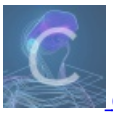
XCTF中hackme

原创

Most3R-03 于 2020-01-16 08:20:37 发布 281 收藏

分类专栏： ctf安全实验室逆向

本文链接：https://blog.csdn.net/recordliu/article/details/103998645

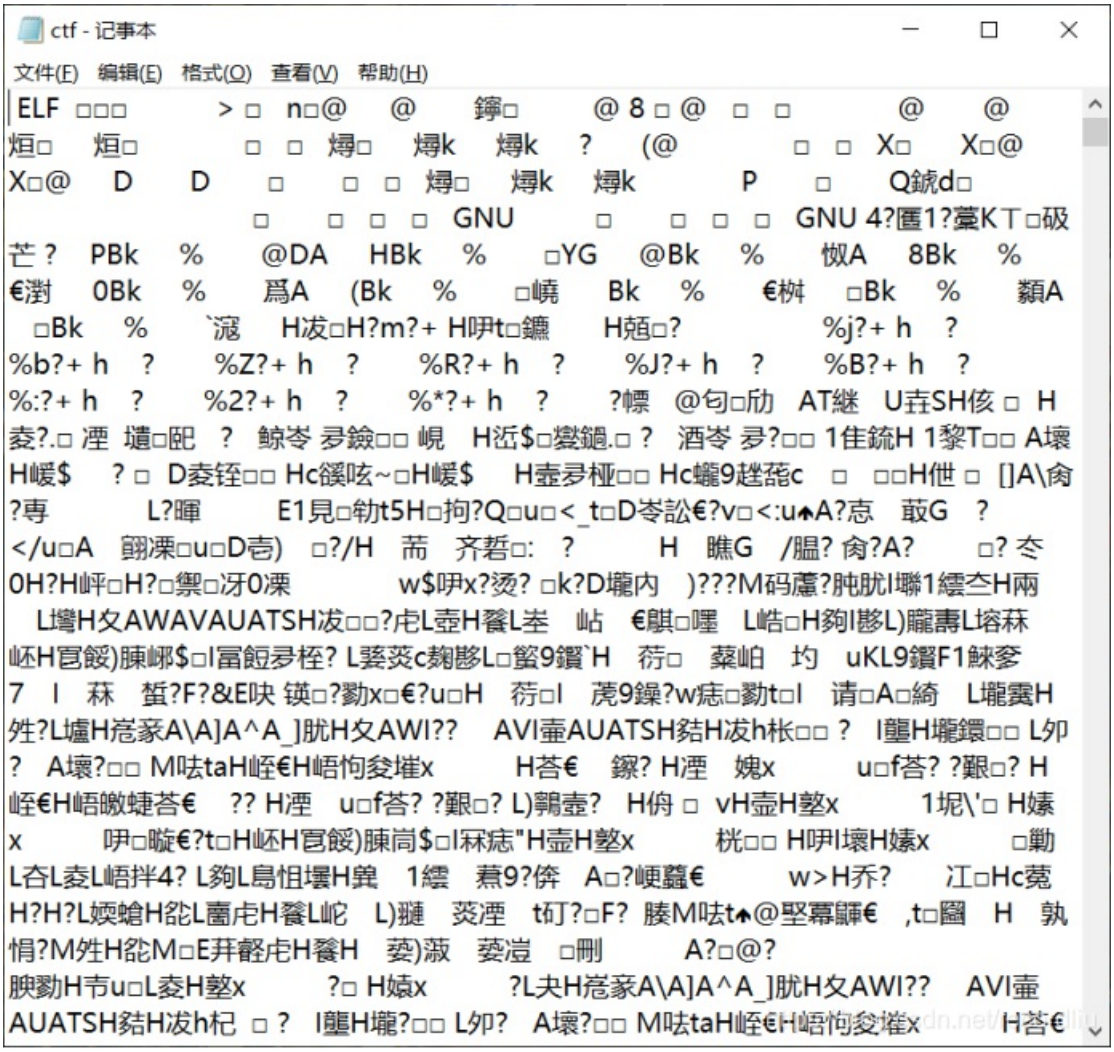


总结

