Fuzzer

https://youtube.com/playlist?list=PLAwxTw4SYaPkWVHeC_8aSIbSxE_NXI76g&si=lhs0mKJKm5pW3D1R

1. Fuzzer

```
#!/usr/bin/python

# 5-line fuzzer below is from Charlie Miller's
# "Babysitting an Army of Monkeys":
# Part 1 - http://www.youtube.com/watch?v=Xnwodi2CBws
# Part 2 - http://www.youtube.com/watch?v=lK5fgCvS2N4

# List of files to use as initial seed
file_list = [
    "blackbox_testing.pdf",
    "code_coverage.pdf",
    "pluginuri_utile_java.pdf",
    "examen.pdf"
]

# List of applications to test
apps = [
    "/Applications/Adobe Acrobat Reader.app/Contents/MacOS/AdobeReader",
    "/Applications/Microsoft Word.app/Contents/MacOS/Microsoft Word"
]

fuzz_output = "fuzz.pdf"

FuzzFactor = 250
num_tests = 10000

############ end configuration ############
```

```
import math
import random
import string
import subprocess
import time

for i in range(num_tests):
    file_choice = random.choice(file_list)
    app = random.choice(apps)

    buf = bytearray(open(file_choice, 'rb').read())

    # start Charlie Miller code
    numwrites = random.randrange(math.ceil((float(len(buf)) / FuzzFactor))) +
1

    for j in range(numwrites):
        rbyte = random.randrange(256)
        rn = random.randrange(len(buf))
        buf[rn] = "%c" % rbyte
    # end Charlie Miller code

    open(fuzz_output, 'wb').write(buf)

    process = subprocess.Popen([app, fuzz_output])

    time.sleep(1)
    crashed = process.poll()
    if not crashed:
        process.terminate()
```

- **Homework**: Write a fuzzer based on the one we give you for real world applications (ex. PDF's)
- Link to your fuzzer
- Show what you fuzzed
- Describe any bugs you found
- How would you improve?

Notă[1]

[1]