HW2. Fuzzing

L091025 清大資工所 熊詩旻

Task1—CVE-2014-0160(openssl)

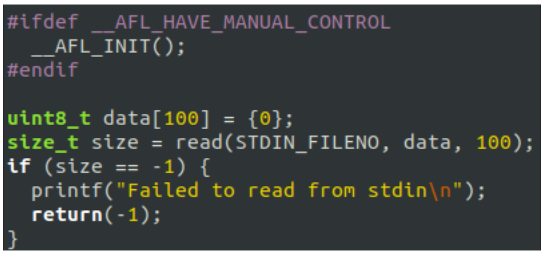
Steps:

1. Configure and build with ASAN

   `CC=afl-clang-fast CXX=afl-clang-fast++ ./config –d`

   `AFL_USE_ASAN=1 make`

2. Add the code below to complete the harness.



```
#ifdef __AFL_HAVE_MANUAL_CONTROL
  __AFL_INIT();
#endif

uint8_t data[100] = {0};
size_t size = read(STDIN_FILENO, data, 100);
if (size == -1) {
  printf("Failed to read from stdin\n");
  return(-1);
}
```

3. Compile the harness

   `AFL_USE_ASAN=1 afl-clang-fast++ -g harness.cc openssl-1.0.1f/libssl.a openssl-1.0.1f/libcrypto.a -o handshake -I openssl-1.0.1f/include -ldl`

