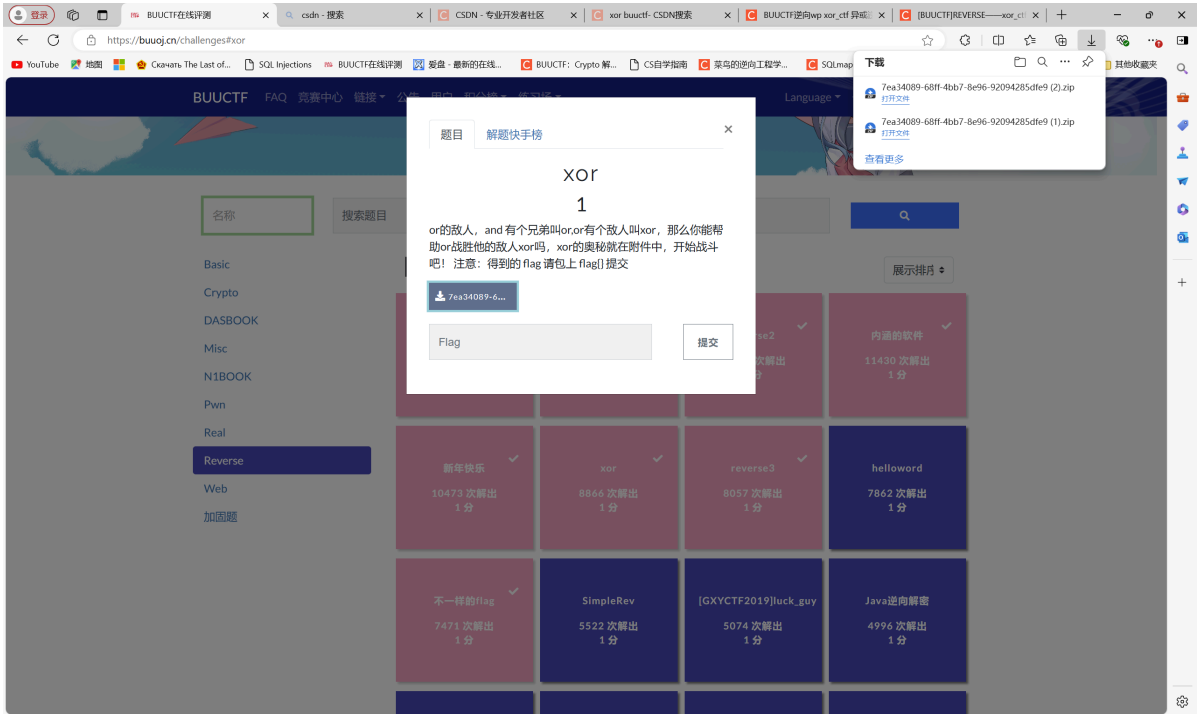
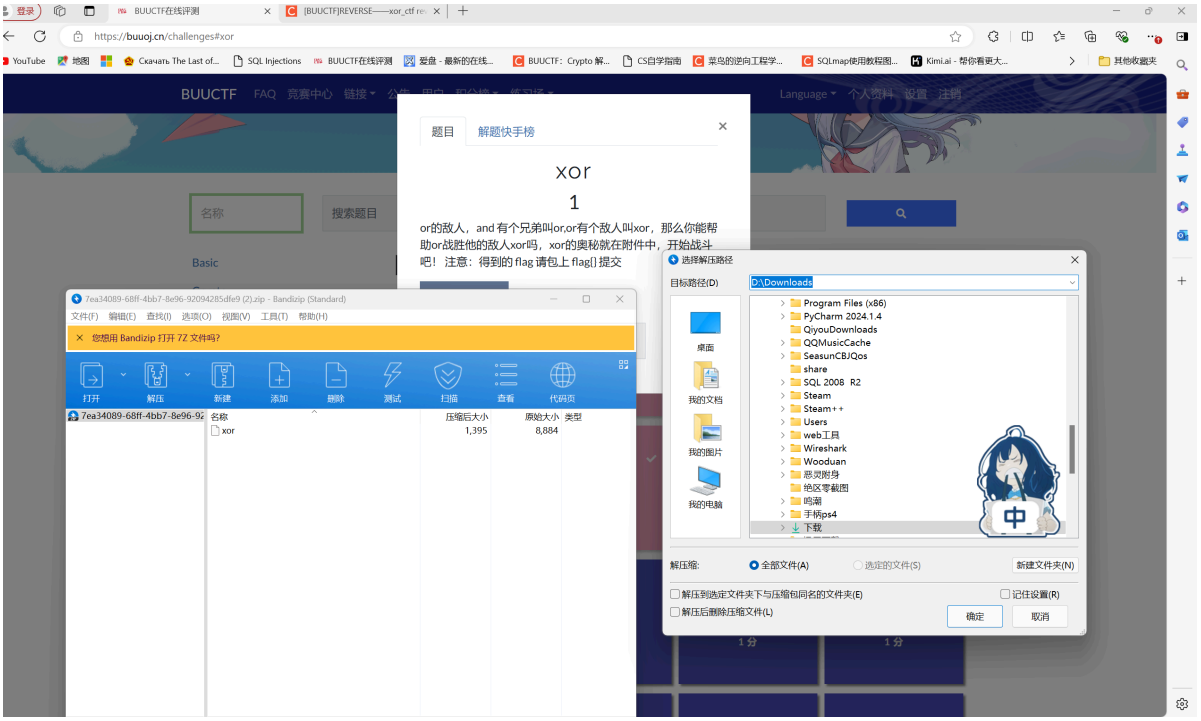
buuctf xor

