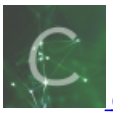
BUUCTF 打卡4

原创

路由(_)生 于 2021-08-23 22:06:51 发布 122 收藏

分类专栏： crypto 文章标签： 其他

本文链接：https://blog.csdn.net/qq_52193383/article/details/119870631


crypto 专栏收录该内容

35 篇文章 3 订阅

订阅专栏

1.rot

首先看到这些数字，第一反应是觉得是ascii码,而且题目是rot，应该是属于移位密码了，把前几个数跟'flag'对应，出来的不对。既然不是小写，那应该是大写'FLAG'，得到

FLAG IS flag{www_shiyanbar_com_is_very_good_???}

MD5:38e4c352809e150186920aac37190cbc

出来的是明文和md5加密后的密文，那应该是要进行爆破了。

```
s = '83 89 78 84 45 86 96 45 115 121 110 116 136 132 132 132 108 128 117 118 134 110 123 111 110 127 108 112 124
 122 108 118 128 108 131 114 127 134 108 116 124 124 113 108 76 76 76 76 138 23 90 81 66 71 64 69 114 65 112 64
66 63 69 61 70 114 62 66 61 62 69 67 70 63 61 110 110 112 64 68 62 70 61 112 111 112'
s = s.split(' ')
for i in s:
    print(chr(int(i)-13),end = '')
#FLAG IS flag{www_shiyanbar_com_is_very_good_????}
#MD5:38e4c352809e150186920aac37190cbc
import hashlib
for i in range(32,127):
    for j in range(32,127):
        for k in range(32,127):
            for l in range(32,127):
                flag = 'flag{www_shiyanbar_com_is_very_good_'+chr(i)+chr(j)+chr(k)+chr(l)+'}'
                des=hashlib.md5(flag.encode()).hexdigest()
                if '38e4c352809e150186920aac37190cbc' == des:
                    print(flag)
```

2.[NCTF2019]Keyboard

```
ooo yyy ii w uuu ee uuuu yyy uuuu y w uuu i i rr w i i rr rrr uuuu rrr uuuu t ii uuuu i w u rrr ee www ee yyy ee
e www w tt ee
```

如果仔细看，可以发现里面出现的字母都在键盘的同一行，而且题目也提示了是键盘，估摸着是键盘加密了。再根据每一组字母的数量不同，想到我之前写过一个九宫格输入法解密的(纯数字)，非常相似。

但这题我们要先将字母转换成数字，按照键盘上从左往右的顺序，得到

```
888 555 77 1 666 22 6666 555 6666 5 1 666 7 7 33 1 7 7 33 333 6666 333 6666 4 77 6666 7 1 6 333 22 111 22 555 22
2 111 1 44 22
```

