

OT Lab 3 - Fuzzing

Student: *Ahmed Elkashef*

1. Playing with AFL:

Use AFL on any old source code and generate crashes. Verify these crashes. Explain what is happening from the crashes generated.

I will use AFL on fuzzgoat, which is an intentionally vulnerable application written to demonstrate fuzzing.

I will clone and cd into the directory of fuzzgoat:

```
git clone https://github.com/fuzzstati0n/fuzzgoat
cd fuzzgoat/
```

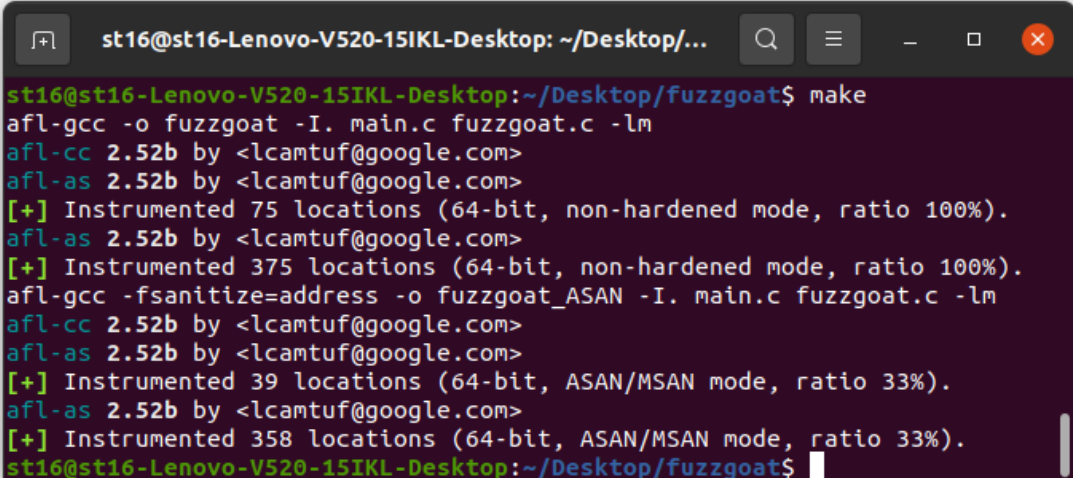
Then compile the binary with one of AFL's compilers:

```
export CC=afl-clang-fast
```

Noting that we can use any of the following:

- afl-clang-fast
- afl-clang-fast++
- afl-gcc
- afl-g++

Then we compile fuzzgoat into a binary:

A terminal window titled 'st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/...' displays the compilation of fuzzgoat. The user runs 'make', which triggers a series of commands: 'afl-gcc -o fuzzgoat -I. main.c fuzzgoat.c -lm', followed by 'afl-cc 2.52b by <lcamtuf@google.com>' and 'afl-as 2.52b by <lcamtuf@google.com>'. The output shows instrumentation of 75 locations (64-bit, non-hardened mode, ratio 100%) and 375 locations (64-bit, non-hardened mode, ratio 100%). Then, 'afl-gcc -fsanitize=address -o fuzzgoat_ASAN -I. main.c fuzzgoat.c -lm' is run, followed by another 'afl-cc' and 'afl-as' command. The output shows instrumentation of 39 locations (64-bit, ASAN/MSAN mode, ratio 33%) and 358 locations (64-bit, ASAN/MSAN mode, ratio 33%). The prompt returns to 'st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat\$'.

The next step is the test corpus, which is basically a “seed input file”, they are the starting point for AFL to mutate and generate new test files as it sees fit to discover new code paths.

I will start by making a directory, and piping some random, garbage value to the directory:

```
mkdir afl_in
cp /bin/ps afl_in/
```

The last thing is to specify where are the files that have resulted in a crash or a hang will be stored, let's call it afl_out:

```
mkdir afl_out
```

The last thing is to finally fuzz the application:

```
afl-fuzz -i afl_in -o afl_out -- ./fuzzgoat @@
```