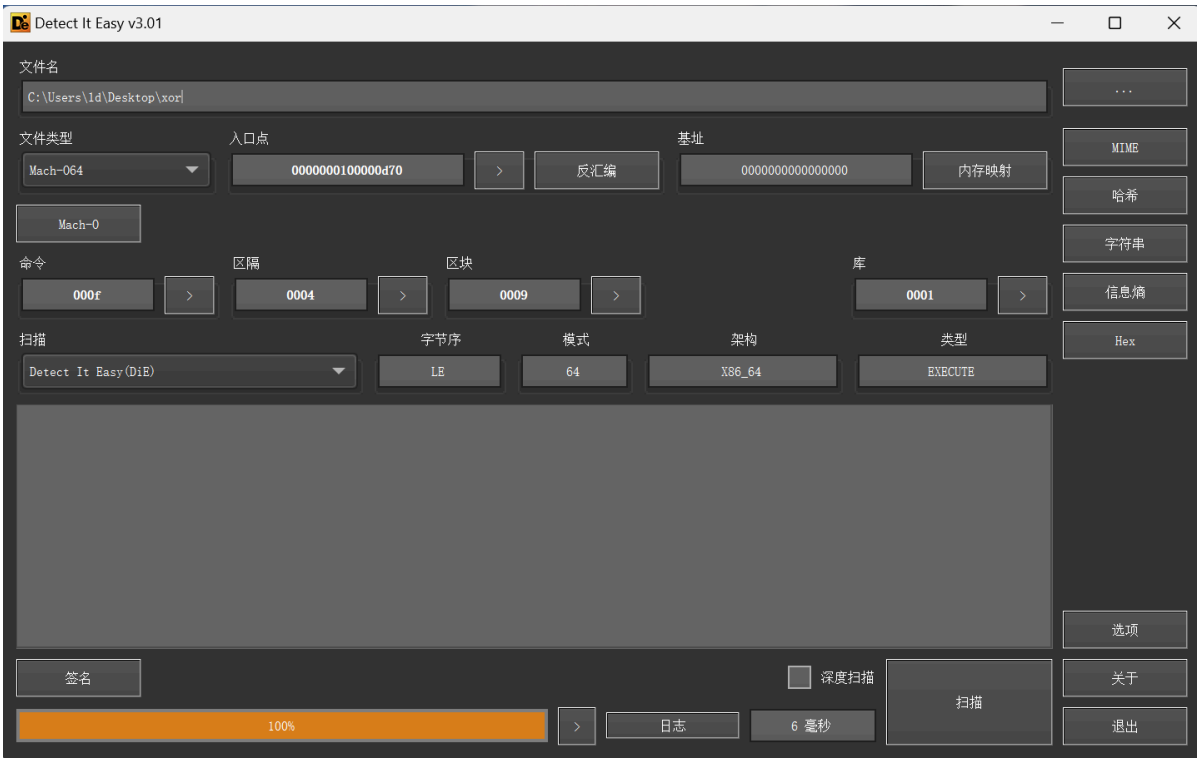
先在刷题网站下载题目源文件



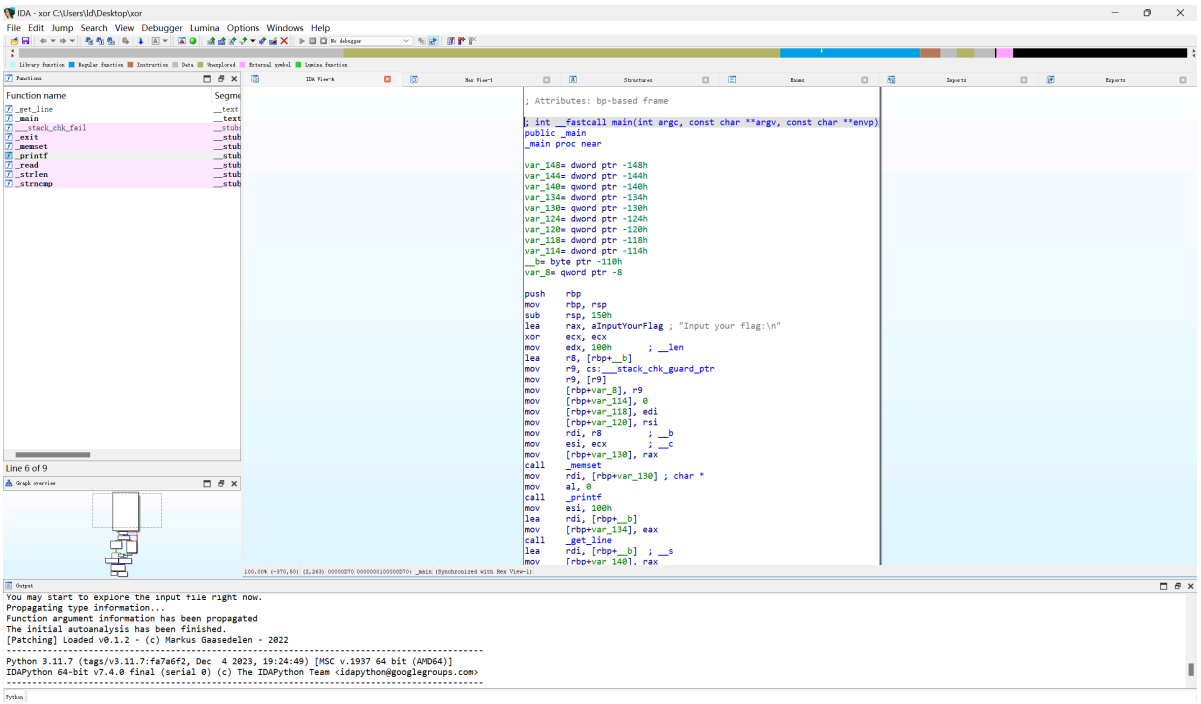
在右上角点击“打开文件”，进行解压(随便解压到一个可以找得到的地方即可)