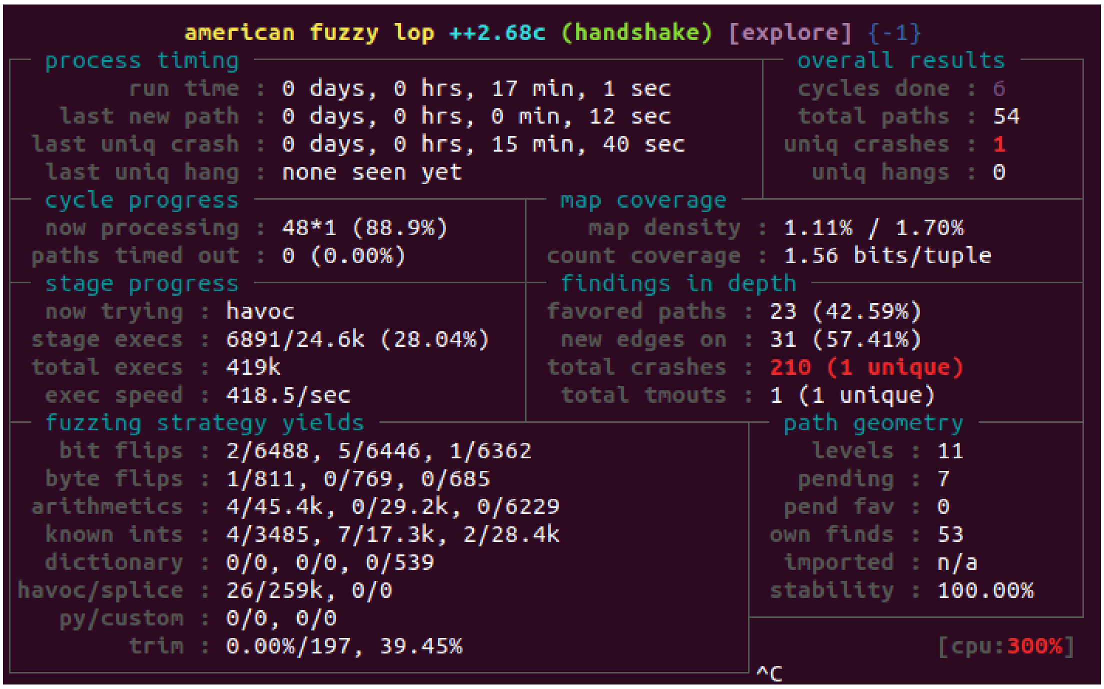
4. Create input seeds

   `mkdir in`

   `echo “iamseed” > in/a`

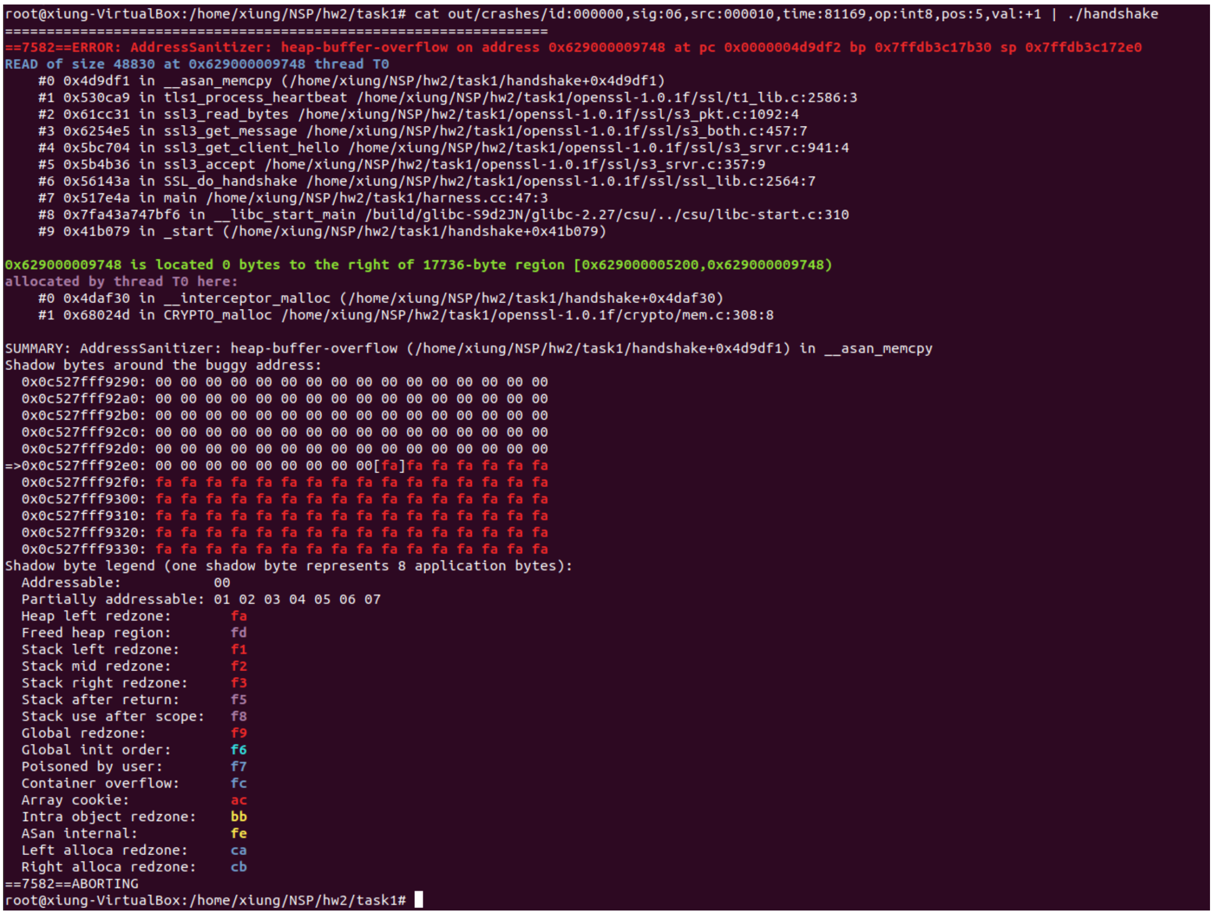
5. Fuzzing

   `afl-fuzz -i in -o out -m none ./handshake`



```
              american fuzzy lop ++2.68c (handshake) [explore] {-1}
┌─ process timing ─────────────────────────────────────┬─ overall results ────┐
│        run time : 0 days, 0 hrs, 17 min, 1 sec       │  cycles done : 6      │
│   last new path : 0 days, 0 hrs, 0 min, 12 sec       │  total paths : 54     │
│ last uniq crash : 0 days, 0 hrs, 15 min, 40 sec      │ uniq crashes : 1      │
│  last uniq hang : none seen yet                      │   uniq hangs : 0      │
├─ cycle progress ─────────────────┬─ map coverage ─┴───────────────────────┤
│  now processing : 48*1 (88.9%)   │    map density : 1.11% / 1.70%         │
│ paths timed out : 0 (0.00%)      │ count coverage : 1.56 bits/tuple       │
├─ stage progress ─────────────────┼─ findings in depth ────────────────────┤
│  now trying : havoc              │ favored paths : 23 (42.59%)            │
│ stage execs : 6891/24.6k (28.04%)│  new edges on : 31 (57.41%)            │
│ total execs : 419k               │ total crashes : 210 (1 unique)         │
│  exec speed : 418.5/sec          │  total tmouts : 1 (1 unique)           │
├─ fuzzing strategy yields ────────┴──────────────┬─ path geometry ────────┤
│   bit flips : 2/6488, 5/6446, 1/6362            │    levels : 11         │
│  byte flips : 1/811, 0/769, 0/685               │   pending : 7          │
│ arithmetics : 4/45.4k, 0/29.2k, 0/6229          │  pend fav : 0          │
│  known ints : 4/3485, 7/17.3k, 2/28.4k          │ own finds : 53         │
│  dictionary : 0/0, 0/0, 0/539                   │  imported : n/a        │
│havoc/splice : 26/259k, 0/0                      │ stability : 100.00%    │
│   py/custom : 0/0, 0/0                          ├────────────────────────┘
│        trim : 0.00%/197, 39.45%                 │          [cpu:300%]
└─────────────────────────────────────────────────┘^C
```

6. See the crashes

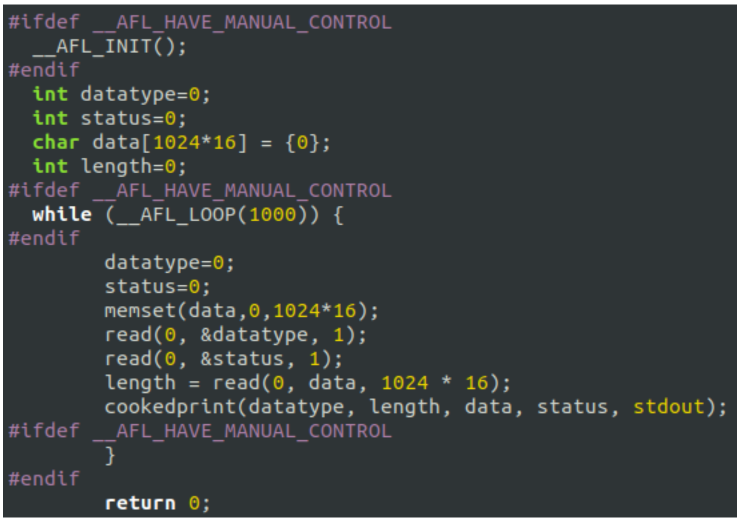


```
root@xiung-VirtualBox:/home/xiung/NSP/hw2/task1# cat out/crashes/id:000000,sig:06,src:000010,time:81169,op:int8,pos:5,val:+1 | ./handshake
=================================================================
