

FUZZ THEM ALL PROJECT

Submitted by: Vaishnavi Vemuri

ASU ID: 1226770885

For this project, I have created a mutative fuzzer using python according to the given requirements. This fuzzer program will take an initial seed and two other arguments ("prng_seed" and "num_of_iterations") as input.

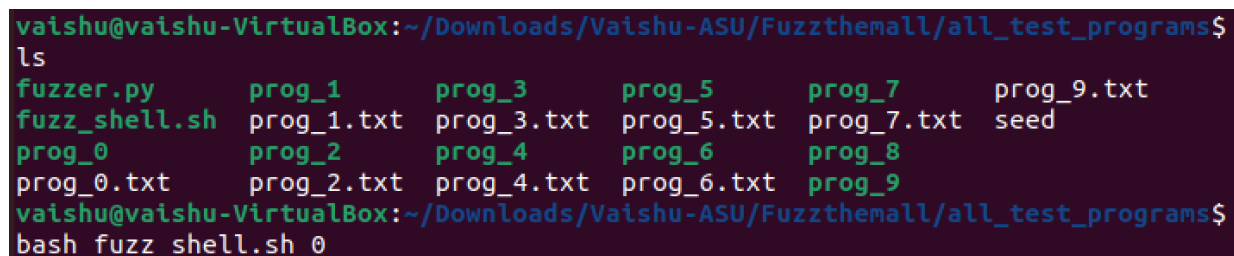
So, firstly, we read the initial seed file which was given under test_programs folder. After reading the seed file, we will add 10 random characters for every 500 iterations and for each iteration, each byte of the input is mutated to a random byte by 13% probability. For every iteration, the program seed is incremented by 1.

I initially tried running the fuzzer by passing random program seed and number of iterations and tried this until I crashed the programs with the segmentation fault. But this approach seemed to be tedious and time taking. Hence, thought of automating this process by creating a shell script program.

I have created a shell script program which generates a random program seed and calls the fuzzer program during each iteration for a maximum of 20,000 iterations. For each iteration, whenever the code breaks, we investigate the stderr and if the error code is 139 i.e., segmentation fault, we then break the loop, and the program stops. Then we note down the program seed and the iteration number where the program crashes. Following is the snippet of the shell program:

```
-----
prng_seed=$RANDOM
echo "Using $prng_seed as PRNG seed"

for i in {1..20000}; do
    echo "i=$i"
    echo "prng_seed=$prng_seed, iter=$i\r"
    python3 fuzzer.py "$prng_seed" "$i" -0 | ./prog_$1 2>/dev/null || {
        status=$?
        if [ "$status" -eq 139 ]; then
            echo "status=$status"
            break
        fi
    }
}
Done
```



```
vaishu@vaishu-VirtualBox: ~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
ls
fuzzer.py      prog_1      prog_3      prog_5      prog_7      prog_9.txt
fuzz_shell.sh  prog_1.txt  prog_3.txt  prog_5.txt  prog_7.txt  seed
prog_0        prog_2      prog_4      prog_6      prog_8
prog_0.txt     prog_2.txt  prog_4.txt  prog_6.txt  prog_9
vaishu@vaishu-VirtualBox: ~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
bash fuzz_shell.sh 0
```

To run the bash shell script program, you must run the above command and give the program number at the end like shown above in the screenshot.

Below are the program seeds and no of iterations for which each of the programs under test_programs folder crashed after running shell script program.

Prog0:
prng_seed = 26275
num_of_iterations = 1619

Prog1:
prng_seed = 19055
num_of_iterations = 1674

Prog2:
prng_seed = 1352
num_of_iterations = 2063

For the other programs under all_test_programs folder, I have created an initial seed myself using some random characters and crashed the programs with the below numbers. I was able to crash all the programs except prog8 with the help of shell scripting program.

