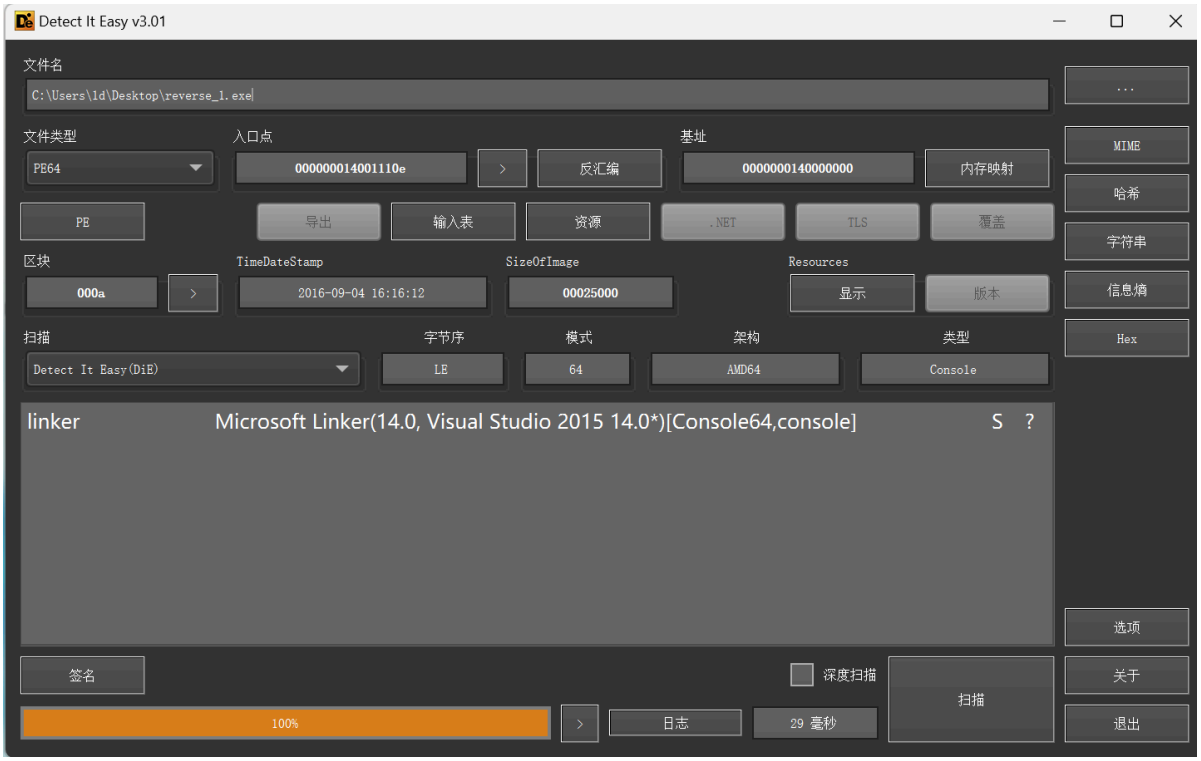
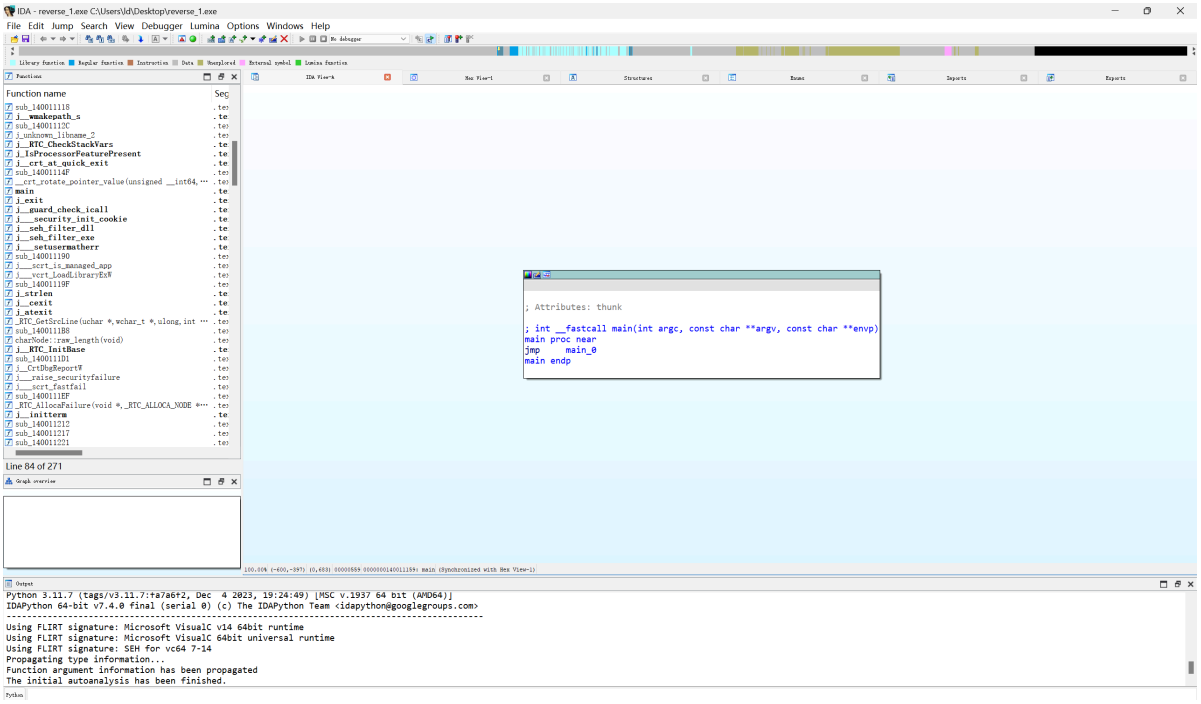
BUUCTF reverse1 1