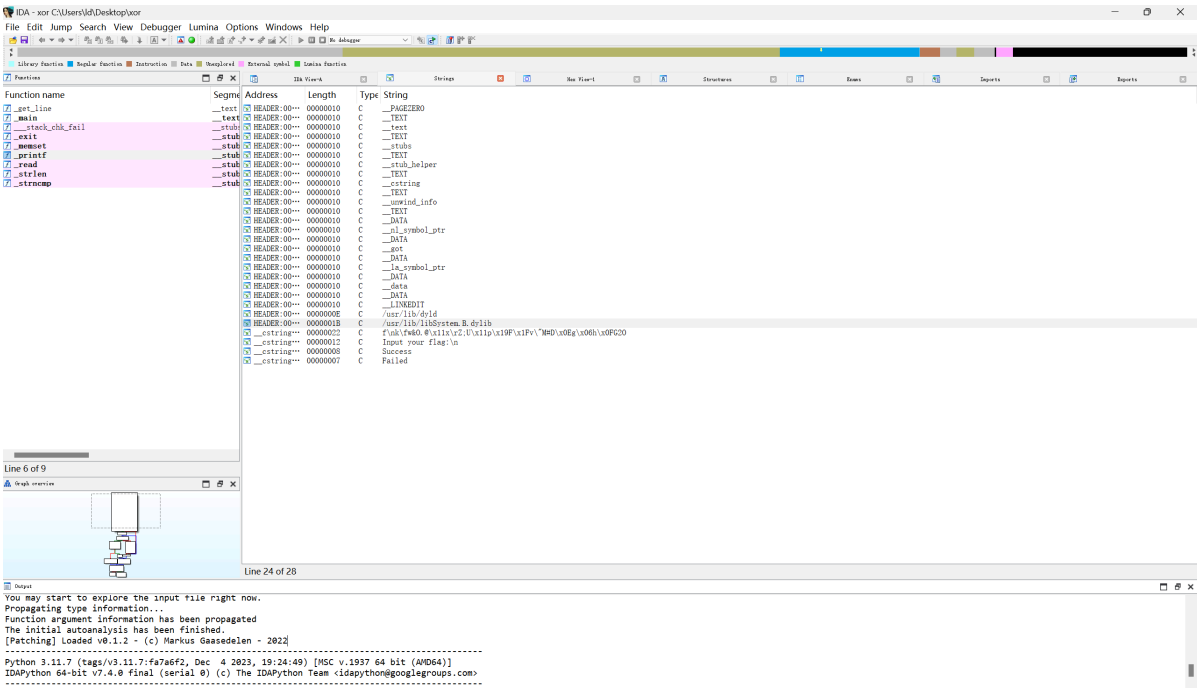
先把xor文件丢die看看有没有壳，可以看出来无壳并且是64位



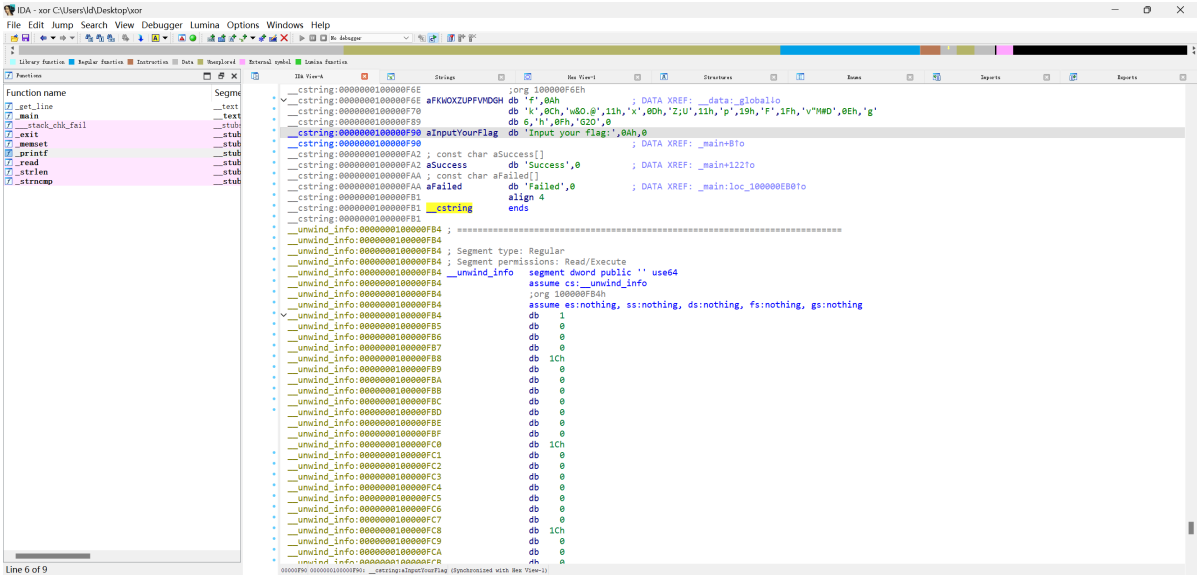
再将xor文件拖进ida里面，打开就是这样



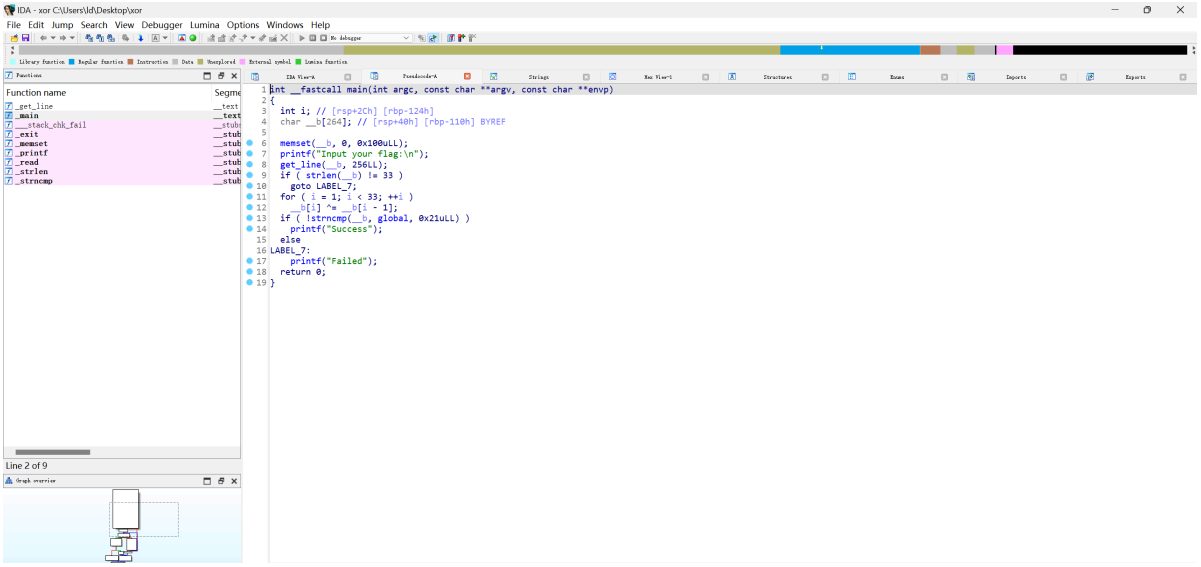
同时按下 `shift+F12` 查找字符串，敏锐的发现有Flag。



双击进入它所在的函数看看



汇编语言还没学看不懂，按下F5反汇编转为伪c代码



