

The Fuzzing Project

<https://fuzzing-project.org/>

Hanno Böck

- Did you expect to be owned by file, strings or less?
- You should!

What is Fuzzing?

- Take a valid input, add random errors, feed software with it
- If software crashes (or shows other undesired behaviour) you found a bug
- Crashes very often memory access issues, potential security threats

State of our software base

- Pick a random free software tool that parses files, fuzz it
- Chances are high you'll find bugs within seconds

- Address Sanitizer: compiler flag that enables better bounds checking - highly effective in finding memory access issues
- american fuzzy lop: intelligent fuzzer with compile time instrumentation - already found dozens of issues, often in security sensitive software (GnuPG, libjpeg, bash, ...)

```
american fuzzy lop 0.94b (unrfl)
-----
process timing:
  run time : 0 days, 0 hrs, 0 min, 37 sec
  last new path : 0 days, 0 hrs, 0 min, 0 sec
  last uniq crash : 0 days, 0 hrs, 0 min, 21 sec
  last uniq hang : none seen yet
cycle progress:
  now processing : 0 (0.00%)
  paths fised out : 0 (0.00%)
stage progress:
  now trying : bitflip 2/1
  stage execs : 7406/13.3k (55.57%)
  total execs : 24.2k
  exec speed : 546.5/sec
fuzzing strategy yields:
  bit flips : 220/13.3k, 0/0, 0/0
  byte flips : 0/0, 0/0, 0/0
  arithmetics : 0/0, 0/0, 0/0
  known ints : 0/0, 0/0, 0/0
  havoc : 0/0, 0/0
  trie : 4 B/820 (0.24% gain)
overall results:
  cycles done : 0
  total paths : 268
  uniq crashes : 1
  uniq hangs : 0
map coverage:
  map density : 1360 (2.08%)
  count coverage : 2.62 bits/tuple
findings in depth:
  favored paths : 1 (0.37%)
  new edges on : 118 (44.03%)
  total crashes : 5 (1 unique)
  total hangs : 0 (0 unique)
path geometry:
  levels : 2
  pending : 268
  pend fav : 1
  own finds : 267
  imported : 0
  variable : 0
[cpu: 29%]
```

The Fuzzing Project

- Some loose coordination and documentation of fuzzing efforts, list of free software projects and their fuzzing robustness
- Tutorial for beginners
- Small sample files archive
- Goal: Wipe out bugs that can be trivially found by fuzzing

What you can do

- If you are a software developer: Make fuzzing part of your development process
- If you care about free software security: Help us fuzz everything

<https://fuzzing-project.org/>