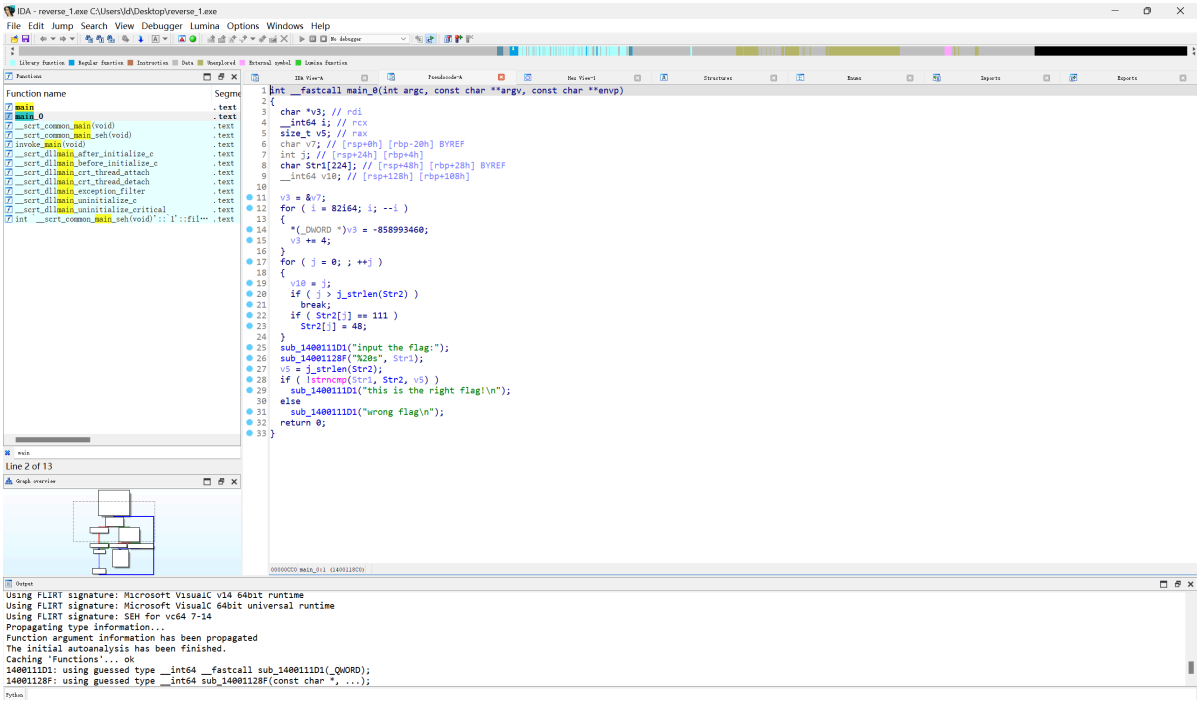
先用die查一下壳，发现无壳且是64位



拖进IDA进行反汇编，界面如下



按照经典套路先找main函数，按下tab键将汇编代码变为伪c代码（对于我这种新手来说看汇编语言还是太难了）



第一步，定位

一是定位加密后的flag字符串，而是准确定位加密的函数（如何加密的flag）

一般来说，是先去找引用"flag"的代码段，然后一步步定位到关键部分，找到真正把flag加密的函数，然后手工逆向或者写解密脚本得到真正的flag

第二步，手搓或者写脚本逆向（有些简单的加密方式可以直接手算，节省时间）

大部分题目逆向脚本建议用python写，语法比较简单，写起来比较快

先定位到flag字段

```
        Str2[j] = 48;
    }
    sub_1400111D1("input the flag:");
    sub_14001128F("%20s", Str1);
    v5 = j_strlen(Str2);
    if ( !strncmp(Str1, Str2, v5) )
      sub_1400111D1("this is the right flag!\n");
    else
      sub_1400111D1("wrong flag\n");
    return 0;
}
```

根据括号内的语句再结合c语言中的输入输出语法合理猜测sub_1400111D1是输出， sub_14001128F是输入

strcnmp函数介绍

```
函数原型：int strncmp(const char* str1, const char* str2, size_t num)
头　文　件：#include <string.h>
返　回　值：（与strcmp相同）str1 = str2　则返回0，
                    str1 > str2　则返回大于0的值，
```

```
str1 < str2   则返回小于0的值
```

即strncmp(str1,str2,v5)是把str1与str2两字符串的前v5位数

做一个比较，若str1=str2，返回0；大于返回正数，小于返回负数，合理猜测v5既是Str2的长度。

if（！strncmp（str1，str2，v5））是一个判断语句，if（）括号里面的内容如果为真，则输出