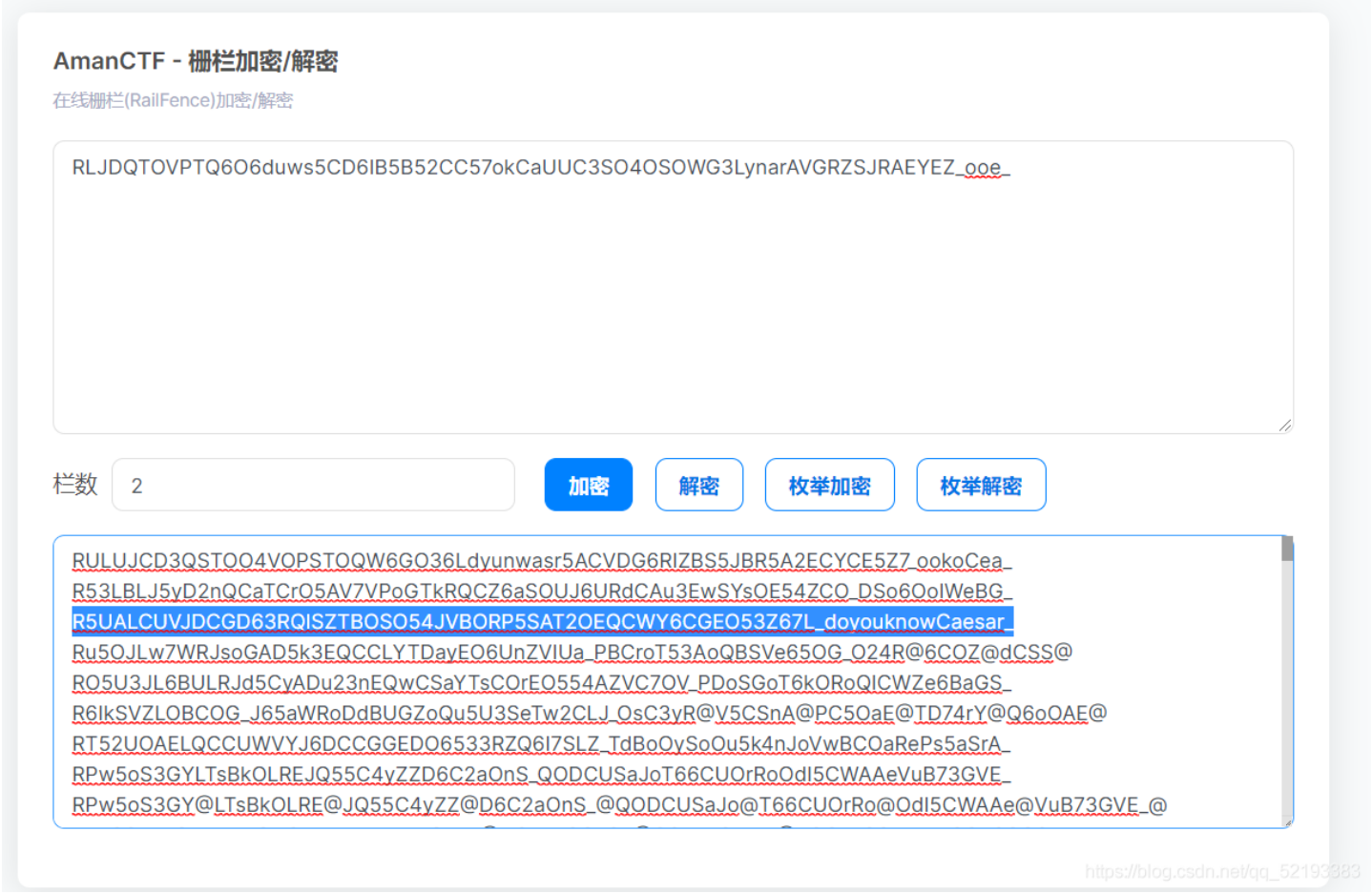
根据九宫格输入法，得到youaresosmartthatthisisjustapieceofcake

3.[WUSTCTF2020]佛说：只能四天

由于之前在解码网站上复制粘贴出来的文本会发生改变，不能解码。但现在又出来了新网站新约佛论禅，成功的解出来了，不过解出来的是核心价值观编码，还需进一步解码，
得到

```
RLJDQTOVPTQ6O6duws5CD6IB5B52CC57okCaUUC3SO4OSOWG3LynarAVGRZSJRAEYEZ_ooe_doyouknowfence
```

