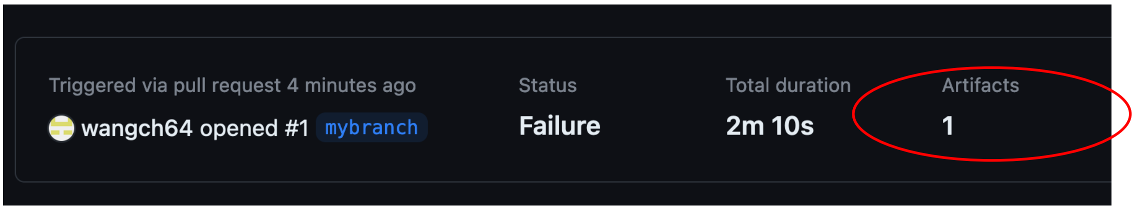
PR (address)
failed 1 minute ago in 1m 56s

- ✓ Set up job
- ✓ Pull gcr.io/oss-fuzz-base/clusterfuzzlite-build-fuzzers:v1
- ✓ Pull gcr.io/oss-fuzz-base/clusterfuzzlite-run-fuzzers:v1
- ✓ Build Fuzzers (address)
- ✗ Run Fuzzers (address)
- ✓ Complete job

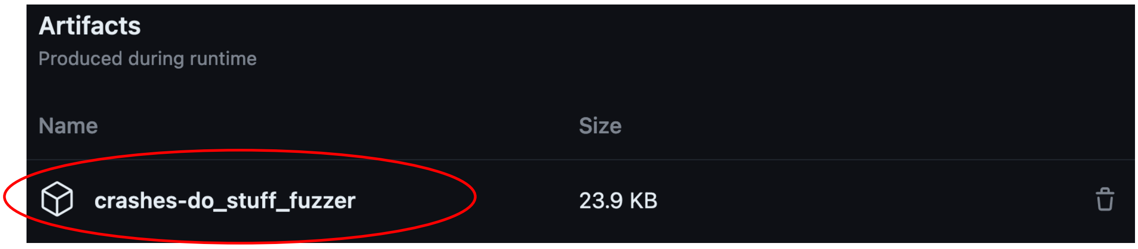


```
linux-gnu/libc.so.6+0x24082)', '_start']
2023-09-22 15:07:31,826 - root - INFO - crash_type: heap-buffer-overflow.
2023-09-22 15:07:31,826 - root - INFO - Rule index: 2.
2023-09-22 15:07:31,827 - root - INFO - Uploading crashes in /github/workspace
/out/artifacts/do_stuff_fuzzer.
2023-09-22 15:07:32,748 - root - INFO - Done uploading crashes.
2023-09-22 15:07:32,749 - root - INFO - Bug found.
```

11. Download the artifacts



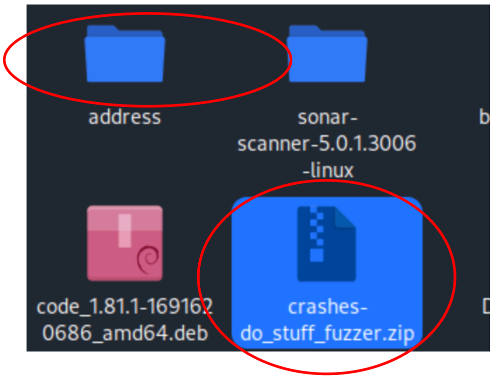
Triggered via pull request 4 minutes ago	Status	Total duration	Artifacts
wangch64 opened #1 mybranch	Failure	2m 10s	1