"this is the right flag"，这时我们只需要知道什么情况为真。

然后看括号里面的内容 !(strncmp(str1,str2,v5))为真的情况

！为非，所以只要(strncmp(str1,str2,v5))为0， !(strncmp(str1,str2,v5))即为真；为0的情况已经在上面对strncmp函数的讲解说过了，**str1，str2两个字符串相等返回值即为0。**

<u>所以此时str2函数就是突破口，双击str2查看</u>

```
.data:000000014001C000 ; Segment permissions: Read/Write
.data:000000014001C000 _data           segment para public 'DATA' use64
.data:000000014001C000                 assume cs:_data
.data:000000014001C000                 ;org 14001C000h
.data:000000014001C000 ; char Str2[]
.data:000000014001C000 Str2            db '{hello_world}',0    ; DATA XREF: main_0+4B↑o
```

可以看到Str2就是{hello_world}

但是将flag{hello_world}提交了以后说flag错误，则此时还需要继续进行分析

```
for ( j = 0; ; ++j )
{
  v10 = j;
  if ( j > j_strlen(Str2) )
    break;
  if ( Str2[j] == 111 )
    Str2[j] = 48;
}
```

猜测是这个for循环改变了Str2的值，按下快捷键'R'，将asii码111和48转变为字符

```
17  for ( j = 0; ; ++j )
18  {
19    v10 = j;
20    if ( j > j_strlen(Str2) )
21      break;
22    if ( Str2[j] == 'o' )
23      Str2[j] = '0';
24  }
```

发现o变成0了，将{hello_world}换成{hell0_w0rld}提交成功。