Bugku旧平台crypto writeup

原创

a370793934 于 2019-11-27 17:06:31 发布 365 收藏
分类专栏： WriteUp 文章标签： Bugku crypto writeup ctf

滴答~滴

摩尔斯电码加密

KEY{BKCTFMISC}

聪明的小羊

栅栏密码 2栏

KEY{sad23jjdsa2}

Ok

http://127.0.0.1/ook-master/

ook加密

flag{ok-ctf-1234-admin}

这不是摩斯密码

http://127.0.0.1/ook-master/

brainfuck加密

flag{ok-c2tf-3389-admin}

easy_crypto

摩尔斯加密0代表.1代表-

flag{m0rse_code_1s_interest1n9!}

简单加密

e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XVlRXlp^Xl5Q6Q6SKY8jUAA

解：看到这一串字符，后面有AA猜测是凯撒密码（注意：这里的凯撒加密为变形凯撒加密，包含符号）和base64的混合加密。首先参照ASCII表，A的ASCII是65，=的ASCII是61，偏移了四位，所以写一个python脚本将所有的字符都偏移四位

脚本如下：

```
# -*- coding:utf8 -*-

from __future__ import print_function

def caesar(text):

    for i in range(len(text)):

        print("{}".format(chr(ord(text[i])-4)), end='')


caesar('e6Z9i~]8R~U~QHE{RnY{QXg~QnQ{^XVlRXlp^Xl5Q6Q6SKY8jUAA')
```

得到的base64字符串：

a2V5ezY4NzQzMDAwNjUwMTczMjMwZTRhNThlZTE1M2M2OGU4fQ==

进行base64解密 ：

key{68743000650173230e4a58ee153c68e8}

散乱的密文

置换密码，用密码机器解密

flag{52048c453d794df1}

凯撒部长的奖励

凯撒密码，用密码机器解密

SYC{here_Is_yOur_rEwArd_enjOy_It_Caesar_or_call_him_vIctOr_is_a_Excellent_man_if_you_want_to_get_hi

一段Base64

用Converter工具解码，先Base64解码再Unescape一下再16进制ASCII解码(hex to text)一下再Unescape一下复制括号里面的参数，再10进制ASCII解码(dec to text)一下再Html解码一下再Html解码一下就出来了

flag{ctf_tfc201717qwe}

.!?

http://127.0.0.1/ook-master/

ook加密

flag{bugku_jiami}

+[]-

http://127.0.0.1/ook-master/

brainfuck加密

flag{bugku_jiami_23}

奇怪的密码

变异得凯撒密码，python脚本：

```
a = 'gndk{rlqhmtkwwp}z'
i = 0
flag = ''
while i < len(a):
    num = ord(a[i])-(i+1)
    flag+=chr(num)
    i+=1
print(flag)
```

flag{lei_ci_jiami}

托马斯.杰斐逊

这个转盘加密，比如第一个密钥匙：2、密文匙：H

把转盘第二行单独提出来　2： <KPBELNACZDTRXMJQOYHGVSFUWI <

从H的地方一直剪切，把剪切的内容放在最前面，变成　2： <HGVSFUWIKPBELNACZDTRXMJQOY <

依次类推把14行都按这样的方式整一遍就得到这个：

2： <HGVSFUWIKPBELNACZDTRXMJQOY <

5： <CPMNZQWXYIHFRLABEUOTSGJVDK <

1： <BVIQHKYPNTCRMOSFEZWAXJGDLU <

3： <TEQGYXPLOCKBDMAIZVRNSJUWFH <

6： <SLOQXVETAMKGHIWPNYCJBFZDRU <

4： <XQYIZMJWAORPLNDVHGFCUKTEBS <

9： <WATDSRFHENYVUBMCOIKZGJXPLQ <

7： <CEONJQGWTHSPYBXIZULVKMRAFD <

8： <RJLXKISEFAPMYGHBQNOZUTWDCV <

14：<QWXPHKZGJTDSENYVUBMLAOIRFC <

10：<GOIKFHENYVUWABMCXPLTDSRJQZ <

13：<LTDENQWAOXPYVUIKZGJBMCSRFH <

11：<ENYSRUBMCQWVJXPLTDAOIKFZGH <

12：<SWAYXPLVUBOIKZGJRFHENMCQTD <

flag在倒数第六列。

flag{XSXSBUGKUADMIN}

不对可能是大小写问题，改成小写

flag{xsxsbugkuadmin}

zip伪加密

第二个14 00 后的09奇数是加密偶数是不加密，改成00，解压得到

flag{Adm1N-B2G-kU-SZIP}

告诉你个秘密(ISCCCTF)

636A56355279427363446C4A49454A7154534230526D6843

56445A31614342354E326C4B4946467A5769426961453067

推测是16进制转字符串：

cjV5RyBscDlJlEJqTSB0RmhCVDZ1aCB5N2lKlFFzWiBiaE0g

有大写有小写还有数字 推测是base64：

r5yG lp9l BjM tFhB T6uh y7iJ QsZ bhM

本来以为这就是flag

提交不对后来联想到之前做过的题

应该是对应键盘上的键位

tongyuan

提交不对.....改成 flag{tongyuan}也不对.....

