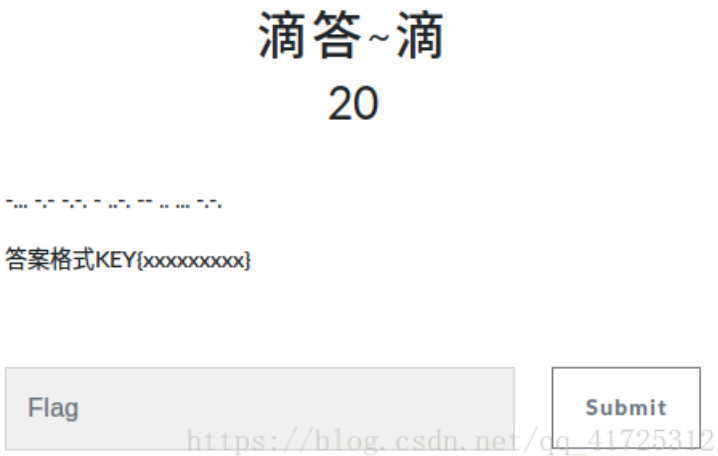
BugkuCTF Crypto wirte up

原创

西西囧 于 2018-07-18 14:39:31 发布 1106 收藏 2
分类专栏： write up Crypto 文章标签： CTF Crypto write up