仔细阅读这个关键函数（实际上就是_main函数，根据习惯思路使用`ctrl+f`找main函数可能更快找到这里）。

这个函数先是要我们输入一个flag（`get_line`函数推测是输入函数），if语句就是判断你输入flag的长度，如果长度等于33就进行接下来的操作，不等于33就直接跳到输出"Failed"

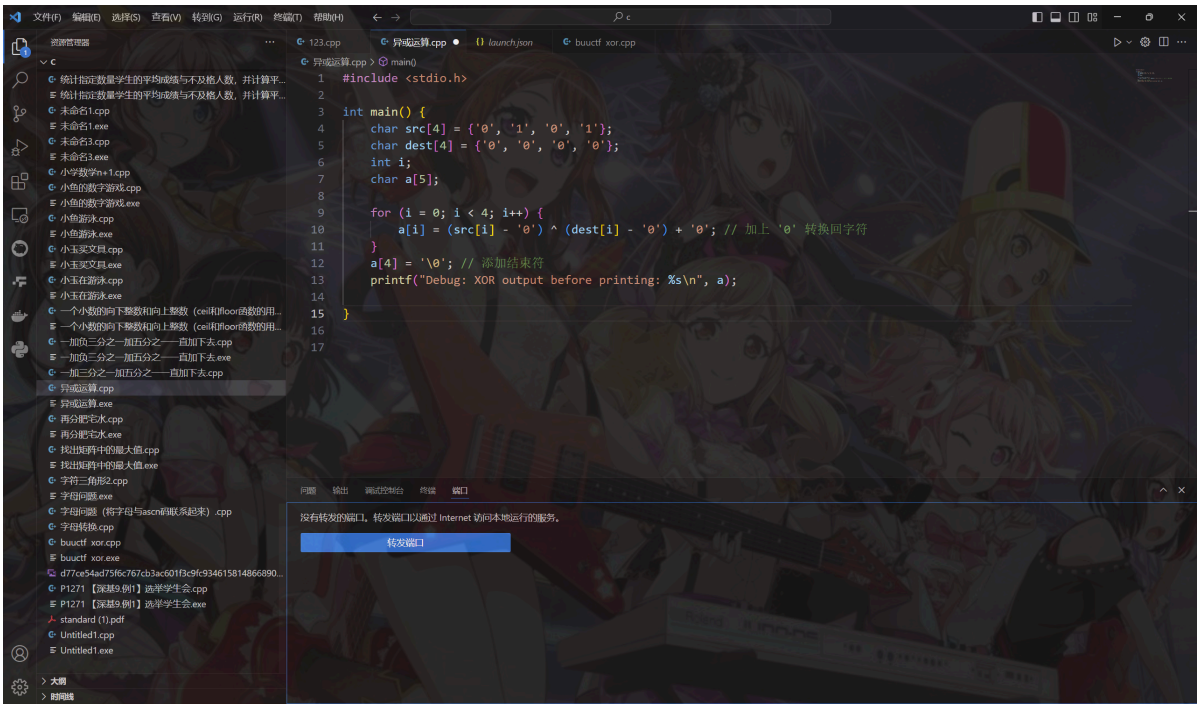
当我们输入的flag长度为33时，就会进入for循环，看到^就猜到应该是进行异或运算，这里是将我们输入的字符数组中每一位数据与前一位数据进行异或运算

