i春秋misc部分writeup

转载

weixin_30681121 于 2018-12-24 22:13:00 发布 421 收藏 1
文章标签： 数据库
原文链接：http://www.cnblogs.com/zwshi/p/10171312.html

i春秋misc部分writeup

一、敲击

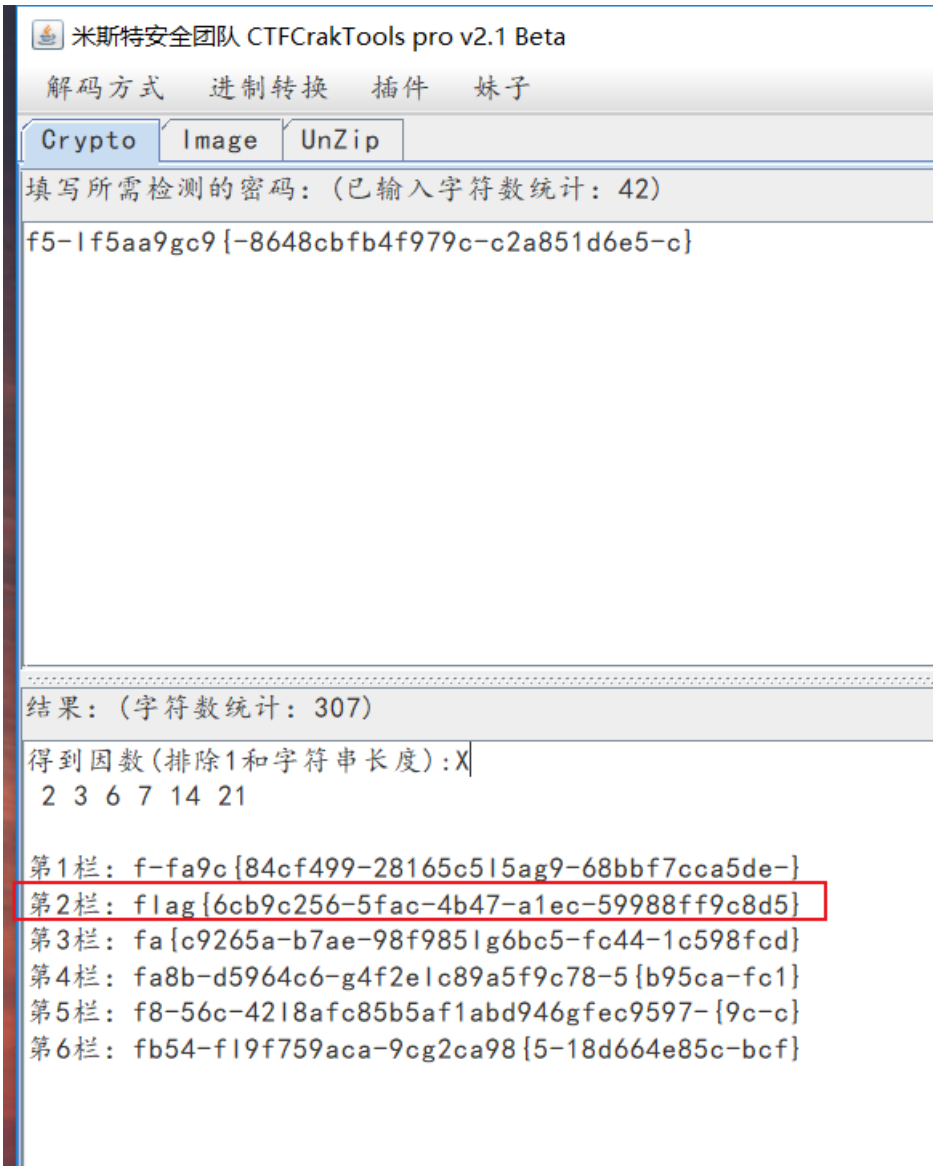
方方格格，然后看到下面的格式，猜测出是键盘上的布局，然后看这些字母形成的形状想那些字母，就是flag了

2、滴滴滴

放到ctfcack里解密，发现时栅栏密码，就得到flag了

3、山岚

一样放到ctfcack里栅栏解密



4、xx

根据题目，知道是xxencode编码，直接在线解码就是了

5、贝丝家族

base家族有base64，base32，base16，

MZWGCZ33MVZGQZLJL5STQOJTGRPWK4SVJ56Q====有36位再加上4位垫字符，所以用base32解码就可以得到flag

6、一个16岁的少年

base16解码

7、藏在邮件头里的秘密

可打印字符编码(Quoted_Printable),在线解码即得到flag , http://www.mxcz.net/tools/QuotedPrintable.aspx