Prog0:
prng_seed = 39019
num_of_iterations = 2527

Prog1:
prng_seed = 13862
num_of_iterations = 2107

Prog2:
prng_seed = 3817
num_of_iterations = 2516

Prog3:
prng_seed = 2672
num_of_iterations = 8000

Prog4:
prng_seed = 153
num_of_iterations = 8500

Prog5:
prng_seed = 15091
num_of_iterations = 8029

Prog6:
prng_seed = 28334
num_of_iterations = 3880

Prog7:
prng_seed = 3702
num_of_iterations = 8100

Prog9:
prng_seed = 3761
num_of_iterations = 18000

Commands to run this program in the ubuntu terminal:

Go into test_programs folder and then run the below commands

1. cd test_programs
cd prog0
python3 ./fuzzer.py 26275 1619 | ./prog_0
2. cd test_programs
cd prog1
python3 ./fuzzer.py 19055 1674 | ./prog_1
3. cd test_programs
cd prog2
python3 ./fuzzer.py 1352 2063 | ./prog_2

```
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/test_programs/prog0
$ python3 ./fuzzer.py 26275 1619 | ./prog_0
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/test_programs/prog0
$ cd ..
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/test_programs$ cd prog1
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/test_programs/prog1
$ python3 ./fuzzer.py 19055 1674 | ./prog_1
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/test_programs/prog1
$ cd ..
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/test_programs$ cd prog2
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/test_programs/prog2
$ python3 ./fuzzer.py 1352 2063 | ./prog_2
Segmentation fault (core dumped)
```

Go into all_test_programs folder and then run the below commands

- cd all_test_programs
- python3 ./fuzzer.py 39019 2527 | ./prog_0
 - python3 ./fuzzer.py 13862 2107 | ./prog_1
 - python3 ./fuzzer.py 3817 2516 | ./prog_2
 - python3 ./fuzzer.py 2672 8000 | ./prog_3
 - python3 ./fuzzer.py 153 8500 | ./prog_4
 - python3 ./fuzzer.py 15091 8029 | ./prog_5
 - python3 ./fuzzer.py 28334 3880 | ./prog_6

- python3 ./fuzzer.py 3702 8100 | ./prog_7
- python3 ./fuzzer.py 3761 18000 | ./prog_9

```
vaishu@vaishu-VirtualBox:~$ cd Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs/
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 39019 2527 | ./prog_0
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 13862 2107 | ./prog_1
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 3817 2516 | ./prog_2
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 2672 8000 | ./prog_3
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 153 8500 | ./prog_4
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 15091 8029 | ./prog_5
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 28334 3880 | ./prog_6
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 3702 8100 | ./prog_7
Segmentation fault (core dumped)
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 3761 18000 | ./prog_9
Segmentation fault (core dumped)
```

Fuzzer testing

I have tested the fuzzer with same pair of program seed and iterations and it generated the same mutated output everytime as expected.

```
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 39019 2527
result 4YqI^&A;é±ðPÜ7.çÒ æOPÁø^ÜFAáÜ|*§
ùsJ|ðð2Ú-Á¹0JgÔ]gt
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 39019 2527
result 4YqI^&A;é±ðPÜ7.çÒ æOPÁø^ÜFAáÜ|*§
ùsJ|ðð2Ú-Á¹0JgÔ]gt
```

When I change either the iteration number or the program seed, the mutated result changed as shown in the below results

```
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 39019 2520
result ²)§\^ñ÷&¿ó±ðáPÜ7.2ð8ýðÁø^ÜF&Ãá ùÉë
ùsHÝôçð%t0²¹v>H?%ôdü
vaishu@vaishu-VirtualBox:~/Downloads/Vaishu-ASU/Fuzzthemall/all_test_programs$
python3 ./fuzzer.py 3019 2520
result ôX0Ë-Kî"²µÃßp;A±ý_UE/ã
²
```

Dependencies

This program has been compiled on ubuntu-22.10-desktop-amd64. The fuzzmodified.py is a python program which needs python3 to be installed. Apart from this, there are no other external dependencies required.

The python version to be used is - Python 3.10.7.