异或运算

异或运算的概念

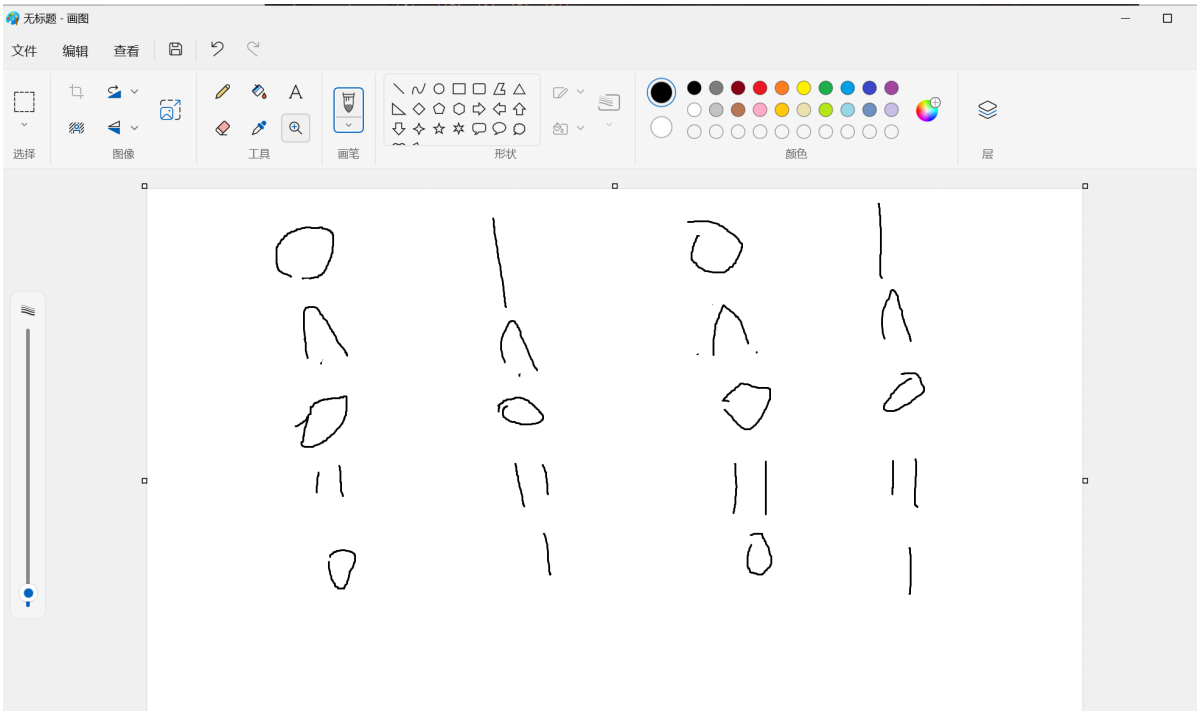
- 对应二进制位进行异或运算
- 对应二进制位上，相同结果为0，不同结果为1

异或运算的例子



这里我们设src为'0101',dest为'0000',我们看看结果会是多少

得到结果是0101，满足异或运算的两者相同结果为零，不同为1

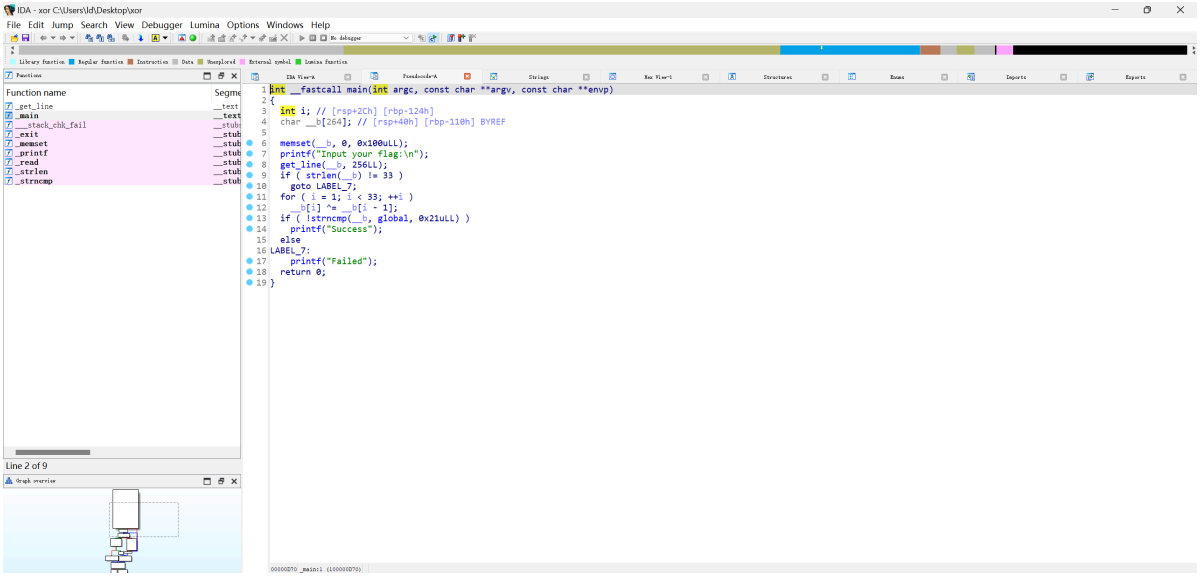


此时就是解题关键，根据一个数进行两次异或运算还是得到自己的定理，我们只要知道异或一次后的flag，再编写脚本将其再进行一次异或运算即可得到原flag