本文链接：https://blog.csdn.net/qq_41725312/article/details/81088571

1.滴答~滴



(1)思路:很简单,一眼看出是**摩斯密码**,直接用工具解码得到flag

> 解密工具:CTFCrakTools

2.聪明的小羊

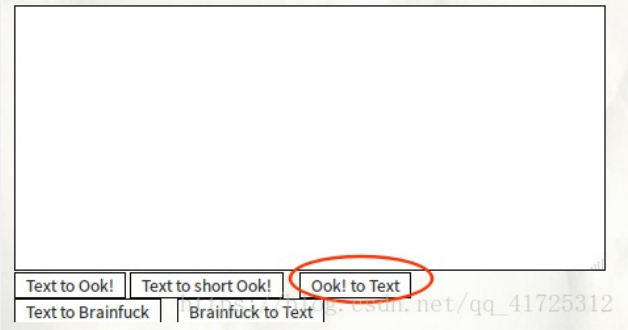
(1)思路:提示当中看到栅栏就想起**栅栏密码**,2个栅栏解密,得到flag

> 解密地址:http://tool.bugku.com/jiemi/

3.ok

(1)思路:直接用**Ook**解密,得到flag

> 解密地址:https://www.splitbrain.org/services/ook



4.这不是摩斯密码

这不是摩斯密码

30

下载看看吧

1.txt

Flag

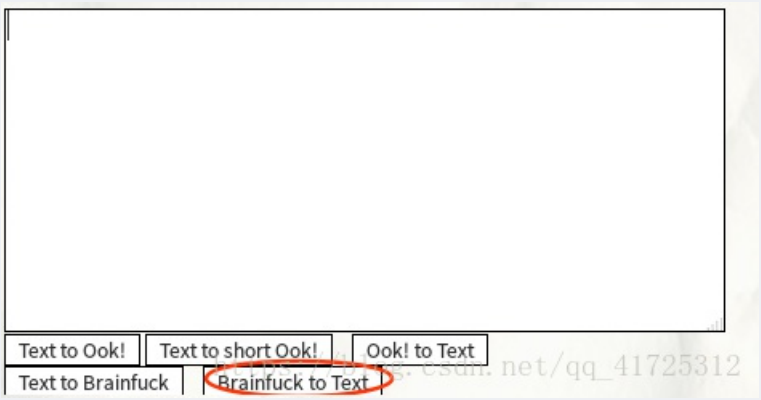
Submit

(1)思路:下载下来查看,确实不是摩斯密码,是一种叫**Brainfuck**的语言,解密出来就是flag

```
+++++ +++++ [->++ +++++ +++<] >++.+ +++++ .<+++ [->-- -<]>- -.+++ +++.<
++++[ ->+++ +<]>+ +++.< +++[- >---< ]>--- .---- .<+++ ++++[ ->--- ----<
]>--- ----- ----- .<+++ ++++[ ->+++ ++++< ]>+++ ++.<+ +++++ +[->- -----
-<]>. <++++ ++++[ ->+++ +++++ <]>++ .<+++ [->-- -<]>- ----. <++++ +++[-
>---- ---<] >---- ----. +++++ +..++ +++.+ .<+++ [->-- -<]>- --.<+ +++++
+[->+ +++++ +<]>+ ++.++ +.+++ +++++ +.--- -.+++ ++.<+ ++[-> +++<] >++++
++.<
```


Brainfuck是一种极小化的计算机语言，按照”Turing complete（完整图灵机）”思想设计的语言，它的主要设计思路是：用最小的概念实现一种“简单”的语言，BrainF**k 语言只有八种符号，所有的操作都由这八种符号(> < + - . , [ ])的组合来完成。

解密地址:https://www.splitbrain.org/services/ook



5.简单加密

(1)思路:看到后面的字符串最后面的AA想到的是**凯撒秘密**和**base64**的混合加密.对照ASCII,的ASCII是65，=的ASCII是61，偏移了四位(base64一般以'=='结束),再用base64解码得到flag
(2)脚本:python脚本将所有的字符都偏移四位

```
def main():
    string = 'e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XVlRXlp^XI5Q6Q6SKY8jUAA'
    list = [chr(ord(i)-4) for i in string]
    print(''.join(list))

if __name__ == '__main__':
    main()
```

打印出来为:

a2V5ezY4NzQzMDAwNjUwMTczMjMwZTRhNThlZTE1M2M2OGU4fQ==

> 解密工具:CTFCrakTools

6.一段Base64

(1)思路:打开是一段特别长的base64编码,base64解码,是8进制转义序列,

```
\134\170\65\143\134\170\67\65\134\170\63\60\1
```

再转是16进制转义序列,

```
\x5c\x75\x30\x30\x35\x33\x5c\x75\x30\x30\x37\
```

又转,出来为Unicode编码

```
\u0053\u0074\u0072\u0069\u006e\u0067\u002e\u0066\u0072\u006f\u006d\u0043\u
```

解码出ASCII码,转义出的是html编码

```
&#10;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#
2;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#
#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#
&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#32;&#
2;&#32;&#32;&#10;&#10;&#51;&#56;&#44;&#51;&#53;&#44;&#49;&#50;&
#48;&#44;&#53;&#48;&#44;&#53;&#52;&#44;&#53;&#57;&#44;&#51;&#5
&#44;&#51;&#53;&#44;&#49;&#50;&#48;&#44;&#53;&#48;&#44;&#53;&#
9;&#44;&#53;&#57;&#44;&#51;&#56;&#44;&#51;&#53;&#44;&#49;&#50;&
```

解码

```
&#102;&#108;&#97;&#103;&#37;&#55;&#66;&#99;&#116;&#102;&#95;&#
116;&#102;&#99;&#50;&#48;&#49;&#55;&#49;&#55;&#113;&#119;&#101;
&#37;&#55;&#68;
```

然后Unicode解码

为url编码,最后解出flag

(2)脚本:一直解到16进制的Python3脚本

```
import base64
import re

def main ():
    cipher_1 = '**' #为base64编码,太长省略
    plain_1 = base64.b64decode(cipher_1).decode('utf-8')
    # cipher = cipher.split('\\')[1:]

    cipher_2 = re.findall(r'\d+',plain_1)
    plain_2 = ''
    for i in cipher_2:
        plain_2 += chr(int(i,8))

    cipher_3 = re.findall(r'\d[0-9]|\d[a-z]',plain_2)
    plain_3 = ''
    for i in cipher_3:
        plain_3 += chr(int(i,16))

    print(plain_3)
if __name__ == '__main__':
    main()
```

