

CTF中压缩包解密

原创

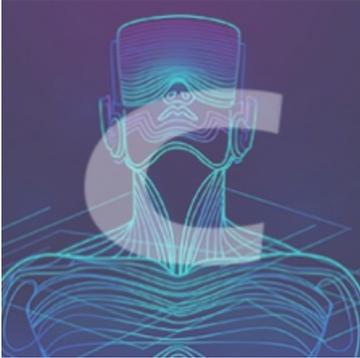
Stray.io 于 2020-07-25 16:40:29 发布 1128 收藏 2

分类专栏: [Web安全-CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/qq_45927819/article/details/107580373

版权



[Web安全-CTF 专栏收录该内容](#)

19 篇文章 1 订阅

订阅专栏

1.修复压缩包 (zip文件修复): 一般使用winhex这个工具, 简单点的就是改一下后缀、修复文件头等等。

2.暴力破解: 就是逐个尝试选定集合中可以组成的所有密码, 直到找到正确的密码。使用暴力破解需要一些工具, 例如rarcrack这个工具, 但它仅支持RAR、ZIP、7Z这三种类型。

3.明文攻击: 明文攻击是一种较为高效的攻击手段, 大致原理是当你不知道一个zip的密码, 但是你有zip中的一个已知文件 (文件大小要大于12Byte) 或者已经通过其他手段知道zip加密文件中的某些内容时, 因为同一个zip压缩包里的所有文件都是使用同一个加密密钥来加密的, 所以可以用已知文件来找加密密钥, 利用密钥来解锁其他加密文件。工具: ARCHPR、PKCRACK

4.字典破解: 字典破解的工作效率比爆破高, 字典中储存了常用密码, 因此也就避免了爆破时把时间浪费在一些简单的密码租场上面。

5.掩码攻击: 如果已知密码的某几位或者一直6位密码的第3位是a, 那么可以构造?? a? ?? 进行掩码攻击, 相当于构造出了第三位密码为a的字典。