Ira A. Fulton Schools of Engineering
Arizona State University

Engineering | School of Computing, Informatics, and Decision Systems Engineering

CSE 543: Information Assurance and Security

Name: Mohammed Ahmed Ragab
university ID: 122******
university: Arizona state university (ASU)
project name: Fuzz them all
course: CSE 543 Information Assurance and Security

Description:

I developed a fuzzer software that generates random string with different length based on two inputs provided in the command line argument, which are seed value and number of iteration

how does my fuzzer program works ?

My fuzzer program takes two inputs from the command line , the first one is a seed value which is used to be given to any random value generator so that each time the random value generator generates the same output, the second input is the number of iterations which represents the length of the generates random string.

in python programming language, if you set a seed value in the "random" module(by calling *random.seed(seed_value)*) before calling any random function in "random" module such as " *random.choice(letters)",* the random function will generate the same value each time you run the python script, this is called "deterministic behavior", I tested this by myself and commented the test code in my python fuzzer source code so that anyone can test it.

How is the random string generated?

in python , there is “string” module which contains a constant named “*printable*”, you can use it by typing “*string.printable*” which contains all printable ASCII characters including upper and lower English letters, digits(0 - 9), and special characters($#@..etc) and space characters.

In addition, there is a random function” *random.choice(letters)”* which chooses a random character from a string(i.e “*string.printable*” constant) , this function is called in number of iterations(giving in the command line argument) so that a random string is built from adding joining(adding) characters to an empty string.

Finally, the string is printed to the standard output (i.e the terminal). In Linux you can pipeline the output of the fuzzer to one of the prog_x where x is the program number you want to crash.

What is the command did I use for crashing the programs?

```
python ./fuzzer.py [seed value] [num of iterations] | ./all_test_programs/prog_x
```

where x is the program number you want to crash

for example:

```
python ./fuzzer.py 2 100 | ./all_test_programs/prog_0

python ./fuzzer.py 2 100 | ./all_test_programs/prog_1

python ./fuzzer.py 2 300 | ./all_test_programs/prog_2

python ./fuzzer.py 2 300 | ./all_test_programs/prog_3

python ./fuzzer.py 2 300 | ./all_test_programs/prog_4

python ./fuzzer.py 2 300 | ./all_test_programs/prog_5

python ./fuzzer.py 2 300 | ./all_test_programs/prog_6

python ./fuzzer.py 2 300 | ./all_test_programs/prog_7

python ./fuzzer.py 3 300 | ./all_test_programs/prog_9
```

how do I know a program is crashed ?

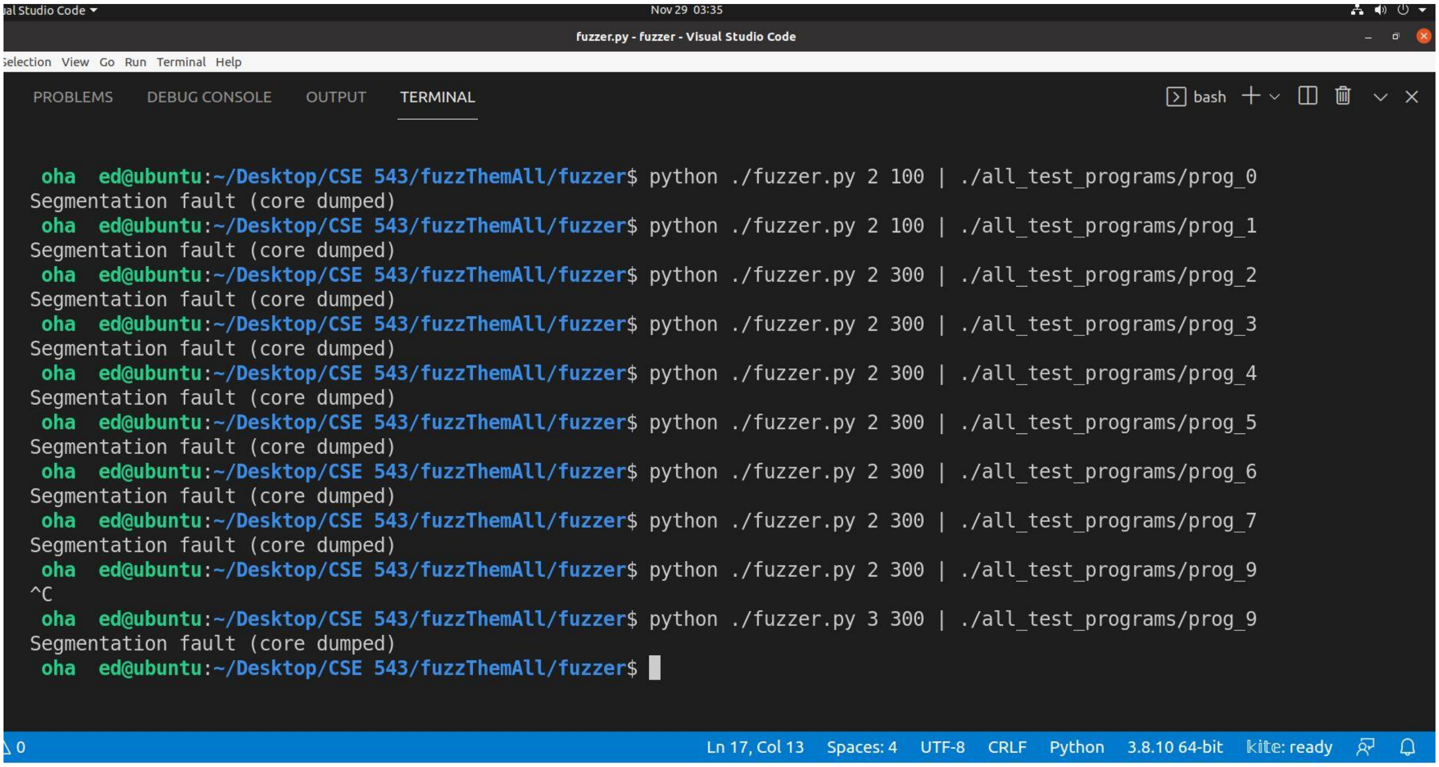
if “Segmentation fault (core dumped)” is printed on the terminal, then the program has been crashed by the fuzzer.

