安全-破译（i春秋）

原创

小狐狸FM   于 2020-03-12 21:13:42 发布   374   收藏

分类专栏： 安全 # CTF夺旗 文章标签： 安全

 安全 同时被 2 个专栏收录

91 篇文章 8 订阅
订阅专栏

CTF夺旗

38 篇文章 0 订阅
订阅专栏

文章目录

前言

本人并不精通CTF，以下的内容不全是自己思考出来的。
有结合了自己的一些思考和大佬的思路来解题。
题目的正确答案和米斯特工具在文章末尾。
建议不要直接复制黏贴flag，还是边学习边成长会更好些。

题目介绍:

题目名称: 破译
类型: Web
分值: 150分
题目内容:
破译下面的密文
TW5650Y - 0TS UZ50S S0V LZW UZ50WKW 9505KL4G 1X WVMUSL510 S001M0UWV 910VSG S0 WFLW0K510 1X LZW54 WF5KL50Y 2S4L0W4KZ52 L1 50U14214SLW X5L0WKK S0V TSK7WLTS88 VWNW8129W0L 50 W8W9W0LS4G, 95VV8W S0V Z5YZ KUZ118K SU41KK UZ50S.LZW S001M0UW9W0L ESK 9SVW SL S K5Y050Y UW4W910G L1VSG TG 0TS UZ50S UW1 VSN5V KZ1W9S7W4 S0V FM LS1, V54WUL14 YW0W4S8 1X LZW 50LW40SL510S8 U112W4SL510 S0V WFUZS0YW VW2S4L9W0L 1X LZW 9505KL4G 1X WVMUSL510.

"EW S4W WFU5LWV L1 T41SVW0 1M4 2S4L0W4KZ52 E5LZ LZW 9505KL4G 1X WVMUSL510 L1 9S7W S 810Y-8SKL50Y 592SUL 10 LZW 85NWK 1X UZ50WKW KLMVW0LK LZ41MYZ S 6150L8G-VWK5Y0WV TSK7WLTS88 UM445UM8M9 S0V S E5VW 4S0YW 1X KUZ118 TSK7WLTS88 241Y4S9K," KS5V KZ1W9S7W4. "LZ5K U1995L9W0L 9S47K S01LZW4 958WKL10W 50 LZW 0TS'K G1MLZ S0V TSK7WLTS88 VWNW8129W0L WXX14LK 50 UZ50S." X8SY{ YK182V9ZUL9STU5V}