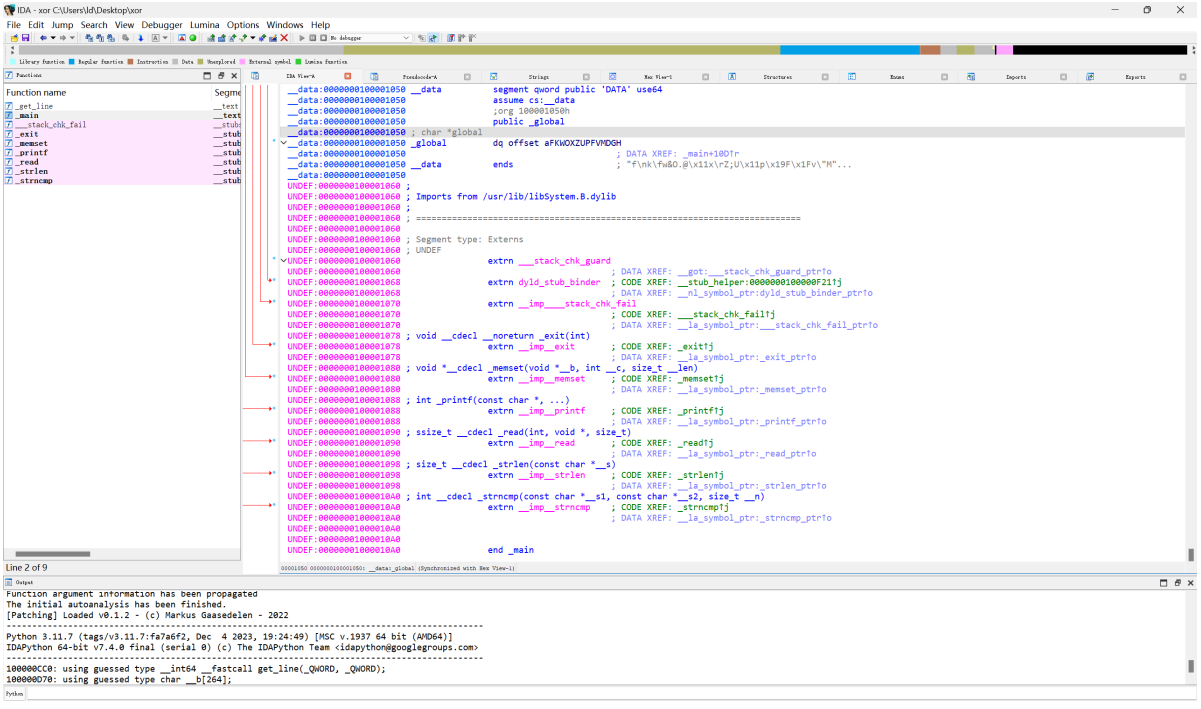
你问为什么两次异或得本身？ a^b^b == a^(b^b)

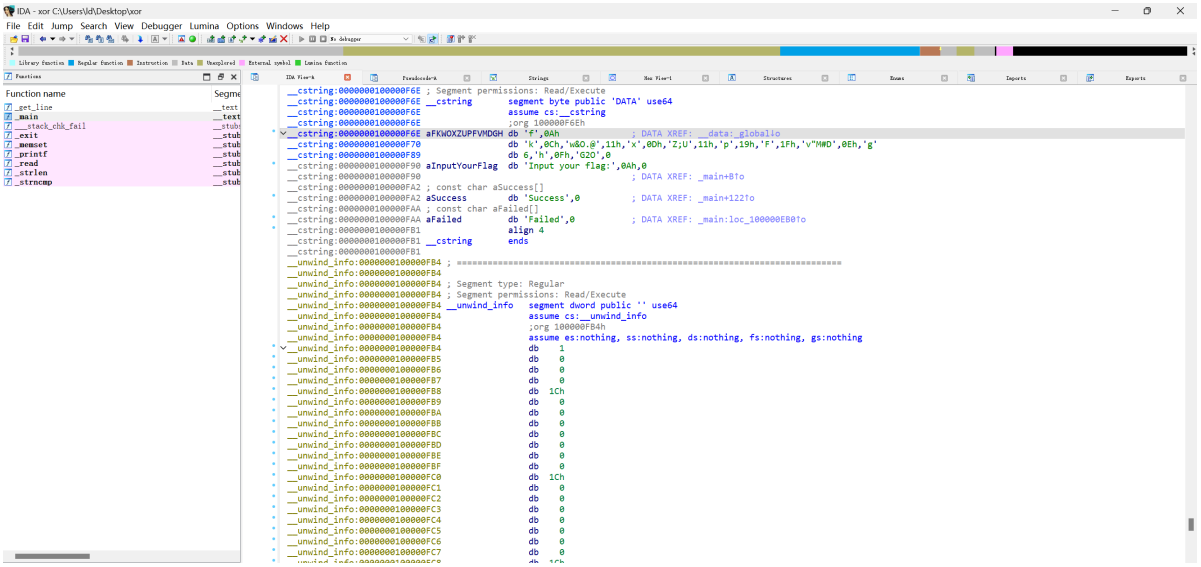
> 因为一个数异或自己等于 0000 0000，而 0000 0000异或任何数字，结果是任何数字本身

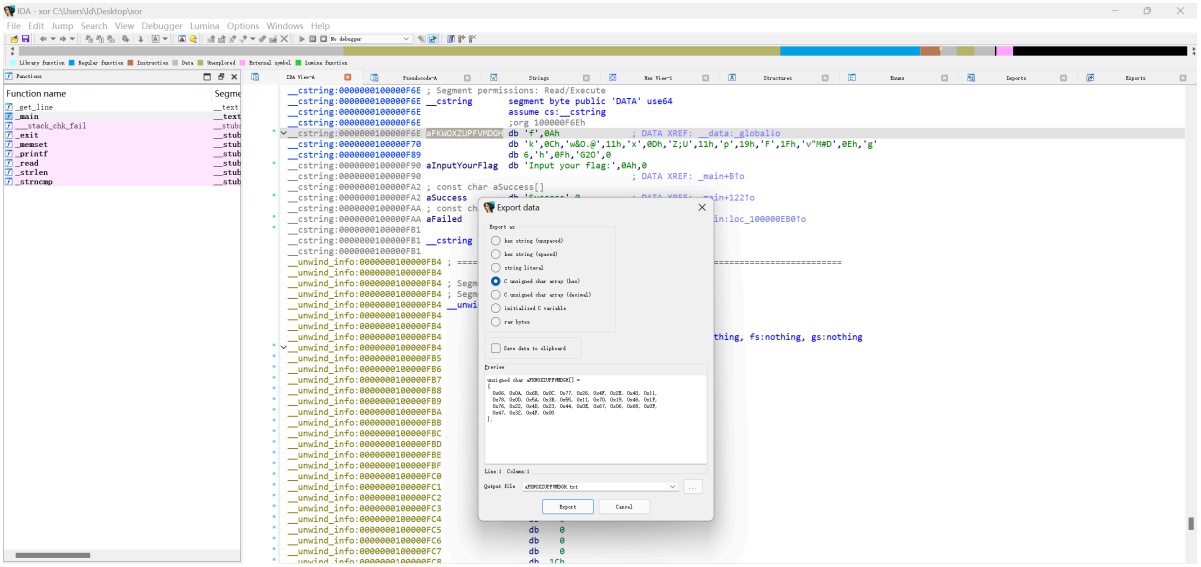
此时我们看到strcnmp函数（比较两个字符串是否相同的函数，可知global里面就是异或一次后的flag）咱们双击global