==7582==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x629000009748 at pc 0x0000004d9df2 bp 0x7ffdb3c17b30 sp 0x7ffdb3c172e0
READ of size 48830 at 0x629000009748 thread T0
    #0 0x4d9df1 in __asan_memcpy (/home/xiung/NSP/hw2/task1/handshake+0x4d9df1)
    #1 0x530ca9 in tls1_process_heartbeat /home/xiung/NSP/hw2/task1/openssl-1.0.1f/ssl/t1_lib.c:2586:3
    #2 0x61cc31 in ssl3_read_bytes /home/xiung/NSP/hw2/task1/openssl-1.0.1f/ssl/s3_pkt.c:1092:4
    #3 0x6254e5 in ssl3_get_message /home/xiung/NSP/hw2/task1/openssl-1.0.1f/ssl/s3_both.c:457:7
    #4 0x5bc704 in ssl3_get_client_hello /home/xiung/NSP/hw2/task1/openssl-1.0.1f/ssl/s3_srvr.c:941:4
    #5 0x5b4b36 in ssl3_accept /home/xiung/NSP/hw2/task1/openssl-1.0.1f/ssl/s3_srvr.c:357:9
    #6 0x56143a in SSL_do_handshake /home/xiung/NSP/hw2/task1/openssl-1.0.1f/ssl/ssl_lib.c:2564:7
    #7 0x517e4a in main /home/xiung/NSP/hw2/task1/harness.cc:47:3
    #8 0x7fa43a747bf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-start.c:310
    #9 0x41b079 in _start (/home/xiung/NSP/hw2/task1/handshake+0x41b079)

0x629000009748 is located 0 bytes to the right of 17736-byte region [0x629000005200,0x629000009748)
allocated by thread T0 here:
    #0 0x4daf30 in __interceptor_malloc (/home/xiung/NSP/hw2/task1/handshake+0x4daf30)
    #1 0x68024d in CRYPTO_malloc /home/xiung/NSP/hw2/task1/openssl-1.0.1f/crypto/mem.c:308:8

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/xiung/NSP/hw2/task1/handshake+0x4d9df1) in __asan_memcpy
Shadow bytes around the buggy address:
  0x0c527fff9290: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c527fff92a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c527fff92b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c527fff92c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c527fff92d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c527fff92e0: 00 00 00 00 00 00 00 00 00[fa]fa fa fa fa fa fa
  0x0c527fff92f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff9300: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff9310: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff9320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c527fff9330: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==7582==ABORTING
root@xiung-VirtualBox:/home/xiung/NSP/hw2/task1# 
```