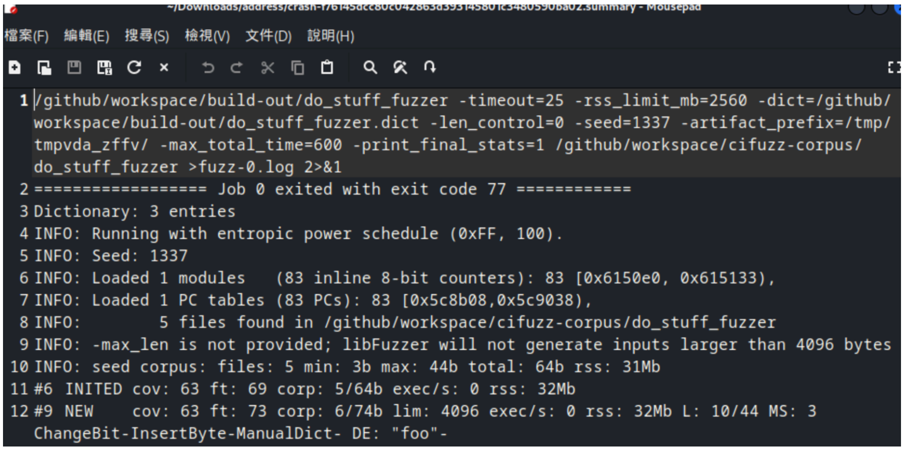
Artifacts
Produced during runtime

Name	Size
crashes-do_stuff_fuzzer	23.9 KB

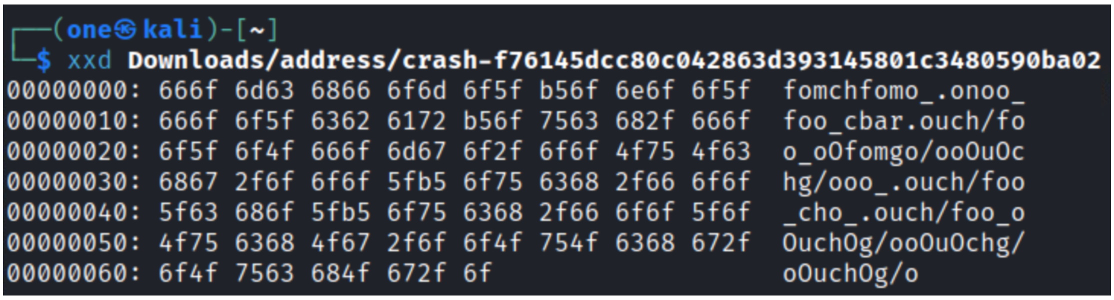
12. You can see the summary and test the crashes in your local computer!



address
sonar-scanner-5.0.1.3006-linux
code_1.81.1-1691620686_amd64.deb
crashes-do_stuff_fuzzer.zip


~/Downloads/address/crash-f76145dcc80c042863d393145801c3480590ba02.summary - Mousepad
檔案(F) 編輯(E) 搜尋(S) 檢視(V) 文件(D) 說明(H)

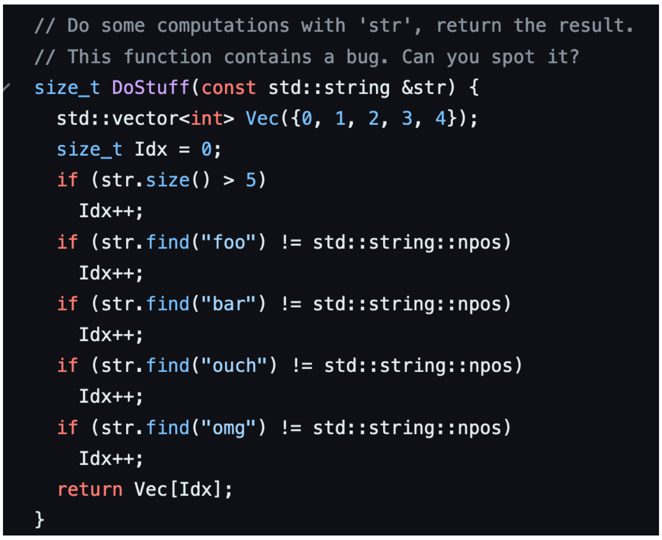
```
/github/workspace/build-out/do_stuff_fuzzer -timeout=25 -rss_limit_mb=2560 -dict=/github/
workspace/build-out/do_stuff_fuzzer.dict -len_control=0 -seed=1337 -artifact_prefix=/tmp/
tmpvda_zffv/ -max_total_time=600 -print_final_stats=1 /github/workspace/cifuzz-corpus/
do_stuff_fuzzer >fuzz-0.log 2>&1
================== Job 0 exited with exit code 77 ============
Dictionary: 3 entries
INFO: Running with entropic power schedule (0xFF, 100).
INFO: Seed: 1337
INFO: Loaded 1 modules   (83 inline 8-bit counters): 83 [0x6150e0, 0x615133),
INFO: Loaded 1 PC tables (83 PCs): 83 [0x5c8b08,0x5c9038),
INFO:        5 files found in /github/workspace/cifuzz-corpus/do_stuff_fuzzer
INFO: -max_len is not provided; libFuzzer will not generate inputs larger than 4096 bytes
INFO: seed corpus: files: 5 min: 3b max: 44b total: 64b rss: 31Mb
#6  INITED cov: 63 ft: 69 corp: 5/64b exec/s: 0 rss: 32Mb
#9  NEW    cov: 63 ft: 73 corp: 6/74b lim: 4096 exec/s: 0 rss: 32Mb L: 10/44 MS: 3
ChangeBit-InsertByte-ManualDict- DE: "foo"-
```



```
┌──(one㉿kali)-[~]
└─$ xxd Downloads/address/crash-f76145dcc80c042863d393145801c3480590ba02
00000000: 666f 6d63 6866 6f6d 6f5f b56f 6e6f 6f5f  fomchfomo_.onoo_
00000010: 666f 6f5f 6362 6172 b56f 7563 682f 666f  foo_cbar.ouch/fo
00000020: 6f5f 6f4f 666f 6d67 6f2f 6f6f 4f75 4f63  o_oOfomgo/ooOuOc
00000030: 6867 2f6f 6f6f 5fb5 6f75 6368 2f66 6f6f  hg/ooo_.ouch/foo
00000040: 5f63 686f 5fb5 6f75 6368 2f66 6f6f 5f6f  _cho_.ouch/foo_o
00000050: 4f75 6368 4f67 2f6f 6f4f 754f 6368 672f  OuchOg/ooOuOchg/
00000060: 6f4f 7563 684f 672f 6f                   oOuchOg/o
```