写代码时注意类型值的范围，防止超出范围导致结果或者运行异常。

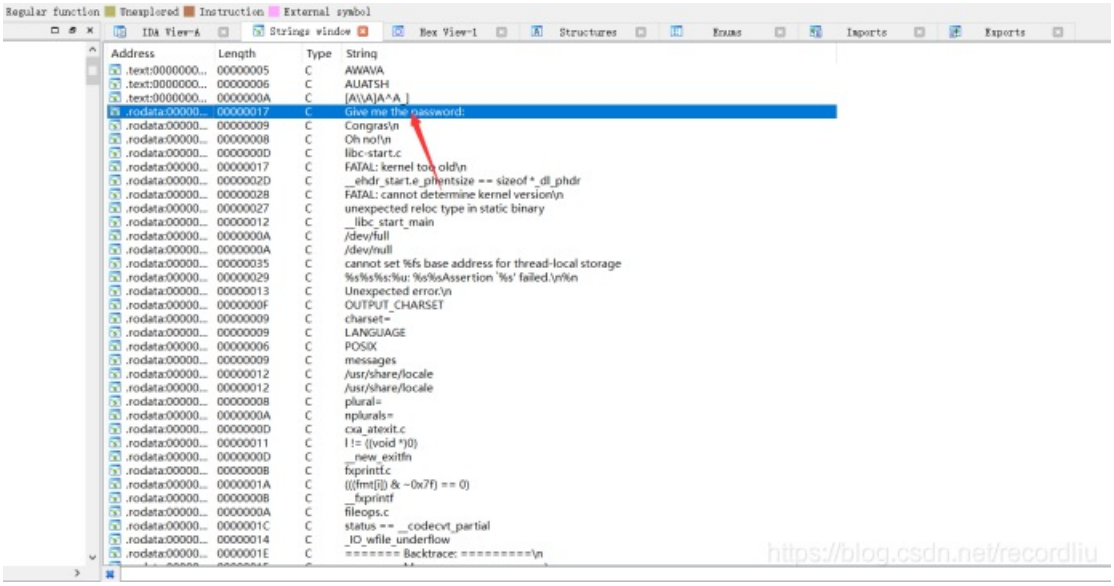
逆向开始

不是exe文件，记事本打开一下，发现是elf linux文件。

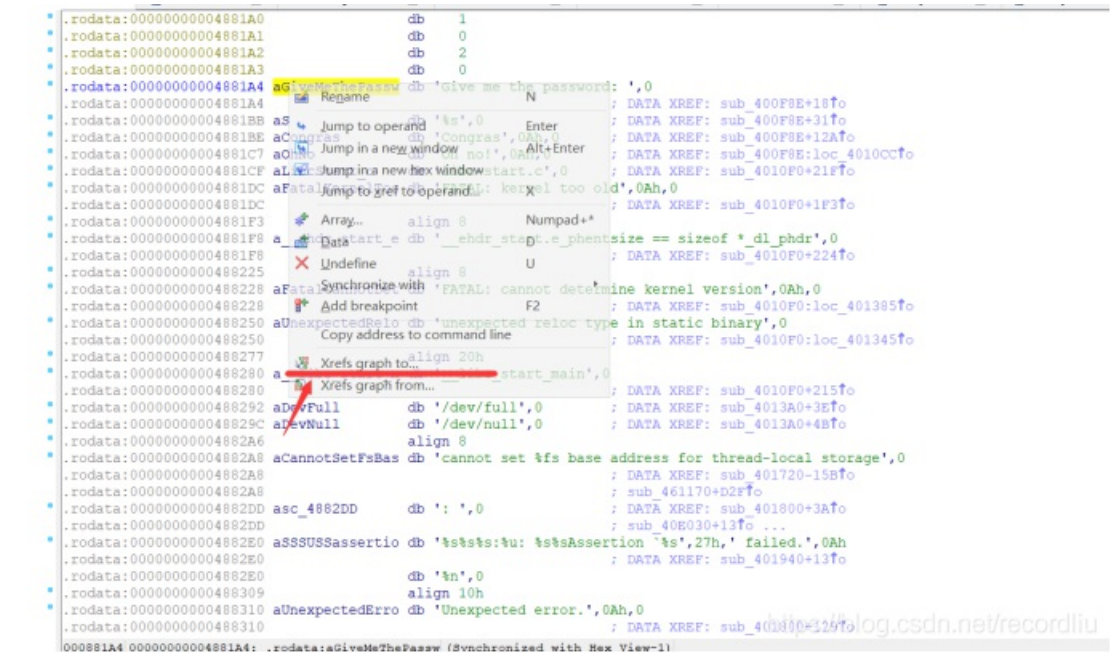


无法载入OD，选择直接拖入ida64位

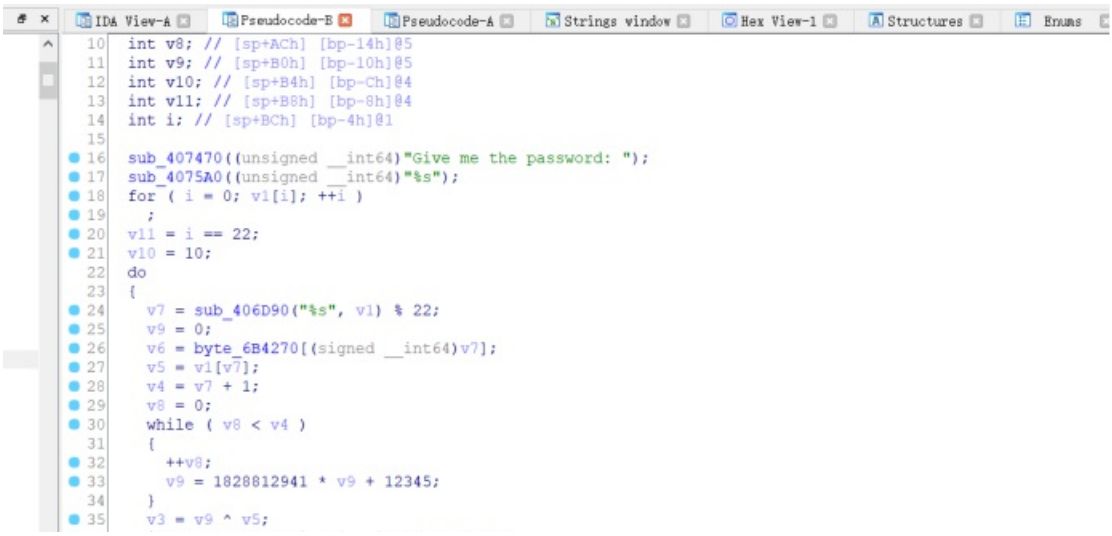
文件略大，直接按shift+f12进入字符串。



发现有关键字，双击进去看看，