Task2—CVE-2009-0159(ntpq)

Steps

1. Replace the code below to ntpqmain()



```
#ifdef __AFL_HAVE_MANUAL_CONTROL
  __AFL_INIT();
#endif
  int datatype=0;
  int status=0;
  char data[1024*16] = {0};
  int length=0;
#ifdef __AFL_HAVE_MANUAL_CONTROL
  while (__AFL_LOOP(1000)) {
#endif
        datatype=0;
        status=0;
        memset(data,0,1024*16);
        read(0, &datatype, 1);
        read(0, &status, 1);
        length = read(0, data, 1024 * 16);
        cookedprint(datatype, length, data, status, stdout);
#ifdef __AFL_HAVE_MANUAL_CONTROL
        }
#endif
        return 0;
```

2. Configure and build ntpq

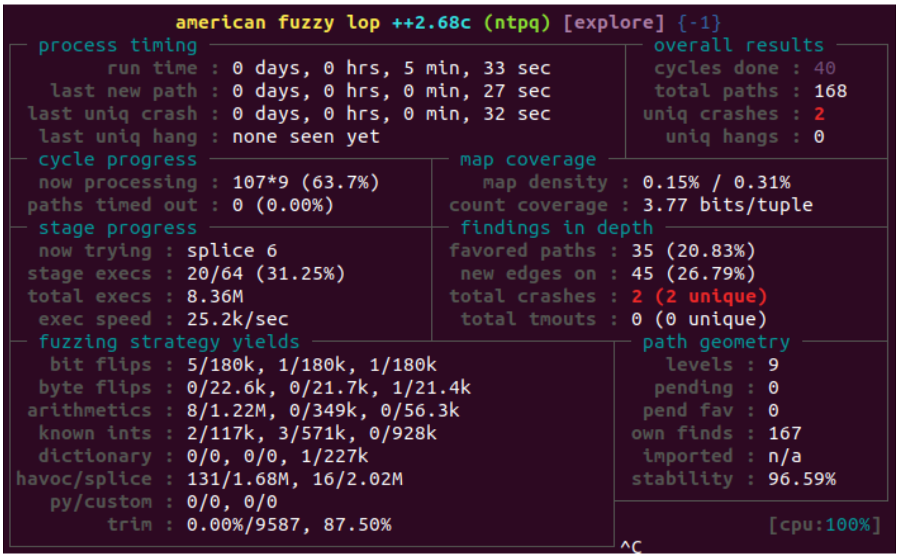
```
CC=afl-clang-fast ./configure
make -C ntpq
```