flag改成大写

TONGYUAN

这不是md5

666c61677b6165373335383762613536626165663 57d

十六进制转字符串

flag{ae73587ba56baef5}

贝斯家族

base91加密

flag{554a5058c9021c76}

富强民主

社会主义核心价值观加密解密

Pip install cve

echo "公正公正公正诚信文明公正民主公正法治法治友善平等和谐敬业和谐 富强和谐富强和谐文明和谐平等公正公正和谐法治公正公正公正文明和谐民主和谐敬业和谐平等和谐敬业和谐敬业和谐和谐和谐公正法治友善法治"|cve -d

flag{90025f7fb1959936}

python(N1CTF)

python逆向解密：

```
import base64,string,N1ES

key = "wxy191iss00000000000cute"

c = base64.b64decode("HRlgC2ReHW1/WRk2DikfNBo1dl1XZBJrRR9qECMNOjNHDktBJSxcl1hZlz07YjVx")

n1es = N1ES.N1ES(key)

f=""

for i in xrange(3):

    for j in xrange(16):

        for k in string.printable:

            s="x"*i*16+"x"*j+k+"x"*(48-i*16-j-1)

            e=n1es.encrypt(s)
```

```
        check=c[i*16+j+8]==e[i*16+j+8] if j<8 else c[i*16+j-8]==e[i*16+j-8]
        if check:
            f+=k
            break
print f
```

N1CTF{F3istel_n3tw0rk_c4n_b3_ea5i1y_s0lv3d_/--/}

进制转换

python2脚本

```
#-*-coding:utf-8-*-
s = ["d87","x65","x6c","x63","o157","d109","o145","b100000","d116","b1101111","o40","x6b","b1100101","b1101100"
flag = ""
for item in s:
s1 = str(item)
if(item[0:1]=="d"):
flag += chr(int(item[1:]))
if(item[0:1]=="x"):
flag += chr(int(item[1:],16))
if(item[0:1]=="o"):
flag += chr(int(item[1:],8))
if(item[0:1]=="b"):
flag += chr(int(item[1:],2))
print(flag)
```

Welcome to kelaibei. Give you a flag as a gift. flag{1e4bf81a6394de5abc005ac6e39a387b} . Have a good time~

flag{1e4bf81a6394de5abc005ac6e39a387b}

Affine

仿射密码（单码加密法的另一种形式称为仿射加密法（affine cipher））

```
#-*-coding:utf-8-*-
i=1
while(17*i%26!=1):
i+=1 #求出17的乘法逆元
x='szzyfimhyzd'
for i in range(len(x)):
print chr(23*(ord(x[i])-ord('a')+8)%26+ord('a')),
```

flag{affineshift}

Crack it

linux密码文件，拿到kali下破解，命令：

john shadow

解出hellokitty

flag{hellokitty}

Rsa

python RsaCtfTool.py --createpub -n 11111 -e 222222

python RsaCtfTool.py --publickey 1.pem --private >1.key

python RsaCtfTool.py --key 1.key --dumpkey

python脚本

```
#coding:utf-8
#已知pqe直接解密密文
import base64
def gcd(a, b):  #求最大公约数
if a < b:
    a, b = b, a
while b != 0:
    temp = a % b
```

```
    a = b
    b = temp
return a

def egcd(a, b):
if a == 0:
    return (b, 0, 1)
else:
    g, y, x = egcd(b % a, a)
    return (g, x - (b // a) * y, y)

def modinv(a, m):
g, x, y = egcd(a, m)
if g != 1:
    raise Exception('modular inverse does not exist')
else:
    return x % m

if __name__ == "__main__":

p=159918469709932133220726269015607499326863257664034048640233418107353192490663709160900

q=288057917712602594868569027290204386866703544412962471482078628360646578497353436182070

e =
3546111024413075720565721818279258991983453502287537309310893932754639165444566268942454

# tmp =
base64.b64decode("qzogS7X8M3ZOpkUhJJcbukaRduLyqHAPblmabaYSm9iatuulrHcEpBmiI7V40N7gbsQXwY

d = modinv(e, (p - 1) * (q - 1))
# c=s2n(tmp)
c =
3823099131622939965182356759069230106004462041219173776463238468054625622845151823884296
```

```
# c =
22503148344463405693106790786585379965019722535137705063229033472107303128770173029781580
n = p*q
m=pow(c,d,n)


sss = hex(int(m)) #转换为16进制
#16进制转字符串
flag = ""
for i in range(2,len(sss)-1,2):
flag += chr(int(sss[i:i+2],16))
print(flag)
```

flag{Wien3r_4tt@ck_1s_3AsY}

来自宇宙的信号

标准银河字母（Standard Galactic Alphabet）出自游戏《指挥官基恩》系列。是系列中使用的书写系统。

对照标准银河字母：https://baike.baidu.com/item/标准银河字母/2691355#1

得到flag：

flag{nopqrst}