Final Writeup

p7zip

Arnav Nidumolu, Atharva Kale, Pascal von Fintel, Patrick Negus

2023-05-14

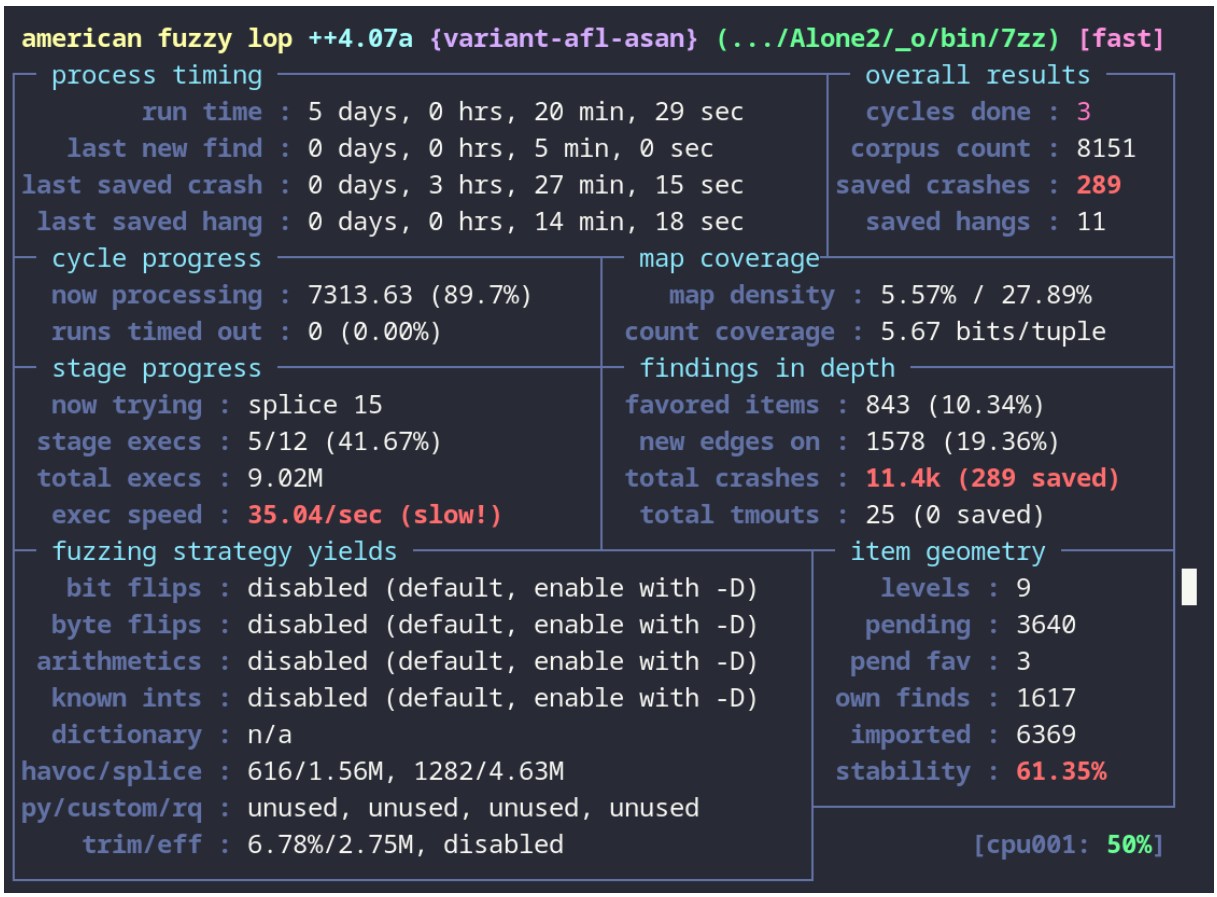
Checkpoint 1

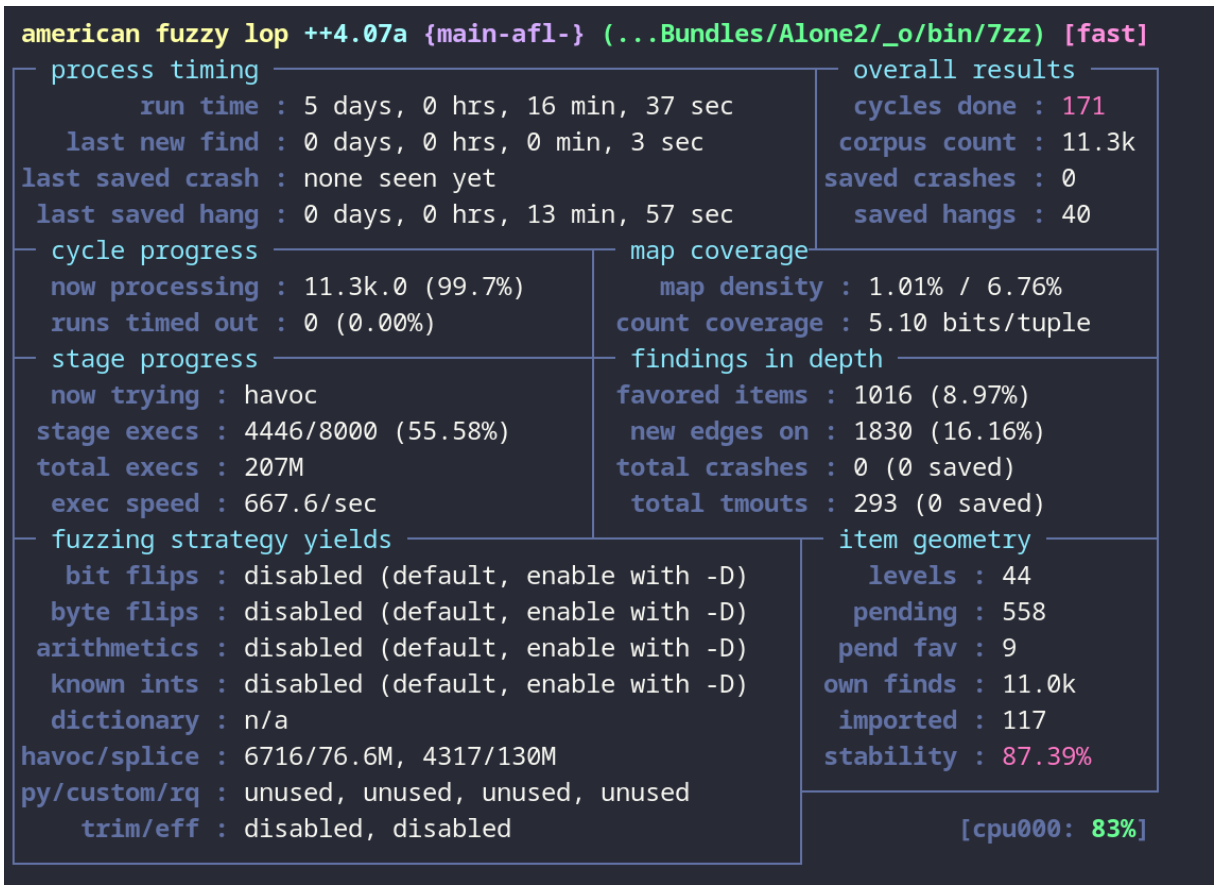
```
Public Github Repository - This should include all code you wrote for
    eg. static analysis, fuzzing harnesses, etc. If you built your
    target with instrumentation for the purposes of fuzzing, this should
     also include build scripts. If you performed reverse engineering on
     your target and eg. started renaming variables/functions/did work
    on that front, include the relevant ghidra files as well.

Start your writeup with a description of what you learned about this
    target. This should include some notes about the code layout, maybe
    some coding practices you noticed while going through the target or
    just more general functionality. Which parts of the target did you
    think were most interesting for the purposes of finding bugs?

Describe what you chose for your automated analysis portion and why.
    How did you set this up, did you encounter issues (eg. slow fuzzer
    performance), and if so what did you to improve on these issues.

What were the biggest challenges you faced when dealing with your
    target?

If given more time, what do you think would be good next steps to
    continue doing research on the target with the goal of finding bugs?
```

