Secure and Depdendable Systems
Assignment 2

Drishti Maharjan
Aayush Sharma Acharya

1^{st} March 2020

1 Problem 2.1

To run the code:
open folder stats,
type these commands with an example test case:

```
$ mkdir build
$ cd build
$ cmake ..
$ make
$ printf "99" | ./src/ds min 0
```

2 Problem 2.2

a Install afl-gcc and follow the commands below to instrument the code and run afl-fuzz:

```
$ rmdir -r build
$ mkdir build
$ cd build
$ CC=afl-gcc cmake .. && make
$ cd ..
$ afl-fuzz -i testCases/ -o gen_tests ./b/src/ds
```

In my folder, testCases is the directory with test cases and gen_tests is a folder created to store all files generated by fuzzer

b
- Source code is able to read input from a file, so, a directory 'testCases' is created with 4 test cases with valid input.
- The test files were written with normally what we would give to printf in problem 2.1. For example, test cases with different number of rows and columns were used:
  (find these in ./stats/testCases):
  - 1 2 3\n
  - 71 82 23 3 45 8\n41 24 34 44 5 10\n
  - 4 5 6\n7 8 9\n9 9 9\n
  - 1 4\n

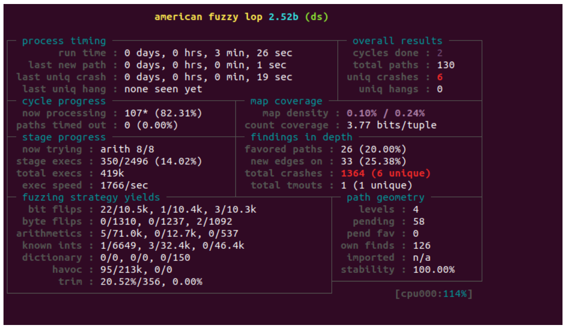
c At initial attempts to run the fuzzer, I noticed program was crashing with some inputs like:

- 1\n
- 1 3a bb \n

- -4 5\n .

So, I realized that my program didn't handle single element cases or invalid input properly. I added more handling and ran the fuzzer again. There were significantly less crashes after I added more error handling part and fixed some bugs. However, there were some crashes shown by fuzzer that I have no clue how to fix.

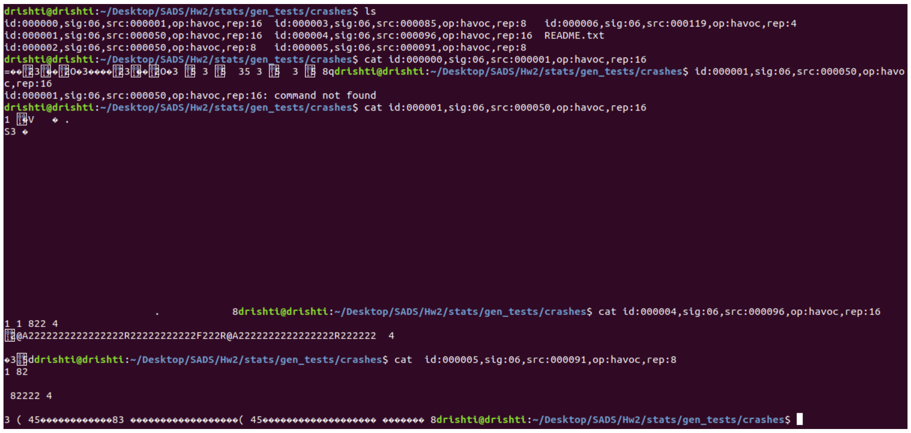
The screenshot below is the stat shown by the fuzzer



```
                     american fuzzy lop 2.52b (ds)

┌─ process timing ─────────────────────────────────────┬─ overall results ─────┐
│        run time : 0 days, 0 hrs, 3 min, 26 sec       │  cycles done : 2      │
│   last new path : 0 days, 0 hrs, 0 min, 1 sec        │  total paths : 130    │
│ last uniq crash : 0 days, 0 hrs, 0 min, 19 sec       │ uniq crashes : 6      │
│  last uniq hang : none seen yet                      │   uniq hangs : 0      │
├─ cycle progress ────────────────────┬─ map coverage ─┴───────────────────────┤
│  now processing : 107* (82.31%)     │    map density : 0.10% / 0.24%         │
│ paths timed out : 0 (0.00%)         │ count coverage : 3.77 bits/tuple       │
├─ stage progress ────────────────────┼─ findings in depth ────────────────────┤
│  now trying : arith 8/8             │ favored paths : 26 (20.00%)            │
│ stage execs : 350/2496 (14.02%)     │  new edges on : 33 (25.38%)            │
│ total execs : 419k                  │ total crashes : 1364 (6 unique)        │
│  exec speed : 1766/sec              │  total tmouts : 1 (1 unique)           │
├─ fuzzing strategy yields ───────────┴───────────────┬─ path geometry ────────┤
│   bit flips : 22/10.5k, 1/10.4k, 3/10.3k            │    levels : 4          │
│  byte flips : 0/1310, 0/1237, 2/1092                │   pending : 58         │
│ arithmetics : 5/71.0k, 0/12.7k, 0/537               │  pend fav : 0          │
│  known ints : 1/6649, 3/32.4k, 0/46.4k              │ own finds : 126        │
│  dictionary : 0/0, 0/0, 0/150                       │  imported : n/a        │
│       havoc : 95/213k, 0/0                          │ stability : 100.00%    │
│        trim : 20.52%/356, 0.00%                     ├────────────────────────┘
└─────────────────────────────────────────────────────┘          [cpu000:114%]
```

To look into the inputs that were crashing the program, most of the inputs had an unsupported/binary type input. Some examples are shown in the screenshot (shown upon command cat):



```
drishti@drishti:~/Desktop/SADS/Hw2/stats/gen_tests/crashes$ ls
id:000000,sig:06,src:000001,op:havoc,rep:16  id:000003,sig:06,src:000085,op:havoc,rep:8   id:000006,sig:06,src:000119,op:havoc,rep:4
id:000001,sig:06,src:000050,op:havoc,rep:16  id:000004,sig:06,src:000096,op:havoc,rep:16  README.txt
id:000002,sig:06,src:000050,op:havoc,rep:8   id:000005,sig:06,src:000091,op:havoc,rep:8
drishti@drishti:~/Desktop/SADS/Hw2/stats/gen_tests/crashes$ cat id:000000,sig:06,src:000001,op:havoc,rep:16
=��□3□�□O�3����□3□�□O�3 □ 3 □  35 3 □  3 □ 8qdrishti@drishti:~/Desktop/SADS/Hw2/stats/gen_tests/crashes$ id:000001,sig:06,src:000050,op:havo
c,rep:16
id:000001,sig:06,src:000050,op:havoc,rep:16: command not found
drishti@drishti:~/Desktop/SADS/Hw2/stats/gen_tests/crashes$ cat id:000001,sig:06,src:000050,op:havoc,rep:16
1 □V   � .
S3 �









                        .           8drishti@drishti:~/Desktop/SADS/Hw2/stats/gen_tests/crashes$ cat id:000004,sig:06,src:000096,op:havoc,rep:16
1 1 822 4
□@A2222222222222222R22222222222F222R@A2222222222222222R222222  4

�3□ddrishti@drishti:~/Desktop/SADS/Hw2/stats/gen_tests/crashes$ cat  id:000005,sig:06,src:000091,op:havoc,rep:8
1 82

 82222 4

3 ( 45������������83 �����������������( 45�������������������� ������� 8drishti@drishti:~/Desktop/SADS/Hw2/stats/gen_tests/crashes$ █
```