




MOCTF crypto 密码学 writeup

原创

Um0  于 2019-03-14 20:32:46 发布  373  收藏

分类专栏: [MOCTF](#) 文章标签: [ctf 密码学](#) [MOCTF 加密与解密](#) [网络信息安全](#)

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_41358038/article/details/88560703

版权



[MOCTF 专栏收录该内容](#)

3 篇文章 0 订阅

订阅专栏

MOCTF crypto 密码学 writeup

- [1.数据库密码](#)
- [2.rot 大法好](#)
- [3.奇怪汉字](#)
- [4.就是这个feel](#)
- [5.贝斯族谱](#)
- [6.贝斯族谱升级版](#)
- [7.卡哇伊](#)
- [8.我觉得ok](#)
- [等待题目更新](#)

1.数据库密码

D8EA7326E6EC5916ACCD6E0C9D264C63

涉及到数据库, 猜到是md5, 但没想到是要把0-9, A-F 之外的字母删掉再md5解密。

还是对md5了解不够

MD5编码:

要么全为大写, 要么全为小写

字符数量16/32

MD5的取值范围是0~9 a~f

2.rot 大法好

想到了rot13

直接凯撒密码位移13位, 发现

}eDocne_toR{ftcom

倒过来就是flag

3.奇怪汉字

题目中的“当铺”是关键点。
当铺密码

当铺密码

由口中 由由夫 由由口 由由口 由中由

转换密码↓

102 117 110 110 121

简介：当前汉字有多少笔画出头，就是转化成数字几。
(例：王夫井工夫口 = 678470)

返回

https://blog.csdn.net/qq_41358038

得到了五个数字，对照ASCII码表，得到funny，套上格式提交，正确。

4.就是这个feel

恰恰 恰恰恰 恰绑恰绑 恰 绑绑恰绑 {恰恰绑 恰恰恰 恰恰恰 恰绑绑}

一开始，我以为

“恰恰 恰恰恰 恰绑恰绑 恰 绑绑恰绑”分别代表“moctf”

所以后面的内容就可以知道是{恰恰绑 o o 恰恰绑}

但是“恰恰绑”又代表什么呢？

没有思路

又观察了一下，发现只有 恰绑 这两个字，是不是可以表示成摩斯电码呢？

把恰表示成- 绑表示成·

所以

“-- -- - . - . . . - { - . - - - . . . }”

摩斯密码转换

英文字母:

MOCTFGOOD

转换为摩斯电码 ↓

转换为英文字母 ↑

摩斯电码: (用空格分隔摩斯电码)

-- -- - . - . . . - { - . - - - . . . }

https://blog.csdn.net/qq_41358038

5. 贝斯族谱

将给出的字符串不断Base64解密，最后得到ngn_qp{qdudtms0u1fz}
猜到是栅栏，但是栅栏解密始终得不到flag
但有一组是 npdug{t1nqmf_dszqu0}
样子很像moctf{xxxx}
再凯撒解密解一下
得到flag

6. 贝斯族谱升级版

将字符串Base64解密，再解下去发现解出乱码
所以再扔到Base32解一次
随后扔到Base16里解一次
得到flag

解密网站：<http://ctf.ssleye.com/base64.html>

7. 卡哇伊

AAencode

解密网站：<http://ctf.ssleye.com/aaencode.html>

8. 我觉得ok

Ook解密

解密网站：<https://tool.bugku.com/brainfuck/>

等待题目更新