8、misc1

用hex打开图片，搜索flag，可以得到flag

8、misc2

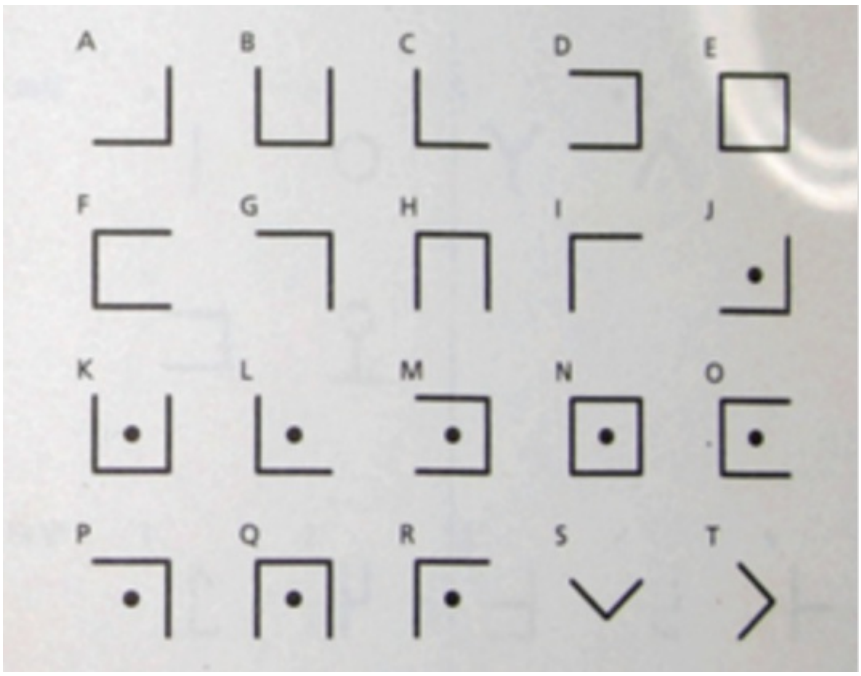
转载：

这题目如果从隐写的思路去做，做不出来

如果不是老司机，很难想到是猪圈密码

1、关于猪圈密码

猪圈密码（亦称朱高密码、共济会暗号、共济会密码或共济会员密码），是一种以格子为基础的简单替代式密码。即使使用符号，也不会影响密码分析，亦可用在其它替代式的方法。



2、关于CTF中的猪圈密码

关于这一点，真是是需要经验累积出来的，刚参加比赛的新人是真的一时半会无法get到关键之处，因此需要多多练习CTF大本营里的真题，这里分享一个关于CTF的一个脑洞的编码解码题目快速入门方法，CTF中脑洞大开的编码解码。配合CTF大本营的题目去学习这篇文章，那么以后在一般的CTF比赛中，遇到类似的问题就很容易解决啦。

PS：像这类的脑洞编码解码类题目，以后应该会慢慢淡出CTF比赛的赛场，对于选手本身的知识收益实在是太少了。

9、泄露的数据

由题可知是数据库泄露的数据，所以猜想可能是md5加密，直接md5解密

10、听说是rc4算法？

直接就提示了rc4算法，但在线解密解不出来（我试的时候）

然后看了别人写的脚本：

import random, base64from hashlib import sha1

def crypt(data, key): x = 0 box = range(256) for i in range(256): x = (x + box[i] + ord(key[i % len(key)])) % 256 box[i], box[x] = box[x], box[i] x = y = 0 out = [] for char in data: x = (x + 1) % 256 y = (y + box[x]) % 256 box[x], box[y] = box[y], box[x] out.append(chr(ord(char) ^ box[(box[x] + box[y]) % 256])) return ''.join(out)

def tdecode(data, key, decode=base64.b64decode, salt_length=16): if decode: data = decode(data) salt = data[:salt_length] return crypt(data[salt_length:], sha1(key + salt).digest())

if **name** =='**main**': data = 'UUyFTj8PCzF6geFn6xgBOYSvVTrbpNU4OF9db9wMcPD1yDbaJw ==' key = 'welcometoicqedu' decoded_data = tdecode(data=data, key=key) print decoded_data

得到flag：flag{rc4_l_keepgoing}

11、福尔摩斯

就是摩斯密码, 不过题目给的这种字符一般解不出 ·-· ·-· ·-· ·-· ·-· ·-· , 一般模式电码是点在下面, 横在上面.

要改为: .-. .-. .-. .-. .-. .-. . 这样就行了.

12、misc（键盘坐标）

解题思路：首先应该了解一下·什么是键盘坐标密码：、

我们注意到大键盘区所有的字母上面都有其对应的数字，这个位置几乎在所有的键盘都是相同的。所以我们可以利用这一点应用单表替换的方法进行加密[注2]：

1 2 3 4 5 6 7 8 9 0

Q W E R T Y U I O P

A S D F G H J K L

Z X C V B N M

我们根据上表可以得出，Q是1下面的第一个，A是1下面的第二个……以此类推，每一个字母都会有其对应的数字： A 12 B 53 C 33 第一个数字代表横向（X坐标）的位置，第二个数字代表纵向（Y坐标）的位置

就可以得到最后的答案：flag{QAZIJ**}

13、+——+

brainfuck

根据题目给的密文特性可以看出来是采用的brainfuck进行的加密，那么采用相应的在线解密工具解密即可！https://www.splitbrain.org/services/ook

解密后得到flag{671fb608-265a-492f-a041-b30bb8569490}

14、misc纵横四海

下载文件解压然后后进入文件夹里面按住shift键然后鼠标右键然后找到在此处打开cmd窗口或者Windows PowerShell窗口然后执行type dabiaojie* >>flag.txt 之后在文件最后找到flag.txt文件去掉换行和后面没用的字母就行了：

你就成功获取到flag此答案咯

转载于:https://www.cnblogs.com/zwshi/p/10171312.html