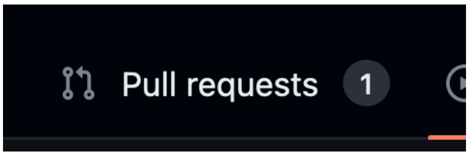
Clone the original project and test the crash!

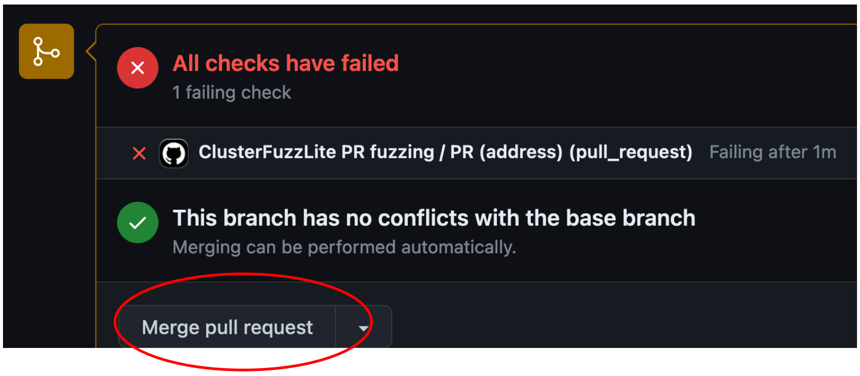
(a modified cpp file can be downloaded from sharefiles)



```cpp
// Do some computations with 'str', return the result.
// This function contains a bug. Can you spot it?
size_t DoStuff(const std::string &str) {
  std::vector<int> Vec({0, 1, 2, 3, 4});
  size_t Idx = 0;
  if (str.size() > 5)
    Idx++;
  if (str.find("foo") != std::string::npos)
    Idx++;
  if (str.find("bar") != std::string::npos)
    Idx++;
  if (str.find("ouch") != std::string::npos)
    Idx++;
  if (str.find("omg") != std::string::npos)
    Idx++;
  return Vec[Idx];
}
```

13. Compare the branches and merge them



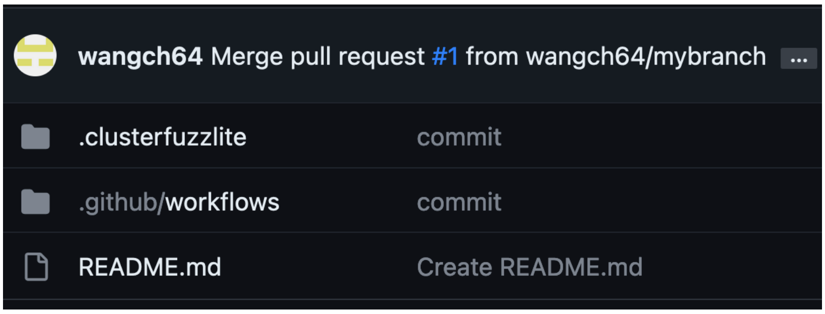


✕ All checks have failed
1 failing check

✕ ClusterFuzzLite PR fuzzing / PR (address) (pull_request) Failing after 1m

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

And confirm merage!



wangch64 Merge pull request #1 from wangch64/mybranch ...

.clusterfuzzlite	commit
.github/workflows	commit
README.md	Create README.md