- 1) -i specifies the input seed files
- 2) -o specifies the output files directory
- 3) -- separates the arguments from the target
- 4) ./fuzzgoat is the target
- 5) @@ is the position where AFL is supposed to insert the test file in the target application's command structure

```
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat

american fuzzy lop 2.52b (fuzzgoat)

process timing
  run time : 0 days, 0 hrs, 0 min, 17 sec
  last new path : 0 days, 0 hrs, 0 min, 0 sec
  last uniq crash : 0 days, 0 hrs, 0 min, 4 sec
  last uniq hang : none seen yet

cycle progress
  now processing : 9* (7.69%)
  paths timed out : 0 (0.00%)

stage progress
  now trying : havoc
  stage execs : 24.2k/24.6k (98.36%)
  total execs : 69.5k
  exec speed : 3928/sec

fuzzing strategy yields
  bit flips : 3/256, 1/248, 0/232
  byte flips : 0/32, 0/24, 0/8
  arithmetics : 7/1789, 0/61, 0/0
  known ints : 2/209, 1/669, 0/352
  dictionary : 0/0, 0/0, 0/0
  havoc : 81/40.4k, 0/0
  trim : 100.00%/20, 0.00%

overall results
  cycles done : 0
  total paths : 117
  uniq crashes : 2
  uniq hangs : 0

map coverage
  map density : 0.12% / 0.49%
  count coverage : 2.00 bits/tuple

findings in depth
  favored paths : 41 (35.04%)
  new edges on : 58 (49.57%)
  total crashes : 4 (2 unique)
  total tmouts : 0 (0 unique)

path geometry
  levels : 3
  pending : 110
  pend fav : 35
  own finds : 116
  imported : n/a
  stability : 100.00%

[cpu000: 70%]
```

I stop the fuzzing after I have generated some crashes:

```
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat

american fuzzy lop 2.52b (fuzzgoat)

process timing | overall results
  run time : 0 days, 0 hrs, 6 min, 15 sec | cycles done : 3
  last new path : 0 days, 0 hrs, 0 min, 1 sec | total paths : 348
  last uniq crash : 0 days, 0 hrs, 2 min, 35 sec | uniq crashes : 15
  last uniq hang : none seen yet | uniq hangs : 0
cycle progress | map coverage
  now processing : 345 (99.14%) | map density : 0.21% / 0.76%
  paths timed out : 0 (0.00%) | count coverage : 2.83 bits/tuple
stage progress | findings in depth
  now trying : havoc | favored paths : 89 (25.57%)
  stage execs : 8856/24.6k (36.04%) | new edges on : 126 (36.21%)
  total execs : 1.56M | total crashes : 3132 (15 unique)
  exec speed : 4120/sec | total tmouts : 1 (1 unique)
fuzzing strategy yields | path geometry
  bit flips : 24/17.7k, 11/17.5k, 8/17.1k | levels : 15
  byte flips : 0/2207, 0/2005, 0/1632 | pending : 147
  arithmetics : 27/123k, 0/28.0k, 0/1619 | pend fav : 1
  known ints : 6/11.5k, 2/54.3k, 0/71.2k | own finds : 347
  dictionary : 0/0, 0/0, 0/0 | imported : n/a
  havoc : 283/1.20M, 0/0 | stability : 100.00%
  trim : 98.56%/602, 0.00%

^C [cpu000: 57%]

+++ Testing aborted by user +++
[+] We're done here. Have a nice day!

st16@st16-Lenovo-V520-15IKL-Desktop:~/Desktop/fuzzgoat$
```

It is recommended to stop the fuzzer after the cycles done are 50:

```
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat

american fuzzy lop 2.52b (fuzzgoat)

process timing | overall results
  run time : 0 days, 6 hrs, 33 min, 35 sec | cycles done : 50
  last new path : 0 days, 0 hrs, 2 min, 59 sec | total paths : 829
  last uniq crash : 0 days, 0 hrs, 54 min, 14 sec | uniq crashes : 29
  last uniq hang : none seen yet | uniq hangs : 0
cycle progress | map coverage
  now processing : 819* (98.79%) | map density : 0.41% / 0.94%
  paths timed out : 0 (0.00%) | count coverage : 5.66 bits/tuple
stage progress | findings in depth
  now trying : bitflip 4/1 | favored paths : 111 (13.39%)
  stage execs : 32.9k/60.0k (54.82%) | new edges on : 169 (20.39%)
  total execs : 66.8M | total crashes : 19.2k (29 unique)
  exec speed : 1373/sec | total tmouts : 119 (12 unique)
fuzzing strategy yields | path geometry
  bit flips : 47/2.23M, 37/2.23M, 3/2.17M | levels : 28
  byte flips : 1/271k, 0/252k, 0/252k | pending : 8
  arithmetics : 71/14.1M, 1/409k, 0/43.1k | pend fav : 0
  known ints : 4/1.62M, 1/7.04M, 0/11.1M | own finds : 828
  dictionary : 0/0, 0/0, 3/1.96M | imported : n/a
  havoc : 649/15.1M, 40/7.94M | stability : 100.00%
  trim : 54.46%/107k, 6.74%

^C [cpu000: 79%]

+++ Testing aborted by user +++
[+] We're done here. Have a nice day!

st16@st16-Lenovo-V520-15IKL-Desktop:~/Desktop/fuzzgoat$
```