【i春秋的CTF训练营】

原题密文:

```
TW5650Y - 0TS UZ50S S0V LZW UZ50WKW 9505KL4G 1X WVMUSL510 S001M0UWV 910VSG S0 WFLW0K510 1X LZW54 WF5KL50Y 2S4L0W
4KZ52 L1 50U14214SLW X5L0WKK S0V TSK7WLTS88 VWNW8129W0L 50 W8W9W0LS4G, 95VV8W S0V Z5YZ KUZ118K SU41KK UZ50S.LZW
S001M0UW9W0L ESK 9SVW SL S K5Y050Y UW4W910G L1VSG TG 0TS UZ50S UW1 VSN5V KZ1W9S7W4 S0V FM LS1, V54WUL14 YW0W4S8
1X LZW 50LW40SL510S8 U112W4SL510 S0V WFUZS0YW VW2S4L9W0L 1X LZW 9505KL4G 1X WVMUSL510. "EW S4W WFU5LWV L1 T41SVW
0 1M4 2S4L0W4KZ52 E5LZ LZW 9505KL4G 1X WVMUSL510 L1 9S7W S 810Y-8SKL50Y 592SUL 10 LZW 85NWK 1X UZ50WKW KLMVW0LK
LZ41MYZ S 6150L8G-VWK5Y0WV TSK7WLTS88 UM445UM8M9 S0V S E5VW 4S0YW 1X KUZ118 TSK7WLTS88 241Y4S9K," KS5V KZ1W9S7W4
. "LZ5K U1995L9W0L 9S47K S01LZW4 958WKL10W 50 LZW 0TS'K G1MLZ S0V TSK7WLTS88 VWNW8129W0L WXX14LK 50 UZ50S." X8SY
{ YK182V9ZUL9STU5V}
```
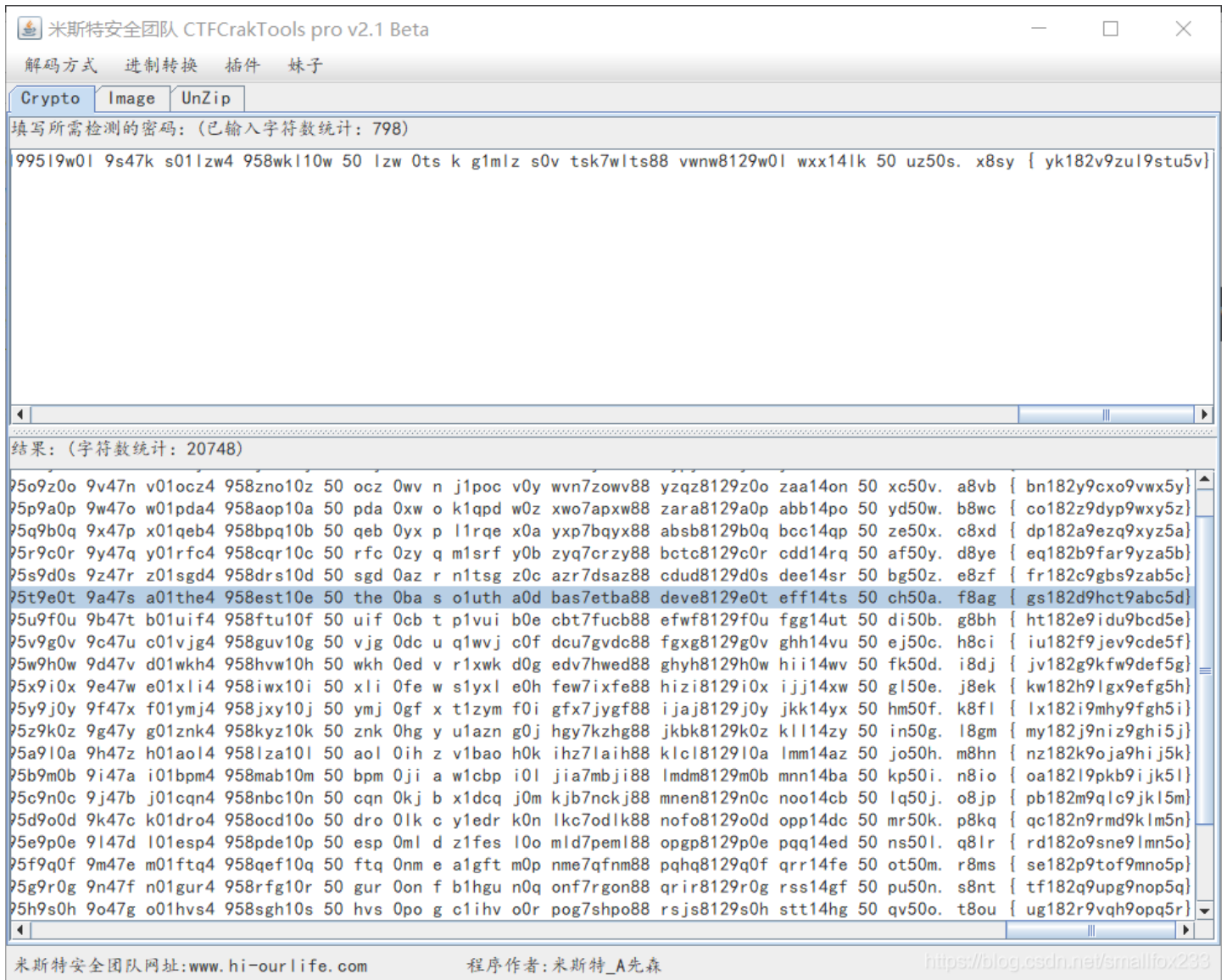
解题步骤:

(1) 凯撒解密

(2) 替换数字

注: 没试过先替换数字，再凯撒解密。 可能先(2)再(1)也行得通

[1]. 凯撒解密

注: 该选中行最可能是经过某个转换后的flag{**}语句,若进行数字的替换或许为正确答案

[2]. 数字替换:

注: 因为密文的总量较多,所以以下就用图片来说明

<1>经过凯撒移位选择后:

```
be5650g - 0ba ch50a a0d the ch50ese 9505st4o
1f educat510 a001u0ced 910dao a0 ente0s510
1f the54 en5st50g 2a4t0e4sh52 t1 50c14214ate
1f5t0ess a0d bas7etba88 deve8129e0t 50 e8e9e0ta4o,
95dd8e a0d h5gh sch118s ac41ss ch50a.
the a001u0ce9e0t mas 9ade at a s5g050g ce4e910o
t1dao bo 0ba ch50a ce1 dav5d sh1e9a7e4 a0d nu ta1,
d54ect14 ge0e4a8 1f the 50te40at510a8 c112e4at510
a0d encha0ge de2a4t9e0t 1f the 9505st4o 1f educat510.
me a4e enc5ted t1 b41ade0 1u4 2a4t0e4sh52 m5th the
```

```
9505st4o 1f educat510 t1 9a7e a 810g-8ast50g 592act
10 the 85ves 1f ch50ese stude0ts th41ugh a
6150t8o-des5g0ed bas7etba88 cu445cu8u9 a0d a m5de
4a0ge 1f sch118 bas7etba88 241g4a9s, sa5d sh1e9a7e4.
th5s c1995t9e0t 9a47s a01the4 958est10e 50 the 0ba s
o1uth a0d bas7etba88 deve8129e0t eff14ts 50 ch50a.
f8ag { gs182d9hct9abc5d}
```

初步可以肯定的数字(单词里仅有少量未知数)：
f8ag (flag)： 8=l   //小写的L
a0d (and)： 0=n
sa5d (said)和 th5s (this)： 5=i
bas7etba88 (basketball)： 7=k
即： 0=>n 5=>i
　　 7=>k 8=>l

<2>将上述可能性较大的数字替换成字母后：
//可用python的replace函数替换

```
bei6ing - nba china and the chinese 9inist4o1f educati1n
 ann1unced 91ndao an entensi1n1f thei4 enisting 2a4tne4shi2
 t1 inc14214atefitness and basketball devel129ent in ele9enta4o,
 9iddle and high sch11ls ac41ss china. the ann1unce9ent mas
 9ade at a signing ce4e91no  t1dao bo nba china ce1 david
 sh1e9ake4 and nu ta1, di4ect14 gene4al 1f the inte4nati1nal
 c112e4ati1n  and enchange de2a4t9ent 1f the 9inist4o 1f educati1n.
 me a4e encited t1 b41aden 1u4 2a4tne4shi2 mith the  9inist4o
 1f educati1n t1 9ake a l1ng-lasting i92act 1n the lives 1f
 chinese students th41ugh a 61intlo-designed basketball cu44iculu9
 and a mide  4ange 1f sch11l basketball 241g4a9s, said sh1e9ake4.
 this c199it9ent 9a4ks an1the4 9ilest1ne in the nba s  o1uth and
 basketball devel129ent eff14ts in china. flag { gs1l2d9hct9abcid}
```

比较能确定的数字(最好是用多个单词进行对比)：
educati1n (education)和 1f (of)： 1=o   //原本根据1f(if)和eff14ts (effects)猜想1对应的i是错误的.
eff14ts (efforts)和 4ange (range)： 4=r
devel129ent (development) 和 ann1unce9ent (announcement)： 2=p 9=m
即： 1=>o 2=>p
　　 4=>r 9=>m

<3>将上述比较能确定的数字替换成字母后为最终结果：
//可用python的replace函数替换

```
bei6ing - nba china and the chinese ministroof education
announced mondao an entensionof their enisting partnership
to incorporatefitness and basketball development in elementaro,
middle and high schools across china. the announcement mas made
at a signing ceremono  todao bo nba china ceo david shoemaker and nu tao,
 director general of the international cooperation  and enchange
 department of the ministro of education. me are encited to broaden
 our partnership mith the  ministro of education to make a long-lasting
 impact on the lives of chinese students through a 6ointlo-designed
 basketball curriculum and a mide  range of school basketball programs,
 said shoemaker. this commitment marks another milestone in the nba s
 oouth and basketball development efforts in china. flag { gsolpdmhctmabcid}
```

经过测试之后，真正的值不为 `flag{gsolpdmhctmabcid}` ，而是需要转换为大写.

正确答案

工具

提取码: r6cm

工具

提取码: r6cm