re2

发表于 2021-01-04 分类于 Challenge， 2016， 西普杯京津冀信息安全挑战赛， Reverse
Challenge | 2016 | 西普杯京津冀信息安全挑战赛 | Reverse | re2

点击此处获得更好的阅读体验

来源

来自Prowes5原创投稿

题目考点

- *MFC逆向*

解题思路

看图标就知道是MFC写的，还是老套路，拖进IDA看下，由于是MFC写的，可能会有些复杂，不过问题不大。先看一下有没有关键的字符串。

可以看到有base64的痕迹，尝试了一下，并不能成功解码。运行起来看看吧。

要求输入正确的密码就会显示flag。但这里又不是标准的base64，猜测可能只是修改的table。

在0x00401743地址处发现了一个比较函数，可以直接动态运行到这里，看看输入的字符串加密过后是什么样的。输入123456，下断点观察一下。（比较函数上方还有一个判断长度的地方，修改一下标志位跳过即可）

发现输入的字符串其实并没有被编码，那就直接输入下边这个HOWMP半块西瓜皮hehe就会得到flag。

FLAG

```
1 flag{881baed760e0fb03d47xeafdf616f322}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2016/西普杯京津冀信息安全挑战赛/Reverse/oSmDDhDzg3Dh7YWazqnFoj.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # 2016 # Reverse # 西普杯京津冀信息安全挑战赛
CrackMe1
re1