3. Create input seeds

```
mkdir in
echo “iamseed” > in/a
```

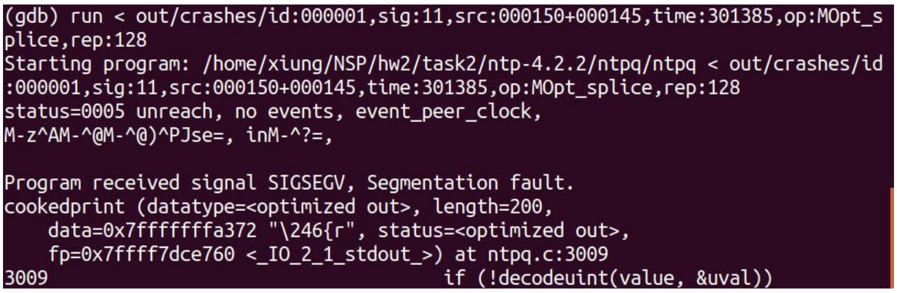
4. Fuzzing without dictionary

```
afl-fuzz -i in -o out ntp-4.2.2/ntpq/ntpq
```



```
              american fuzzy lop ++2.68c (ntpq) [explore] {-1}
┌─ process timing ────────────────────────────────────┬─ overall results ────┐
│        run time : 0 days, 0 hrs, 5 min, 33 sec      │  cycles done : 40    │
│   last new path : 0 days, 0 hrs, 0 min, 27 sec      │  total paths : 168   │
│ last uniq crash : 0 days, 0 hrs, 0 min, 32 sec      │ uniq crashes : 2     │
│  last uniq hang : none seen yet                     │   uniq hangs : 0     │
├─ cycle progress ───────────────────┬─ map coverage ─┴──────────────────────┤
│  now processing : 107*9 (63.7%)    │    map density : 0.15% / 0.31%        │
│ paths timed out : 0 (0.00%)        │ count coverage : 3.77 bits/tuple      │
├─ stage progress ───────────────────┼─ findings in depth ───────────────────┤
│  now trying : splice 6             │ favored paths : 35 (20.83%)           │
│ stage execs : 20/64 (31.25%)       │  new edges on : 45 (26.79%)           │
│ total execs : 8.36M                │ total crashes : 2 (2 unique)          │
│  exec speed : 25.2k/sec            │  total tmouts : 0 (0 unique)          │
├─ fuzzing strategy yields ──────────┴─────────────┬─ path geometry ────────┤
│   bit flips : 5/180k, 1/180k, 1/180k             │    levels : 9          │
│  byte flips : 0/22.6k, 0/21.7k, 1/21.4k          │   pending : 0          │
│ arithmetics : 8/1.22M, 0/349k, 0/56.3k           │  pend fav : 0          │
│  known ints : 2/117k, 3/571k, 0/928k             │ own finds : 167        │
│  dictionary : 0/0, 0/0, 1/227k                   │  imported : n/a        │
│havoc/splice : 131/1.68M, 16/2.02M                │ stability : 96.59%     │
│   py/custom : 0/0, 0/0                           ├────────────────────────┘
│        trim : 0.00%/9587, 87.50%                 │          [cpu:100%]
└──────────────────────────────────────────────────┘^C
```