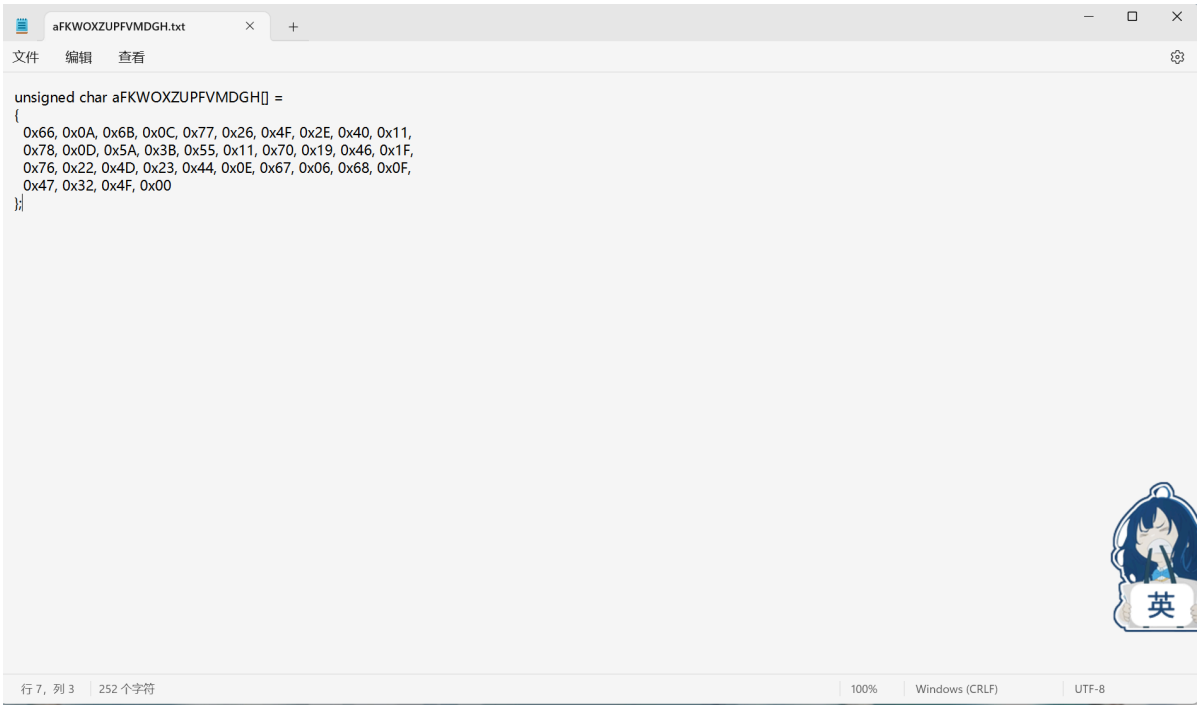
跟进flag可以看到一个偏移地址，再跟进aF一堆字母就可以得到一堆字符串



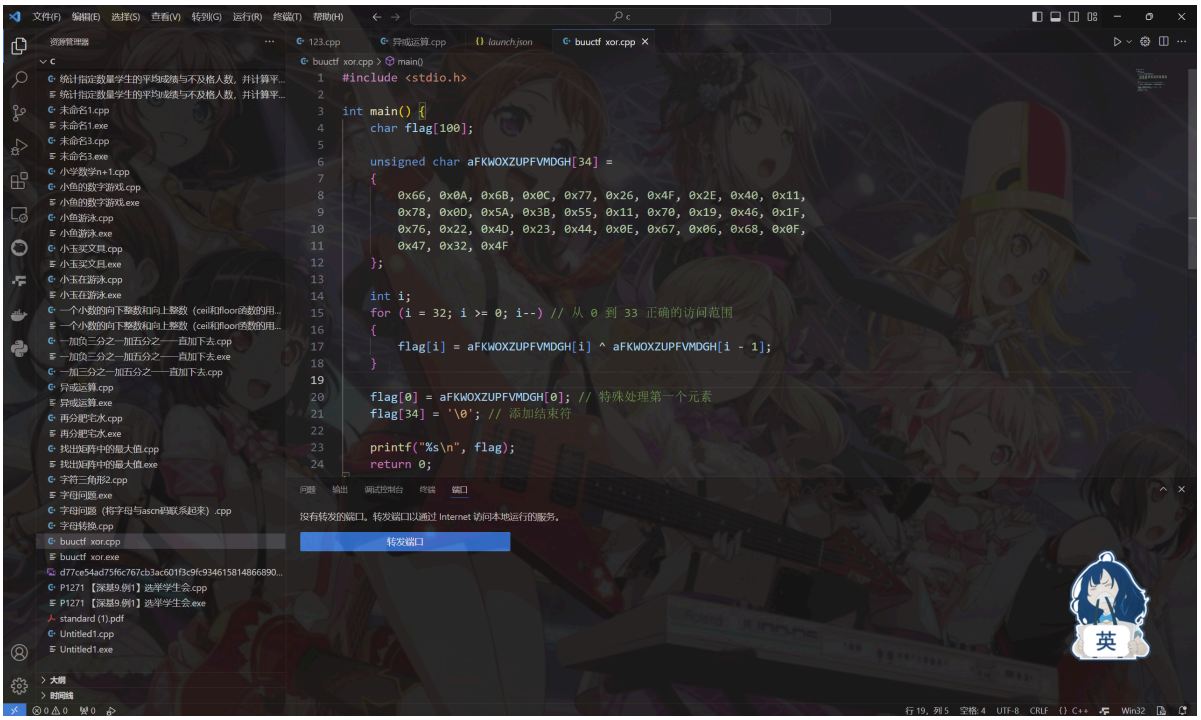




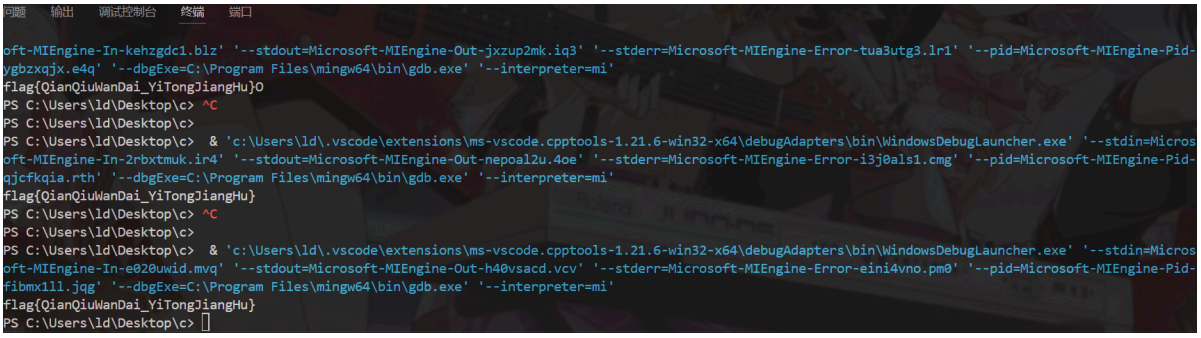
将这个字符串按 `shift+E` 即可将数据导出成一个txt文件



这个时候我们就可以利用它来写逆向脚本了（这里我用c写的）


#include <stdio.h>
int main() {
char flag[100];
unsigned char aFKWOXZUPFVMDGH[34] =
{
0x66, 0x0A, 0x6B, 0x0C, 0x77, 0x26, 0x4F, 0x2E, 0x40, 0x11,
0x78, 0x0D, 0x5A, 0x3B, 0x55, 0x11, 0x70, 0x19, 0x46, 0x1F,
0x76, 0x22, 0x4D, 0x23, 0x44, 0x0E, 0x67, 0x06, 0x68, 0x0F,
0x47, 0x32, 0x4F
};
int i;
for (i = 32; i >= 0; i--) // 从 0 到 33 正确的访问范围
{
flag[i] = aFKWOXZUPFVMDGH[i] ^ aFKWOXZUPFVMDGH[i - 1];
}
flag[0] = aFKWOXZUPFVMDGH[0]; // 特殊处理第一个元素
flag[34] = '\0'; // 添加结束符
printf("%s\n", flag);
return 0;
}
没有转发的端口。转发端口以通过 Internet 访问本地运行的服务。
转发端口

运行以后即可得到答案


oft-MIEngine-In-kehzgdc1.blz' '--stdout=Microsoft-MIEngine-Out-jxzup2mk.iq3' '--stderr=Microsoft-MIEngine-Error-tua3utg3.lr1' '--pid=Microsoft-MIEngine-Pid-ygbzxqjx.e4q' '--dbgExe=C:\Program Files\mingw64\bin\gdb.exe' '--interpreter=mi'
