BUUCTF_Crypto题目：rot

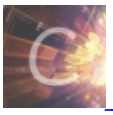
原创

好想变强啊 已于 2022-03-18 09:40:19 修改 1219 收藏

分类专栏： BUUCTF刷题记录 文章标签： python 网络安全

于 2022-03-17 18:49:10 首次发布

本文链接：https://blog.csdn.net/qq_38798840/article/details/123556380



BUUCTF刷题Crypto篇

文章目录

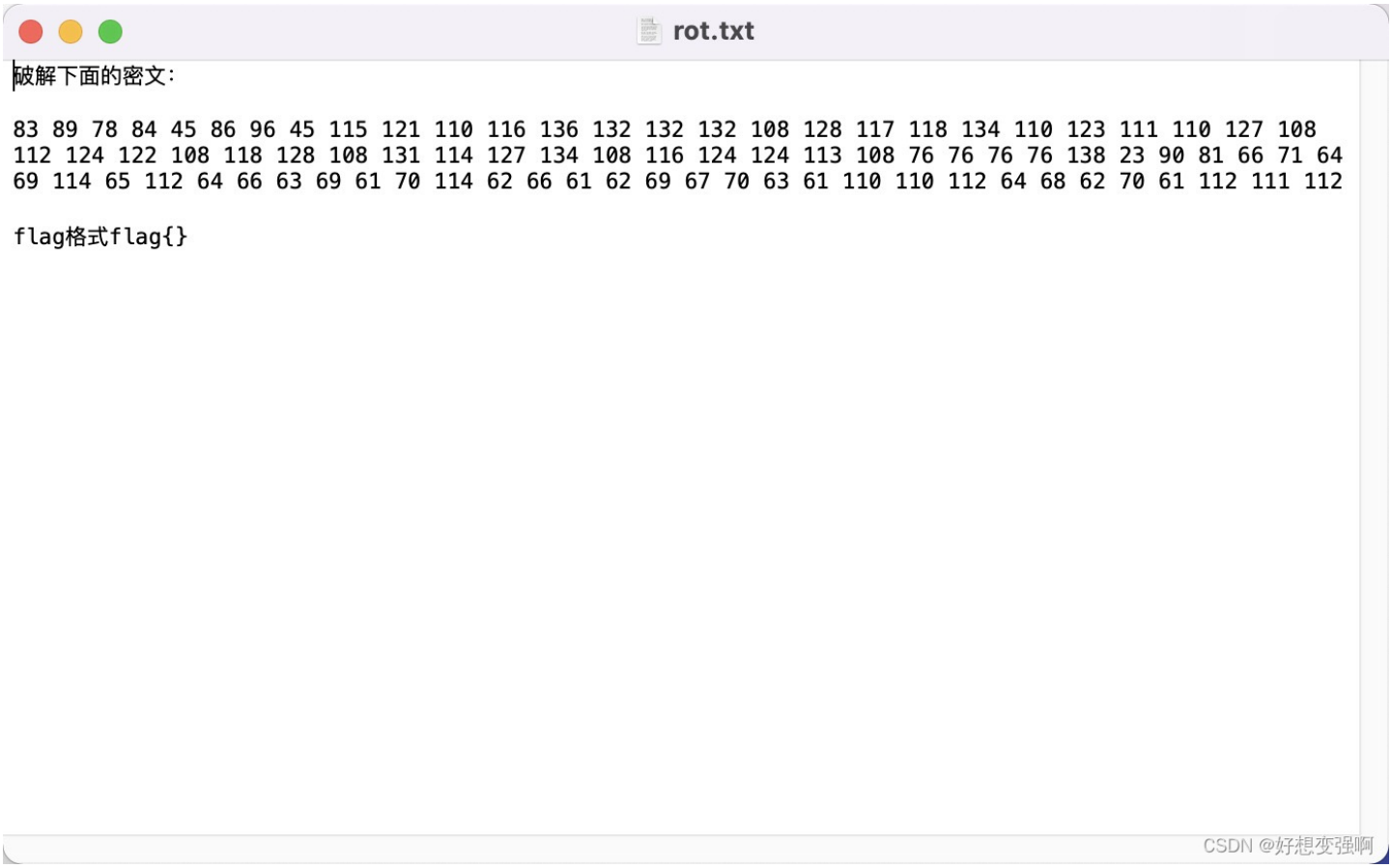
前言

从今天起记录一下自己做过的印象比较深刻的题目吧！

本题来自BUUCTF，Crypto部分，题目在第2页，叫rot

一、原题

下载题目文件打开后内容如图：



二、解题步骤

1.求解移位之前的字符串

根据题目名称叫“rot”，可以初步判断给出的数字可能是十进制ascii码，然后还要经过移动一定的位数来得出明文。先写Python脚本来处理一下这串数字，然后借助循环遍历不同的移位位数。

> 代码如下：

```
c='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 1
22 108 118 128 108 131 114 127 134 108 116 124 124 113 108 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'
l=c.split(' ')    #去掉空格放入list中方便转字符，要注意split之后产生的list中每个元素都是str
s=''
for i in range(len(l)):    #逐个先转int，再转字符后又组成字符串
    s+=chr(int(l[i]))
for i in range(1,14):    #这里是因为我后来已经知道是rot13，所以这里就只循环到13方便看一下结果
    for j in range(len(s)):
         print(chr(ord(s[j])-i),end='')
    print()
```

当然啦，先移位再转换成字符输出，步骤更少更简洁：

```
'''先移位再转换成ascii字符步骤更简单'''
for i in range(1,14):
    s=''
    for j in range(len(l)):
        s+=chr(int(l[j])-i)