Then I navigate to the afl_out directory -> crashes and check its contents:

```
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzg...
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ ls
id:000000,sig:06,src:000000,op:havoc,rep:128
id:000001,sig:06,src:000000,op:havoc,rep:64
id:000002,sig:11,src:000012,op:havoc,rep:64
id:000003,sig:11,src:000030,op:havoc,rep:4
id:000004,sig:06,src:000030,op:havoc,rep:8
id:000005,sig:06,src:000062,op:havoc,rep:64
id:000006,sig:11,src:000073,op:havoc,rep:16
id:000007,sig:06,src:000076,op:havoc,rep:2
id:000008,sig:06,src:000076,op:havoc,rep:4
id:000009,sig:06,src:000159,op:havoc,rep:4
id:000010,sig:11,src:000191,op:havoc,rep:2
id:000011,sig:11,src:000191,op:havoc,rep:2
id:000012,sig:06,src:000192,op:flip1,pos:1
id:000013,sig:06,src:000192,op:havoc,rep:2
id:000014,sig:06,src:000199,op:flip1,pos:0
id:000015,sig:06,src:000234,op:havoc,rep:2
id:000016,sig:11,src:000225,op:havoc,rep:8
id:000017,sig:11,src:000409,op:flip4,pos:3
id:000018,sig:06,src:000409,op:havoc,rep:2
id:000019,sig:06,src:000408,op:havoc,rep:2
id:000020,sig:11,src:000421,op:havoc,rep:2
id:000021,sig:11,src:000421,op:havoc,rep:2
id:000022,sig:11,src:000231,op:havoc,rep:2
id:000023,sig:11,src:000475,op:havoc,rep:2
id:000024,sig:11,src:000318,op:havoc,rep:4
id:000025,sig:06,src:000613,op:havoc,rep:8
id:000026,sig:06,src:000432+000718,op:splice,rep:2
id:000027,sig:11,src:000432+000732,op:splice,rep:2
id:000028,sig:11,src:000433+000689,op:splice,rep:2
README.txt
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$
```

To have a look at these crashes and see what triggered it:

```
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000001\,sig\06\,src\000000\,op\havoc\,rep\64
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000000\,sig\06\,src\000000\,op\havoc\,rep\128
"" st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000002\,sig\11\,src\000012\,op\havoc\,rep\64
"" st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000003\,sig\11\,src\000030\,op\havoc\,rep\4
""
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000004\,sig\06\,src\000030\,op\havoc\,rep\8
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000005\,sig\06\,src\000062\,op\havoc\,rep\64
"" st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000006\,sig\11\,src\000073\,op\havoc\,rep\16
"" st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000007\,sig\06\,src\000076\,op\havoc\,rep\2
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000008\,sig\06\,src\000076\,op\havoc\,rep\4
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000009\,sig\06\,src\000159\,op\havoc\,rep\4
[st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000010\,sig\11\,src\000191\,op\havoc\,rep\2
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000011\,sig\11\,src\000191\,op\havoc\,rep\2
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000012\,sig\06\,src\000192\,op\flip1\,pos\1
[ ]st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000013\,sig\06\,src\000192\,op\havoc\,rep\2
[ ]st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000014\,sig\06\,src\000199\,op\flip1\,pos\0
[ "" ]st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000015\,sig\06\,src\000234\,op\havoc\,rep\2
[ ]
[st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000016\,sig\11\,src\000225\,op\havoc\,rep\8
"" st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000017\,sig\11\,src\000409\,op\flip4\,pos\3
[["\0"]st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000018\,sig\06\,src\000409\,op\havoc\,rep\2
[["["]]st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000019\,sig\06\,src\000408\,op\havoc\,rep\2
[["["]]]st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000020\,sig\11\,src\000421\,op\havoc\,rep\2
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000021\,sig\11\,src\000421\,op\havoc\,rep\2
[["["["["]]]st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$ cat id\000022\,sig\11\,src\000231\,op\havoc\,rep\2
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat/afl_out/crashes$
```

The list of characters are emphasized when I cat these files.