末尾给出提示：
do you know fence(栅栏)
将提示去掉，进行栅栏解密，穷举：



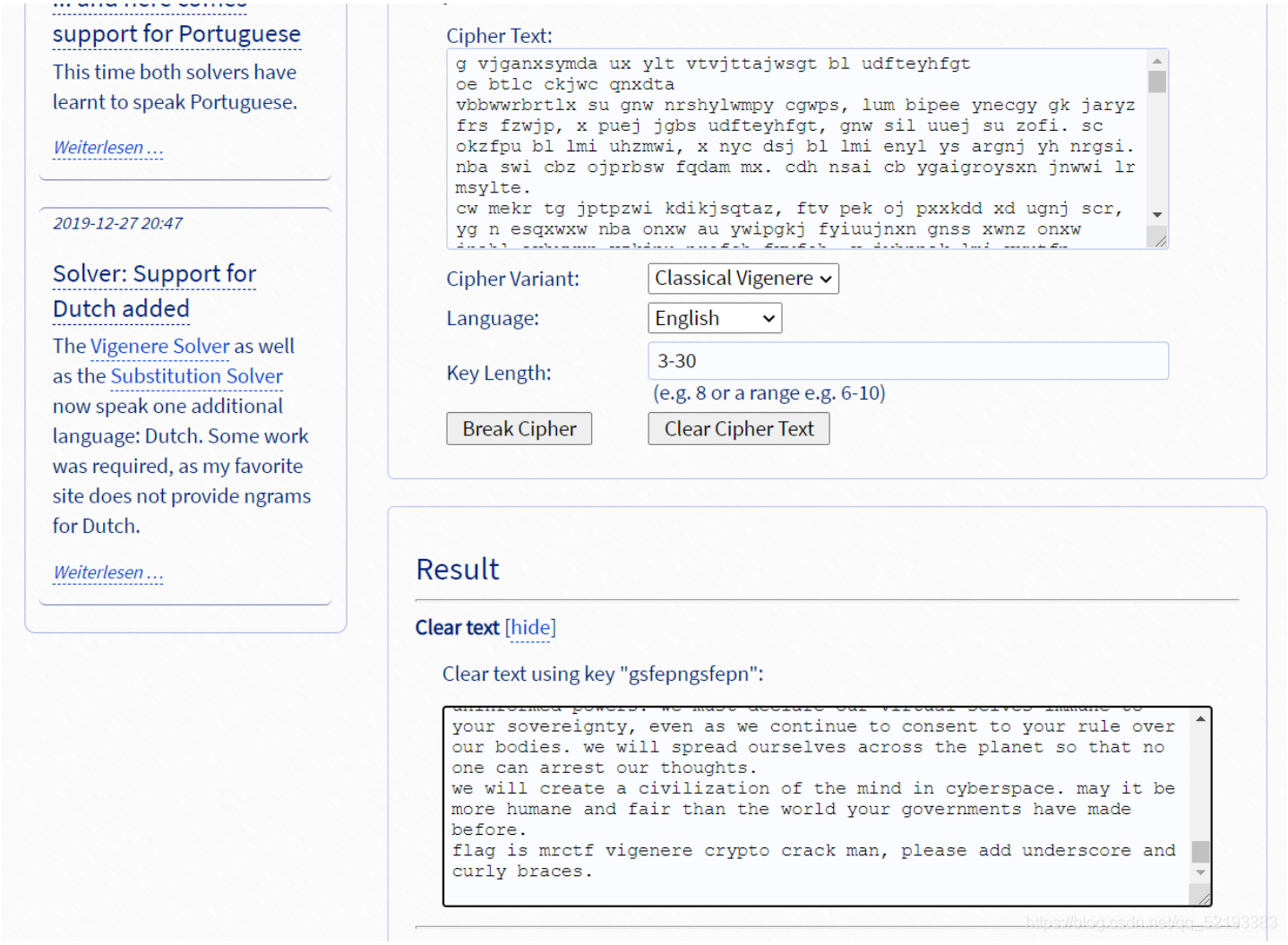
在第三条发现最合适的：R5UALCUVJDCGD63RQISZTBOSO54JVBORP5SAT2OEQCWY6CGEO53Z67L_doyouknowCaesar_
提示凯撒加密。
题目提示了凯撒不是最后一步。根据凯撒解密的出的内容可知，只含字母和数字，且字母均为大写，数字范围为2~7，应该是base32解码。对每行字符串进行base32解码。在位移量为3的时候解出wctf2020{ni_hao_xiang_xiang_da_wo}