Note: I could not be able to crash prog_8, I always get "Reading too much!" output.

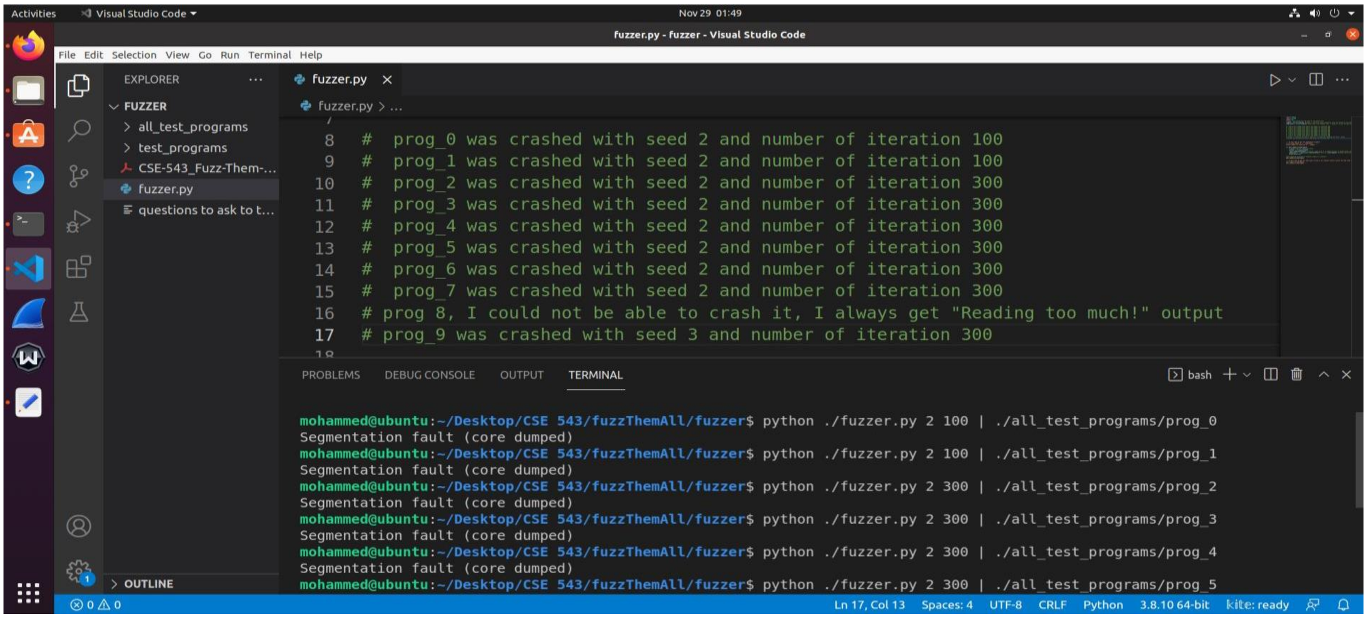
Environment:

- operating system : Linux Ubuntu 20.04 LTS run on virtual machine using VMware workstation 16 player on windows 10
- Python 3.8.10
- text editor: VS code

Screenshots:

