[Bugku][Crypto][CTF][2020]Crypto 1-20 write up

原创

CryptWinter 于 2020-12-27 22:33:55 发布 405 收藏 1

分类专栏： CTF 文章标签： CTF Crypto Bugku 2020 write up

工具：CaptEncoder
https://www.freebuf.com/sectool/188397.html
Convert:https://pan.baidu.com/s/17YPXfvBHl_HyA00AffTBvg 密码：skqw
推荐网站：http://ctf.ssleye.com/

Crypto 1
关键字： 莫斯 /.-
步骤：莫斯解码得：FLAG%u7bD3FCBF17F9399504%u7d，%u7b web解码得{，%u7d web解码得}。中间的大写转换为小写，组合起来就是flag。
莫斯转码：https://www.atool99.com/morse.php

Crypto 2
关键字： 栅栏密码 两个一组
步骤：在线栅栏 直接解密

Crypto 3
关键字： Ook.
步骤： ook解码，https://www.splitbrain.org/services/ook在线工具，直接ook！to text

Crypto 4
关键字： [±<>] brainfuck
知识点： brainfuck语言用> < + - . , [ ]八种符号来替换C语言的各种语法和命令
步骤：https://www.splitbrain.org/services/ook，然后Brainfuck to Text

Crypto 5
关键字： 莫斯密码
知识点：
步骤：查表一一对应 或者在线 http://ctf.ssleye.com/morse.html
https://blog.csdn.net/qq_42777804/article/details/90742966

Crypto 6
关键字：base64
步骤：AA和==相似 A超出base64范围
移4位后 base64解码

```
import base64
#'miwen.txt'
miwen = open('miwen.txt').readline()
res = '' # 存储结果
for i,enu in enumerate(miwen):
    res += chr(ord(enu)-4)
print('ascii码偏移后结果：'+res)
res = base64.b64decode(res).decode()
print('base64解码后结果：'+res)
```

Crypto 7
关键字： 移位密码
步骤：按照 2 1 6 5 3 4移位

```
# 此脚本用来根据顺序调整密文以得到明文
miwen = open('miwen.txt').readline()
tem = '' # 临时存储
resList = [] # 结果数组
res = '' # 最终结果
for i,enu in enumerate(miwen): # 先把密文每六个一组分好
    tem += enu
    if len(tem)==6 or i == len(miwen) - 1:
        resList.append(tem)
        tem = ''
for i in range(len(resList)):
    res += resList[i][1]+resList[i][0]+resList[i][4]+resList[i][5]+resList[i][3]+resList[i][2]
print(res)
```

Crypto 9 一段base64 Hex to text
步骤：1.Base64解密 2.unescape 3.Hex to text .4.unescape
5.ascii码转字符 6.Decode HTML

https://blog.csdn.net/qq_40980391/article/details/79194128

Crypto 8 .!?
关键字： short ook编码
步骤：

Crypto 10
关键字：累次加密

步骤：看到这串字符…像常见的提交flag{xxx}格式…
先看一下ascii的编码吧，试一下是否和flag有关系~
gndk的10进制的ASCII码分别是：103 110 100 107
flag的10进制的ASCII码分别是 ：102 108 97 103
发现ASCII以此减少 1 2 3 4，所以以此类推后面会继续减少…

```
# 此脚本用于解决累次加密
miwen = open('miwen.txt').readline()
for j in range(10):
    for i,enu in enumerate(miwen):
        print(chr(ord(enu)-i-j),end = '')
    print()
```

Crypto11 托马斯.杰斐逊
步骤：写脚本进行移位
含有bugku的即为答案
https://www.cnblogs.com/0yst3r-2046/p/11810574.html

Crypto 12 告诉你个秘密
知识点： 键盘密码
步骤：1. hex后 base64
2.r5yG lp9I BjM tFhBT6uh y7iJ QsZ bhM 围着的字母大写
flag{TONGYUAN}

Crypto 13 不是md5
关键字： hex
666c61677b6165373335383762613536626165663 57d

Crypto 14 贝斯家族
关键字： base91
知识点： base91字符较多

步骤：http://www.atoolbox.net/Tool.php?Id=935
@iH<,{bdR2H;i6*Tm,Wx2izpx2!