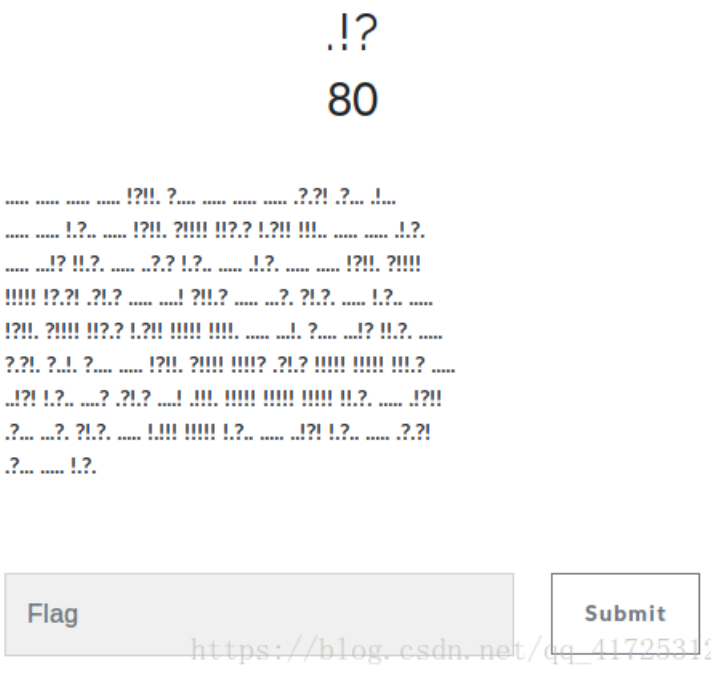
(3)总结:要多熟悉常见的编码,看到就能认出来.

还有一种简单的方法,用coverter的工具

https://blog.csdn.net/pdsu161530247/article/details/74640746

> 解密网站:http://tool.chinaz.com/tools/unicode.aspx
>
> 解密工具:coverter

7..!?



另类的Ook编码

直接解出flag

> 解密地址:https://www.splitbrain.org/services/ook

8.+[]-

(1)思路:很眼熟,就是上面的brainfuck编码,直接解出flag

9.奇怪密码

(1)思路:格式有点像flag的格式,对照ASCII表发现规律,gndk与flag的相差依次增多,直接写个脚本打印出类似flag的值

flagPtslei_ci_jiami

发现不对,Pts不知道怎么回事,试着改成flag{lei_ci_jiami},成功

(2)脚本:

```
def main():
    string = 'gndk€rlqhmtkwwp}z'
    count = 0
    result = ''
    for i in string:
        count += 1
        result = result + chr(ord(i)- count)
    print(result)
```

10.托马斯.杰斐逊

(1)思路: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，然后从密钥与密文一样的地方开始的部分，放到内容最前面
例如:

<KPBELNACZDTRXMJQOYHGVSFUWI < 密钥对应为:H

<HGVSFUWIKPBELNACZDTRXMJQOY <
最后得到下面的密文

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

明文为是按列来读取的

然后一列列去尝试，倒数第六列是flag

最后提交的flag是小写

11.zip伪加密

(1)思路:标题很明确,只要知道可以直接就解了

> 关于zip伪加密:https://blog.csdn.net/qq_41725312/article/details/81069184

12.告诉你个秘密

(1)思路:仔细观察发现字母都没超过F,猜测为16进制

解出来发现,应该为base54编码

cjV5RyBscDlJlEJqTSB0RmhCVDZ1aCB5N2lKlFFzWiBiaE0g

解出来几组字母与数字组合

r5yG lp9l BjM tFhBT6uh y7iJ QsZ bhM

是键盘密码,一组中对应的键盘位置回围绕一个键

比如 r5yg t就被围在他们中间

解出flag

> 解密网站:http://www.ab126.com/goju/1711.html

13.来自宇宙的信号

(1)思路:搜索'银河战队密码',没搜到什么,再试'银河密码',发现了对应的图

直接对应解出flag