    print(s)
```

输出的结果中合理的是：
FLAG IS flag{www_shiyanbar_com_is_very_good_???}
MD5:38e4c352809e150186920aac37190cbc

发现有未知的部分，并已知了md5的结果，看来还需进一步求解才能拿到flag。

2.暴力破解找出做md5之前的明文

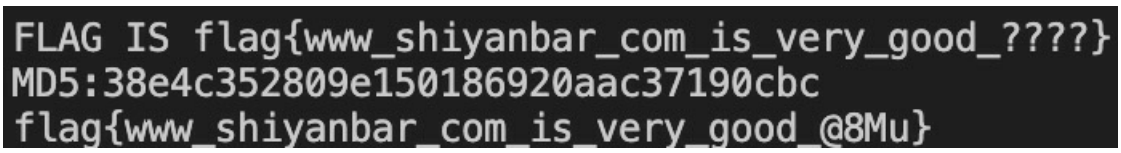
四层循环遍历ascii码在33-126范围的可见字符，拼接字符串，借助Python中已有的函数（注意要记得import hashlib）计算md5值，找出与上一步得到的MD5相等的结果，最终输出的运行结果为:
flag{www_shiyanbar_com_is_very_good_@8Mu}

备注：
这个脚本在我的电脑上大概运行30多秒之后出结果，得到结果（找到@、8、M、u）前一共会执行25955553次，也就是(64-33)*94**3+(56-33)*94**2+(77-33)*94+(117-33+1)，是不是很清晰呢？
**是代表乘方运算，同Python中的写法
代码如下：

```
import hashlib
s='flag{www_shiyanbar_com_is_very_good_'
m='38e4c352809e150186920aac37190cbc'

def revmd5():
    #count=0
    for i in range(33,127):
        for j in range(33,127):
            for k in range(33,127):
                for n in range(33,127):
                    #count+=1
                    #print(count)
                    a=s+chr(i)+chr(j)+chr(k)+chr(n)+'}'
                    #print(a)
                    ha=hashlib.md5(a.encode()).hexdigest()
                    if(ha == m):
                        print(a)
                        return
revmd5()
```

留个运行结果图的纪念~



总结

以上就是今天要记录的全部内容了~