
README

Instructions for use of this program are as follows:

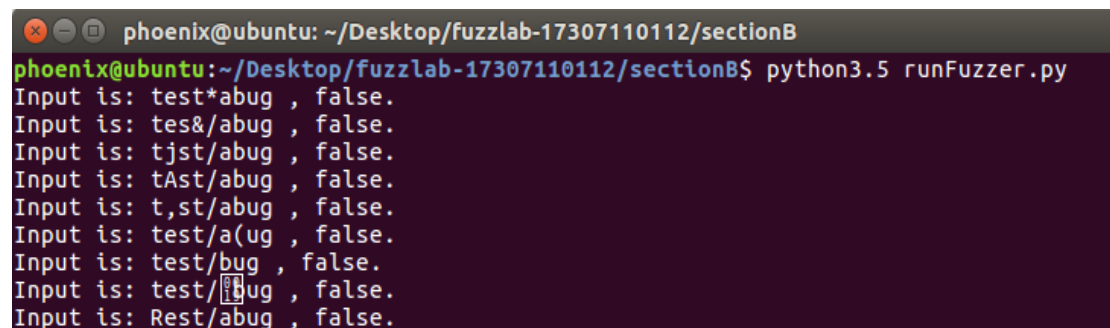
1. Dependences:

Python 3.5 is preferred, and generally 3.6 or above versions can run the program successfully.

Please keep file "runFuzzer.py", file "runFuzzer" and file "ls" in the same directory at all times.

2. Run the source code in the terminal:

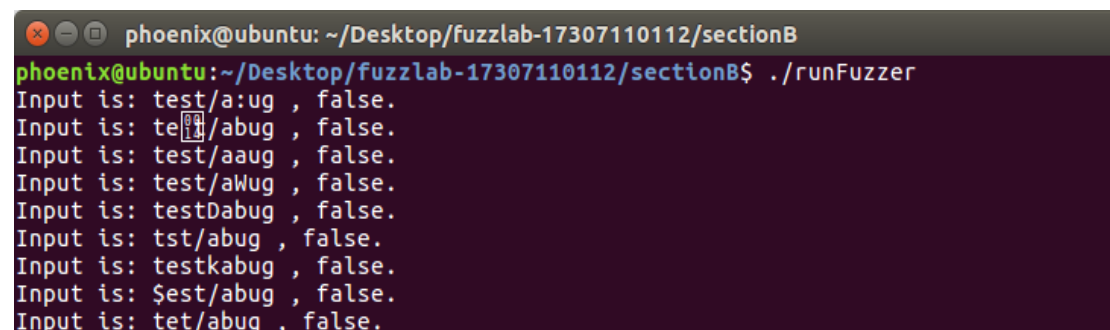
Open the terminal program, type in the command "**python3.5 runFuzzer.py**", and press enter to start the program. The "python3.5" here should be replaced with the version of Python you have installed. If you want to exit the program, close the terminal window.

A terminal window with a dark background and light text. The title bar shows 'phoenix@ubuntu: ~/Desktop/fuzzlab-17307110112/sectionB'. The prompt is 'phoenix@ubuntu:~/Desktop/fuzzlab-17307110112/sectionB\$'. The command 'python3.5 runFuzzer.py' has been entered. The output shows ten lines of 'Input is: [string], false.' where the strings are variations of 'test' and 'abug' separated by various characters like asterisk, ampersand, slash, space, and parentheses.

```
phoenix@ubuntu: ~/Desktop/fuzzlab-17307110112/sectionB
phoenix@ubuntu:~/Desktop/fuzzlab-17307110112/sectionB$ python3.5 runFuzzer.py
Input is: test*abug , false.
Input is: tes&/abug , false.
Input is: tjst/abug , false.
Input is: tAst/abug , false.
Input is: t,st/abug , false.
Input is: test/a(ug , false.
Input is: test/bug , false.
Input is: test/ug , false.
Input is: Rest/abug , false.
```

3. Run the executable file in the terminal:

Open the terminal program, type in the command "**./runFuzzer**", and press enter to start the program. If you want to exit the program, close the terminal window.

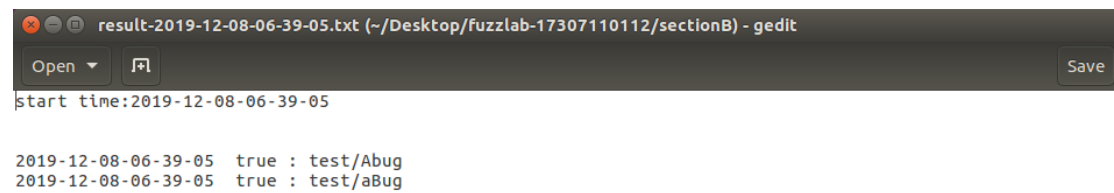
A terminal window with a dark background and light text. The title bar shows 'phoenix@ubuntu: ~/Desktop/fuzzlab-17307110112/sectionB'. The prompt is 'phoenix@ubuntu:~/Desktop/fuzzlab-17307110112/sectionB\$'. The command './runFuzzer' has been entered. The output shows ten lines of 'Input is: [string], false.' where the strings are variations of 'test', 'tst', and 'tet' followed by different combinations of 'a', 'u', and 'g' and 'abug'.

```
phoenix@ubuntu: ~/Desktop/fuzzlab-17307110112/sectionB
phoenix@ubuntu:~/Desktop/fuzzlab-17307110112/sectionB$ ./runFuzzer
Input is: test/a:ug , false.
Input is: te/abug , false.
Input is: test/aaug , false.
Input is: test/aWug , false.
Input is: testDabug , false.
Input is: tst/abug , false.
Input is: testkabug , false.
Input is: $est/abug , false.
Input is: tet/abug , false.
```

4. Result of the program:

You can find the result of program execution in the current directory. Its name is usually

similar to "result-2019-12-08-06-39-05.txt". The first line of the file records when the program started running. In each row after this, the first column records the time of finding the input that can cause crash, the second column records whether it can cause crash, and the third column records the content of the string that can cause crash.



```
result-2019-12-08-06-39-05.txt (~/.Desktop/fuzzlab-17307110112/sectionB) - gedit
start time:2019-12-08-06-39-05

2019-12-08-06-39-05 true : test/Abug
2019-12-08-06-39-05 true : test/aBug
```

5. Performance:

Usually, the first input that causes crash can be found in the first 1000 cycles. The second can also be found within ten seconds of the program's execution.