bugku Crypto write up

原创

0verWatch 于 2018-02-12 17:13:03 发布 1913 收藏 2

文章标签： CTF bugku Crypto

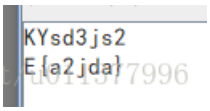
本文链接：https://blog.csdn.net/u011377996/article/details/79317665

0x01 滴答~滴

一看就知道是摩斯密码，直接摩斯解密，获得密码

0x02 聪明的小羊

根据提示应该是栅栏加密而且是2栏，遂尝试栅栏解密，竖着看就是key



0x03 ok

解密网址:http://tool.bugku.com/brainfuck/

全都是Ook就尝试Ook解密，得出flag，如图

0x04 这不是摩斯密码

解密网址:http://tool.bugku.com/brainfuck/

brainfuck解码就得到flag

0x05 简单加密

凯撒解密后发现有一段Base64，然后再来一波base64解码得到flag

```
_0T3cxW2LxOxKB?uLhSuKRaxKhKuXRPfLRfjXRC/K0K0MES2dO;;
`1U4dyX3MyPyLC@vMiTvLSbyLiLvYSQgMSgkYSD0L1L1NFT3eP<<
a2V5ezY4NzQzMDAwNjUwMTczMjMwZTRhNThlZTE1M2M2OGU4fQ==
b3W6f{Z5O{R{NEBxOkVxNUd{NkNx[USiOUim[UF2N3N3PHV5qR>>
```


0x06 一段Base64

把文件下载下来后，第一次base64之后发现是8进制转义序列，直接复制下来利用python中print函数的默认属性打印一波，得到一个16进制转义序列，再用一次print，下面是我解题时的代码

```
#encoding:utf-8
import base64
f = open('C:/Users/Vinson Chan/Desktop/bs.txt','r')
str=f.read()

f.close()


#print base64.b64decode(str)


str = [38,35,120,50,54,59,38,35,120,50,51,59,38,35,120,51,49,59,38,35,120,51,48,59,38,35,120,51,50,59,3
str2 = ''
for i in str:
    str2 = str2+chr(i)

#print str2



#下面步骤是是百度的
from HTMLParser import HTMLParser
h = HTMLParser()
s = h.unescape(h.unescape(str2))


print s
```

得到一个Unicode编码，放在站长工具跑一下，得到一串ASCII码，再来转义一下，发现是html编码，解码之后发现还有URL编码，放在站长工具上跑一下就行

其实网上还有一中简单的方法，用一个叫converter的工具,方法自己找

0x07 .!?

另类的Ook编码
直接去网站解码即可

0x08 +[]-

另类的brainfuck编码，直接去网站解码即可

0x09 奇怪的密码

给的提示不知道是啥，只能一个个试一下，又毫无头绪，再看看题目，发现那一段密文特别像flag，于是对比gndk与flag的ASCII码，突然发现是依次减少的
于是分别用C还有python写个脚本解密，得到flag,代码如下：

C语言的

```
#include <iostream>
#include <cstring>
using namespace std;
char a[]="gndk€rlqhmtkwwp}z";
int main()
{
    for (int i = 0; i<strlen(a);i++)
    {
        a[i]=a[i]-(i+1);
    }
    cout<<a<<endl;
    return 0;

 }
```

python的

```
#encoding:utf-8

str1 = 'gndk€rlqhmtkwwp}z'
#print str1
flag = ''
count = 1
for i in str1:
 flag = flag+chr((ord(i)-count))
 count=count+1
print flag
```

0x10 托马斯.杰斐逊

这是个杰斐逊密码盘，根据第一个密钥跟密文，把第二行单独取出来，然后从的地方开始，放到内容最前面
例如`: <KPBELNACZDTRXMJQOYHGVSFUWI < --> <HGVSFUWIKPBELNACZDTRXMJQOY <`
最后得到下面的密文

```
HGVSFUWIKPBELNACZDTRXMJQOY
CPMNZQWXYIHFRLABEUOTSGJVDK
BVIQHKYPNTCRMOSFEZWAXJGDLU
TEQGYXPLOCKBDMAIZVRNSJUWFH
SLOQXVETAMKGHIWPNYCJBFZDRU
XQYIZMJWAORPLNDVHGFCUKTEBS
WATDSRFHENYVUBMCOIKZGJXPLQ
CEONJQGWTHSPYBXIZULVKMRAFD
RJLXKISEFAPMYGHBQNOZUTWDCV
QWXPHKZGJTDSENYVUBMLAOIRFC
GOIKFHENYVUWABMCXPLTDSRJQZ
LTDENQWAOXPYVUIKZGJBMCSRFH
ENYSRUBMCQWVJXPLTDAOIKFZGH
SWAYXPLVUBOIKZGJRFHENMCQTD
```

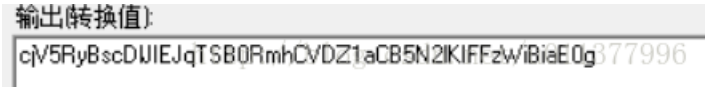
然后一列列去尝试，倒数第六列是flag
最后提交的flag是小写

0x11 伪加密

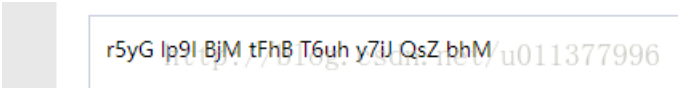
上次的博客内容就介绍过，不多说，把09改为00即可

0x12 告诉你个秘密

发现没有超过F的字母，边猜测是16进制，然后16进制转码，发现一串全都是数字跟字母的字符串，应该是Base64



解码后发现几组英文。。。。



发现跟上次校赛的键盘题格式差不多，猜测应是键盘密码，这题格式试了好久，都快想说MMP了，google之后才知道这题格式是flag:xxxxxxx(全是大写)
坑惨了!!

0x13 来自宇宙的信号

百度银河字母，对照着下图就能找到flag