Analyze with gdb

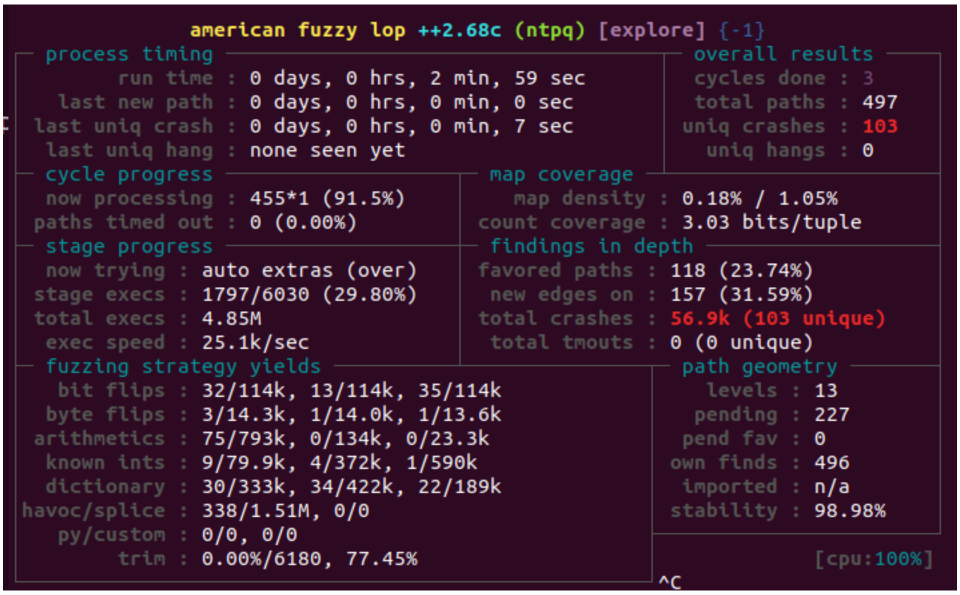


```
(gdb) run < out/crashes/id:000001,sig:11,src:000150+000145,time:301385,op:MOpt_s
plice,rep:128
Starting program: /home/xiung/NSP/hw2/task2/ntp-4.2.2/ntpq/ntpq < out/crashes/id
:000001,sig:11,src:000150+000145,time:301385,op:MOpt_splice,rep:128
status=0005 unreach, no events, event_peer_clock,
M-z^AM-^@M-^@)^PJse=, inM-^?=,

Program received signal SIGSEGV, Segmentation fault.
cookedprint (datatype=<optimized out>, length=200,
    data=0x7fffffffa372 "\246{r", status=<optimized out>,
    fp=0x7ffff7dce760 <_IO_2_1_stdout_>) at ntpq.c:3009
3009                                    if (!decodeuint(value, &uval))
```

See the segmentation fault.

5. Fuzzing with dictionary

```
afl-fuzz -i in -o out -x ntpq.dict ntp-4.2.2/ntpq/ntpq
```



```
              american fuzzy lop ++2.68c (ntpq) [explore] {-1}
┌─ process timing ────────────────────────────────────┬─ overall results ────┐
│        run time : 0 days, 0 hrs, 2 min, 59 sec      │  cycles done : 3     │
│   last new path : 0 days, 0 hrs, 0 min, 0 sec       │  total paths : 497   │
│ last uniq crash : 0 days, 0 hrs, 0 min, 7 sec       │ uniq crashes : 103   │
│  last uniq hang : none seen yet                     │   uniq hangs : 0     │
├─ cycle progress ───────────────────┬─ map coverage ─┴──────────────────────┤
│  now processing : 455*1 (91.5%)    │    map density : 0.18% / 1.05%        │
│ paths timed out : 0 (0.00%)        │ count coverage : 3.03 bits/tuple      │
├─ stage progress ───────────────────┼─ findings in depth ───────────────────┤
│  now trying : auto extras (over)   │ favored paths : 118 (23.74%)          │
│ stage execs : 1797/6030 (29.80%)   │  new edges on : 157 (31.59%)          │
│ total execs : 4.85M                │ total crashes : 56.9k (103 unique)    │
│  exec speed : 25.1k/sec            │  total tmouts : 0 (0 unique)          │
├─ fuzzing strategy yields ──────────┴─────────────┬─ path geometry ────────┤
│   bit flips : 32/114k, 13/114k, 35/114k          │    levels : 13         │
│  byte flips : 3/14.3k, 1/14.0k, 1/13.6k          │   pending : 227        │
│ arithmetics : 75/793k, 0/134k, 0/23.3k           │  pend fav : 0          │
│  known ints : 9/79.9k, 4/372k, 1/590k            │ own finds : 496        │
│  dictionary : 30/333k, 34/422k, 22/189k          │  imported : n/a        │
│havoc/splice : 338/1.51M, 0/0                     │ stability : 98.98%     │
│   py/custom : 0/0, 0/0                           ├────────────────────────┘
│        trim : 0.00%/6180, 77.45%                 │          [cpu:100%]
└──────────────────────────────────────────────────┘^C
```