flag{QianQiuWanDai_YiTongJiangHu}O
PS C:\Users\ld\Desktop\c> ^C
PS C:\Users\ld\Desktop\c>
PS C:\Users\ld\Desktop\c> & 'c:\Users\ld\.vscode\extensions\ms-vscode.cpptools-1.21.6-win32-x64\debugAdapters\bin\WindowsDebugLauncher.exe' '--stdin=Microsoft-MIEngine-In-2rbxtmuk.ir4' '--stdout=Microsoft-MIEngine-Out-nepoal2u.4oe' '--stderr=Microsoft-MIEngine-Error-i3j0als1.cmg' '--pid=Microsoft-MIEngine-Pid-qjcfkqia.rth' '--dbgExe=C:\Program Files\mingw64\bin\gdb.exe' '--interpreter=mi'
flag{QianQiuWanDai_YiTongJiangHu}
PS C:\Users\ld\Desktop\c> ^C
PS C:\Users\ld\Desktop\c>
PS C:\Users\ld\Desktop\c> & 'c:\Users\ld\.vscode\extensions\ms-vscode.cpptools-1.21.6-win32-x64\debugAdapters\bin\WindowsDebugLauncher.exe' '--stdin=Microsoft-MIEngine-In-e020uwid.mvq' '--stdout=Microsoft-MIEngine-Out-h40vsacd.vcv' '--stderr=Microsoft-MIEngine-Error-eini4vno.pm0' '--pid=Microsoft-MIEngine-Pid-fibmx1ll.jqg' '--dbgExe=C:\Program Files\mingw64\bin\gdb.exe' '--interpreter=mi'
flag{QianQiuWanDai_YiTongJiangHu}
PS C:\Users\ld\Desktop\c>