when_did_you_born 攻防世界

v4溢出，覆盖v5，进而改变程序执行流程。

```
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 == 0x786 )
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;
37   }
38   return result;
39 }
```