不过根据提示”by the way，凯撒为什么叫做凯撒？“也可以猜测位移量为3，因为凯撒大帝使用的是3位位移量。

4.[MRCTF2020]vigenere

看到这么一大段字母，还以为是要先进行词频分析再vigenere解密。可惜词频分析还是一串乱序字母。看了别人的writeup才知道有网站可以在不知道密钥的情况下进行解密。

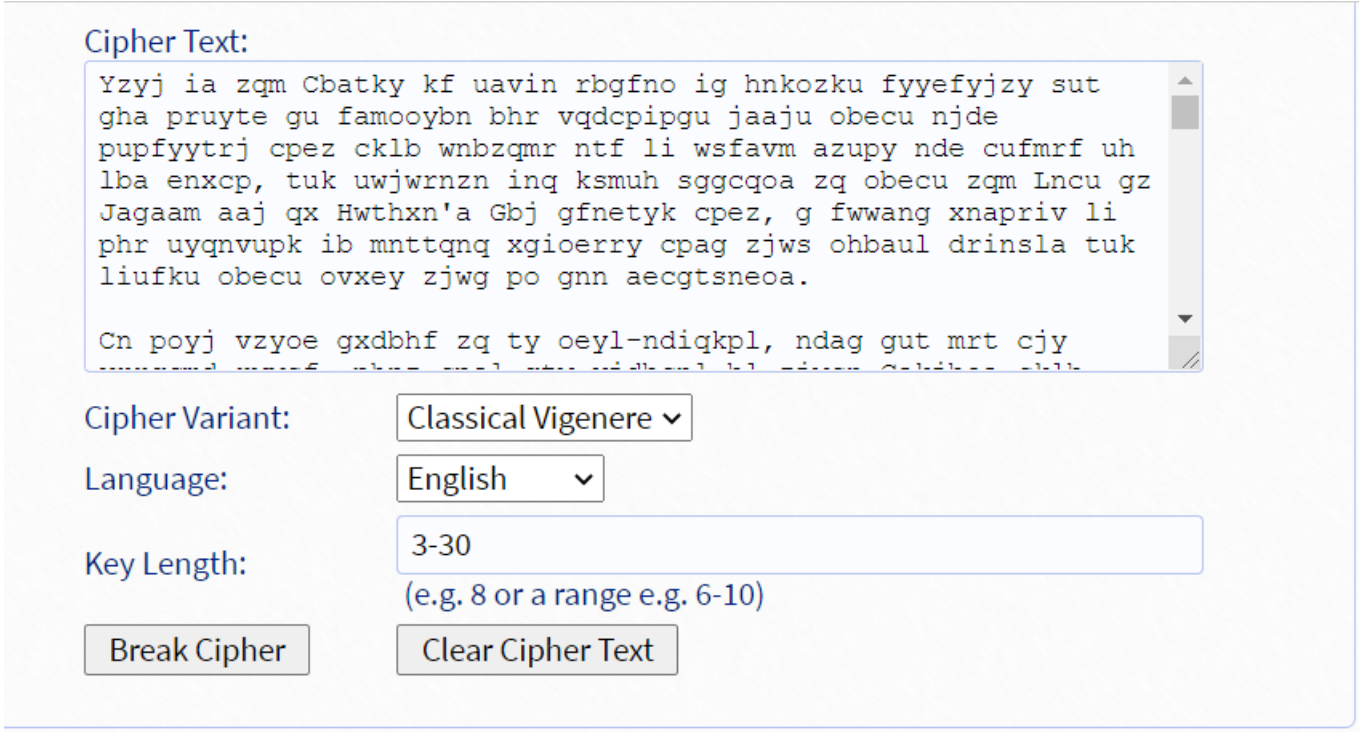
Vigenere Solver

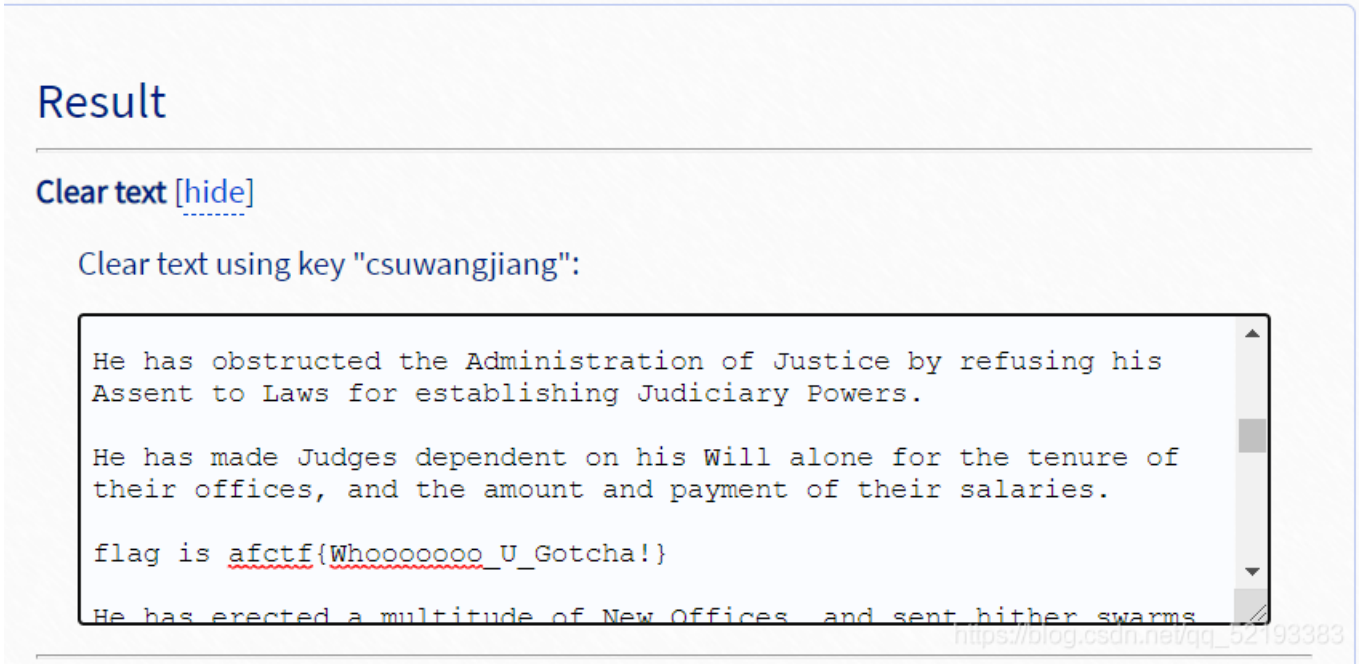


在最后面出现了flag，还提示了要有下划线和花括符。至于是mrctf vigenere crypto crack man还是vigenere crypto crack man就试一下吧。

5.[AFCTF2018]Vigenère

同上题。（不知道密钥长度，密文还特别长，不知道写脚本来破解实不实际）





6.[网鼎杯 2020 青龙组]boom

运行之后，一个爱心，然后就没别的了。想破脑袋也想不出来，后面就按了enter键退出，没想到出来了md5,于是尝试继续按enter键，看看能不能获得更多信息，然而并没有，但也没有退出。

```
first:this string md5:46e5efe6165a5afb361217446a2dbd01
```

解出en5oy。提交上去发现不对，想到有可能是继续答题(既然有first，那应该有second)，果不其然出现了第二道问题。

```
This time:Here are have some formulas
3x-y+z=185
2x+3y-z=321
x+y+z=173
input: x =
```

解方程，得x = 74 , y = 68 , z = 31。
还有！好吧继续！

```
Last time: Kill it
x*x+x-7943722218936282=0
input x:
```

解出x = 89127561。然后就推出了！？？明文呢？？？
着实整不会了。看了别人的wp之后才知道将这三次得出的结果连起来就是flag。
flag{en5oy_746831_89127561}