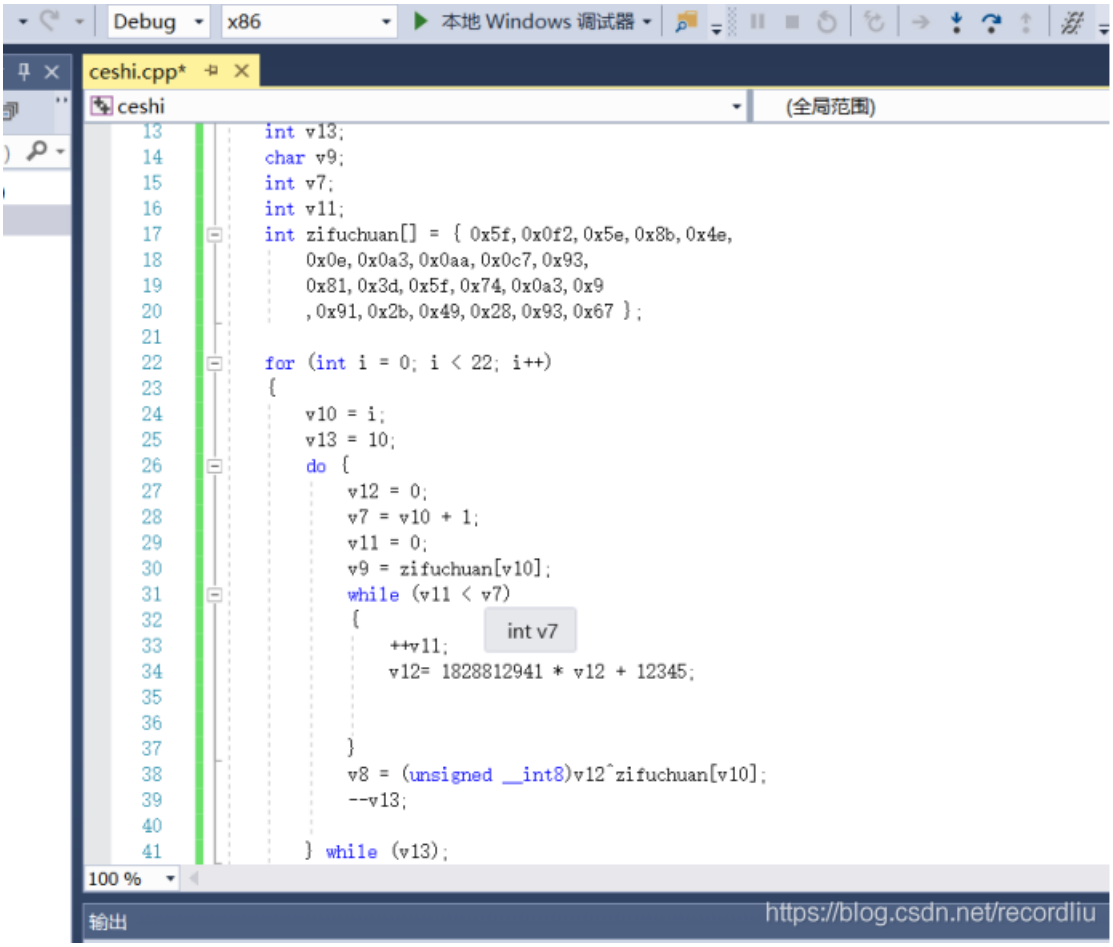
右击选择交叉引用，到400f8e处直接按f5伪代码。

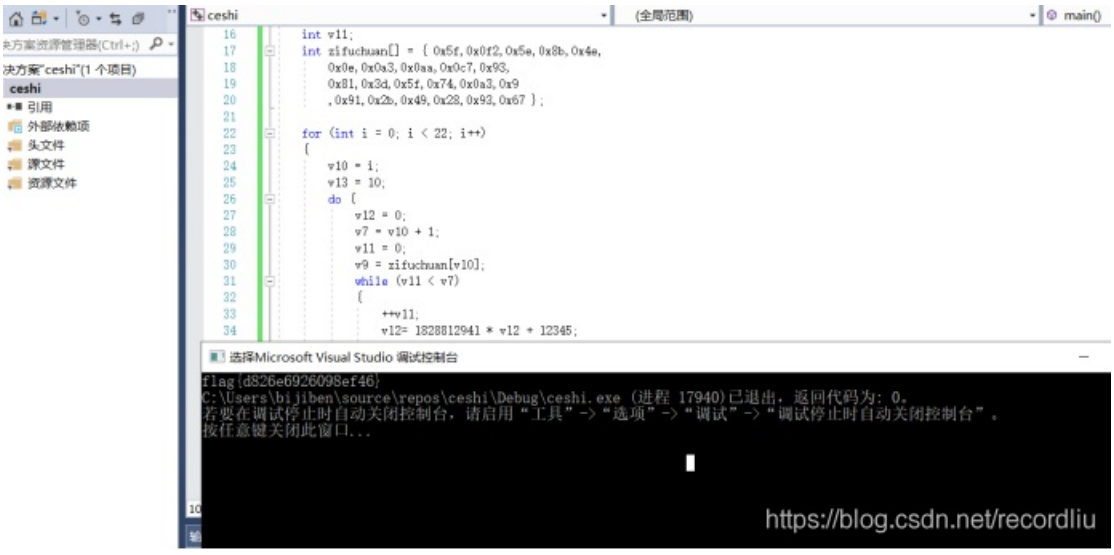


```
36    if ( v6 != ((unsigned __int8)v9 ^ v5) )
37      v11 = 0;
38    --v10;
39  }
40  while ( v10 );
41  if ( v11 )
42    v2 = sub_407470((unsigned __int64)"Congras\n");
43  else
44    v2 = sub_407470((unsigned __int64)"Oh no!\n");
45  return 0LL;
46}
000010B8 sub_400F8E:42
```

找到关键代码，开始分析写题解

v7只有22个数，我们可以用一个for循环，把v10都等于一遍





A12应该在do里每次循环都置一次0，防止过大超出int的范围导致循环异常。