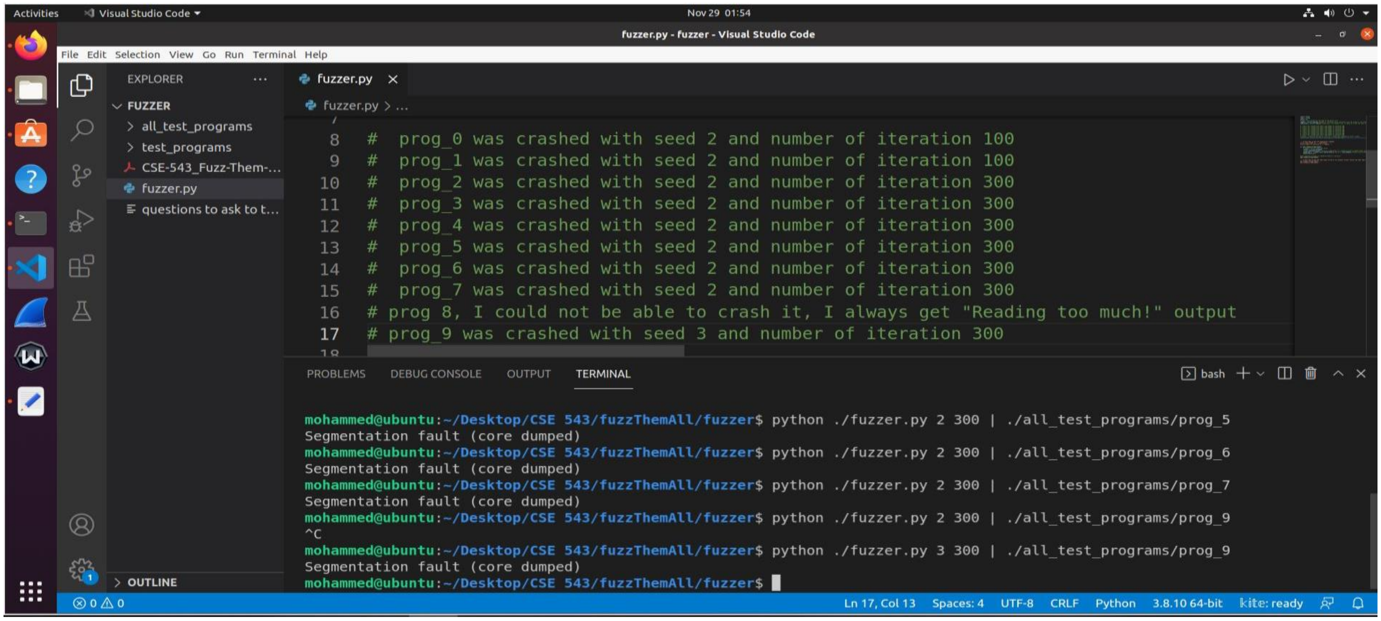


```
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 100 | ./all_test_programs/prog_0
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 100 | ./all_test_programs/prog_1
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_2
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_3
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_4
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_5
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_6
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_7
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_9
^C
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 3 300 | ./all_test_programs/prog_9
Segmentation fault (core dumped)
 oha  ed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ 
```



```
#  prog_0 was crashed with seed 2 and number of iteration 100
#  prog_1 was crashed with seed 2 and number of iteration 100
#  prog_2 was crashed with seed 2 and number of iteration 300
#  prog_3 was crashed with seed 2 and number of iteration 300
#  prog_4 was crashed with seed 2 and number of iteration 300
#  prog_5 was crashed with seed 2 and number of iteration 300
#  prog_6 was crashed with seed 2 and number of iteration 300
#  prog_7 was crashed with seed 2 and number of iteration 300
# prog 8, I could not be able to crash it, I always get "Reading too much!" output
# prog_9 was crashed with seed 3 and number of iteration 300
```

```
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 100 | ./all_test_programs/prog_0
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 100 | ./all_test_programs/prog_1
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_2
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_3
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_4
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_5
```



```
#  prog_0 was crashed with seed 2 and number of iteration 100
#  prog_1 was crashed with seed 2 and number of iteration 100
#  prog_2 was crashed with seed 2 and number of iteration 300
#  prog_3 was crashed with seed 2 and number of iteration 300
#  prog_4 was crashed with seed 2 and number of iteration 300
#  prog_5 was crashed with seed 2 and number of iteration 300
#  prog_6 was crashed with seed 2 and number of iteration 300
#  prog_7 was crashed with seed 2 and number of iteration 300
# prog 8, I could not be able to crash it, I always get "Reading too much!" output
# prog_9 was crashed with seed 3 and number of iteration 300
```

```
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_5
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_6
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_7
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 2 300 | ./all_test_programs/prog_9
^C
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ python ./fuzzer.py 3 300 | ./all_test_programs/prog_9
Segmentation fault (core dumped)
mohammed@ubuntu:~/Desktop/CSE 543/fuzzThemAll/fuzzer$ 
```