Now, I will run the program with gdb and pass in the crash file and see for more details:

```
st16@st16-Lenovo-V520-15IKL-Desktop: ~/Desktop/fuzzgoat
GNU gdb (Ubuntu 9.2-0ubuntu1~20.04) 9.2
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from fuzzgoat...
(gdb) run afl_out/crashes/id:000001,sig:06,src:000000,op:havoc,rep:64
Starting program: /home/st16/Desktop/fuzzgoat/fuzzgoat afl_out/crashes/id:000001,sig:06,src:000000,op:havoc,rep:64
""
-----
string:
free(): invalid pointer

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
50      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
```

```
string:
free(): invalid pointer

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
50      ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
```

Another crash we can backtrace with bt on gdb:

```
(gdb) run afl_out/crashes/id:000009,sig:06,src:000159,op:havoc,rep:4
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program: /home/st16/Desktop/fuzzgoat/fuzzgoat afl_out/crashes/id:000009,sig:06,src:000159,op:havoc,rep:4
[]
-----
free(): double free detected in tcache 2

Program received signal SIGABRT, Aborted.
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
50  ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
(gdb) bt
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
#1  0x00007ffff7c8e859 in __GI_abort () at abort.c:79
#2  0x00007ffff7cf93ee in __libc_message (action=action@entry=do_abort, fmt=fmt@entry=0x7ffff7e23285 "%s\n")
    at ../sysdeps/posix/libc_fatal.c:155
#3  0x00007ffff7d0147c in malloc_printerr (
    str=str@entry=0x7ffff7e255d0 "free(): double free detected in tcache 2") at malloc.c:5347
#4  0x00007ffff7d030ed in _int_free (av=0x7ffff7e54b80 <main_arena>, p=0x5555555628a0, have_lock=0)
    at malloc.c:4201
#5  0x0000555555557c9a in json_value_free_ex (settings=settings@entry=0x7fffffd7d8, value=0x0) at fuzzgoat.c:311
#6  0x0000555555558c8c in json_value_free_ex (value=<optimized out>, settings=0x7fffffd7d8) at fuzzgoat.c:222
#7  json_parse_ex (settings=settings@entry=0x7fffffd8f0, json=<optimized out>, length=<optimized out>,
    error_buf=error_buf@entry=0x0) at fuzzgoat.c:1065
#8  0x000055555555e295 in json_parse (json=<optimized out>, length=<optimized out>) at fuzzgoat.c:1073
#9  0x00005555555567b in main (argc=<optimized out>, argv=<optimized out>) at main.c:156
(gdb) █
```

```
free(): double free detected in tcache 2
```

```
Program received signal SIGABRT, Aborted.
```

```
__GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
```

```
50  ../sysdeps/unix/sysv/linux/raise.c: No such file or directory.
```

Looking at the backtrace, it looks like a free() function that was called twice on the same pointer, or calling a free on a null pointer.

Looking at the code in fuzzgoat.c, the origin of the problem is traced to here:

```
/* ***** Fuzzgoat Vulnerability ***** */

WARNING: Fuzzgoat Vulnerability

The code below creates and dereferences a NULL pointer if the string
is of length one.

Diff      - Check for one byte string - create and dereference a NULL pointer
Payload    - A JSON string of length one : "A"
Input File - oneByteString
Triggers   - NULL pointer dereference
***** */

    if (value->u.string.length == 1) {
        char *null_pointer = NULL;
        printf ("%d", *null_pointer);
    }

/* ***** END vulnerable code ***** */

    settings->mem_free (value->u.string.ptr, settings->user_data);
    break;

default:
    break;
};
```

- **References:**

1. <https://forums.gentoo.org/viewtopic-t-1098826-start-0.html>
2. <https://stackoverflow.com/questions/29382571/seg-fault-signal-received-sigabort>
3. <https://github.com/fuzzstati0n/fuzzgoat>
4. <https://github.com/google/AFL>
5. <https://medium.com/@ayushpriya10/fuzzing-applications-with-american-fuzzy-lop-afl-54facc65d102>
6. https://www.reddit.com/r/programminghelp/comments/juqrrp/c_free_double_free_detected_in_tcache_2/
7. <https://github.com/fuzzstati0n/fuzzgoat/issues/1>
8. <https://www.delftstack.com/howto/c/c-free-invalid-pointer-error/>
- 9.