Contents:

- Github Repository
- Overview of the Target
  - Code Layout
  - Coding Observations
  - Analyzing a Target Feature
- Automated Analysis
  - Fuzzing
    - How was it set up
    - Results etc…
  - Static Analysis
    - …
- Challenges Faced
  - …

- Next Steps


american fuzzy lop ++4.07a {variant-afl-asan} (.../Alone2/_o/bin/7zz) [fast]
process timing
run time : 5 days, 0 hrs, 20 min, 29 sec
last new find : 0 days, 0 hrs, 5 min, 0 sec
last saved crash : 0 days, 3 hrs, 27 min, 15 sec
last saved hang : 0 days, 0 hrs, 14 min, 18 sec
overall results
cycles done : 3
corpus count : 8151
saved crashes : 289
saved hangs : 11
cycle progress
now processing : 7313.63 (89.7%)
runs timed out : 0 (0.00%)
map coverage
map density : 5.57% / 27.89%
count coverage : 5.67 bits/tuple
stage progress
now trying : splice 15
stage execs : 5/12 (41.67%)
total execs : 9.02M
exec speed : 35.04/sec (slow!)
findings in depth
favored items : 843 (10.34%)
new edges on : 1578 (19.36%)
total crashes : 11.4k (289 saved)
total tmouts : 25 (0 saved)
fuzzing strategy yields
bit flips : disabled (default, enable with -D)
byte flips : disabled (default, enable with -D)
arithmetics : disabled (default, enable with -D)
known ints : disabled (default, enable with -D)
dictionary : n/a
havoc/splice : 616/1.56M, 1282/4.63M
py/custom/rq : unused, unused, unused, unused
trim/eff : 6.78%/2.75M, disabled
item geometry
levels : 9
pending : 3640
pend fav : 3
own finds : 1617
imported : 6369
stability : 61.35%
[cpu001: 50%]


american fuzzy lop ++4.07a {main-afl-} (...Bundles/Alone2/_o/bin/7zz) [fast]
process timing
run time : 5 days, 0 hrs, 16 min, 37 sec
last new find : 0 days, 0 hrs, 0 min, 3 sec
last saved crash : none seen yet
last saved hang : 0 days, 0 hrs, 13 min, 57 sec
overall results
cycles done : 171
corpus count : 11.3k
saved crashes : 0
saved hangs : 40
cycle progress
now processing : 11.3k.0 (99.7%)
runs timed out : 0 (0.00%)
map coverage
map density : 1.01% / 6.76%
count coverage : 5.10 bits/tuple
stage progress
now trying : havoc
stage execs : 4446/8000 (55.58%)
total execs : 207M
exec speed : 667.6/sec
findings in depth
favored items : 1016 (8.97%)
new edges on : 1830 (16.16%)
total crashes : 0 (0 saved)
total tmouts : 293 (0 saved)
fuzzing strategy yields
bit flips : disabled (default, enable with -D)
byte flips : disabled (default, enable with -D)
arithmetics : disabled (default, enable with -D)
known ints : disabled (default, enable with -D)
dictionary : n/a
havoc/splice : 6716/76.6M, 4317/130M
py/custom/rq : unused, unused, unused, unused
trim/eff : disabled, disabled
item geometry
levels : 44
pending : 558
pend fav : 9
own finds : 11.0k
imported : 117
stability : 87.39%
[cpu000: 83%]