

icekey

发表于 2021-01-04 分类于 [Challenge](#) , [2019](#) , [湖湘杯](#) , [Misc](#)
[Challenge](#) | [2019](#) | [湖湘杯](#) | [Misc](#) | [icekey](#)

[点击此处](#)获得更好的阅读体验

题目考点

- C#逆向

解题思路

载入dnspy后，找到main函数。发现程序将输入的32个字节字符串进行加密，密钥是icekey的md5值，然后内存16进制转为64字节大小的字符串和密文b比较，相同则输入的内容为flag。题目内置了解密函数，通过右键对调用加密函数的地方编辑IL指令，选择方法引用，修改enc操作的那个函数为dec操作的那个函数。然后在输入字符串后下断，断下来之后将输入字符串地址通过cheatengine修改它的内存数据为密文b，也就是让程序对密文调用解密操作，完了后再通过cheatengine查看解密结果：

□

Flag

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge/2019/湖湘杯/Misc/fHGrYUW2jCuJWrjWvQQVd.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](#) # [Misc](#) # [2019](#) # [湖湘杯](#)

[ezre](#)

[misc4](#)