Crypto 15 python(N1CTF)
知识点： Feistel加密 DES算法
步骤：https://www.cnblogs.com/0yst3r-2046/p/12123653.html

Crypto 16 进制转换
关键字：
步骤： b开头是二进制，o开头是八进制，d开头是十进制，x开头是十六进制。

```
# 此脚本针对不同进制字符，统一转换成十进制，再转成字符
miwen = open('text.txt').readline().split(' ')
res = ''
for i in range(len(miwen)):
    if miwen[i][0] == 'b':
        res += chr(int(miwen[i][1:],2))
    elif miwen[i][0] == 'd':
        res += chr(int(miwen[i][1:],10))
    elif miwen[i][0] == 'o':
        res += chr(int(miwen[i][1:],8))
    elif miwen[i][0] == 'x':
        res += chr(int(miwen[i][1:],16))
print(res)
```

Crypto 17 affine加密
关键字： 仿射加密
知识点： affine加密，仿射加密，其实也就是明文和密文之间有一个一次函数变化，y=kx+b，只不过为了让y能转换成对应的密文，要对kx+b取余。
步骤：
一般常用的字符集就是a-z，分别对应0-26。
并且，一次函数能用于做密码是因为他有个特性，就是每一个x对应唯一的y，所以为了保证取余之后也能保持这种特性，就要求k与字符集的大小（这里是26）互质。
两种方法，一种是用解密函数，一种是暴力破解，哪种都可以。

```
# 此脚本用于暴力破解仿射加密
# 加密函数：y=17x-8
# 密文： szzyfimhyzd
miwen = "szzyfimhyzd"

def baoLi(miwen): # 暴力解密
    miwen = miwen.lower() # 全部转换成小写
    res = ''
    for i,enu in enumerate(miwen): # 遍历每一个字母
        for j in range(26): # 遍历字母表
            if (17 * j - 8) % 26 == ord(enu) - 97: # 比对加密结果
                res += chr(j + 97)
                break # 成功直接跳出
    return res
#仿射密码解密
#改进欧几里得算法求线性方程的x与y
def get(a, b):
    if b == 0:
        return 1, 0
    else:
        k = a //b
        remainder = a % b
        x1, y1 = get(b, remainder)
        x, y =y1, x1 - k * y1
    return x, y
def jiemi(miwen): # 解密函数解密
    miwen = miwen.lower()
    res = ''
    k = 17
    b = -8
    #求a关于26的乘法逆元
    x, y = get(k, 26)
    a1 = x % 26
    for i, enu in enumerate(miwen):
        res += chr((a1 * (ord(enu)- 97 - b) % 26)+ 97)
    return res

print("暴力解密结果："+baoLi(miwen))
print("解密函数解密："+jiemi(miwen))
```

Crypto 18 Crack it
关键字： shadow join
步骤：https://blog.csdn.net/Onlyone_1314/article/details/89287327?utm_medium=distribute.pc_relevant.none-task-blog-OPENSEARCH-5.not_use_machine_learn_pai&depth_1-utm_source=distribute.pc_relevant.none-task-blog-OPENSEARCH-5.not_use_machine_learn_pai

Crypto 19 rsa
关键字： RSA
知识点：

步骤：
1.给出了N、e、密文，RsaCtfTool把N分解成大素数，求出p、q
2.知道p、q，求出d后，解密函数是M ＝C^D mod N
https://blog.csdn.net/shenzhang7331/article/details/84311280
最后一行修改 print(n2s(m))

Crypto 20 来自宇宙的信号
关键字： 银河字母

步骤：百度搜索银行字母 一一对应

总结

- 有两种符号组成，每几个一组，每组符号个数不一定相同的加密结果，考虑摩斯密码；
- 每组有五个字符，一共有三种类型的字符，可能是short ook加密，一般是.!?这三种字符；
- 每组有五个字符，一共有七种类型的字符，可能是brainfuck加密，一般是±[]<>.这七种字符；
- \123\123\123，类似的反斜杠加数字的组合，是escape加密结果；
- f7，类似的组合是encode HTML的结果；
- &#，类似的组合是encode HTML的结果；
- \u0053\u0074，类似的组合是escape加密结果；
- \u0053\u0074，类似的组合是escape加密结果；

参考博客：https://www.cnblogs.com/qiaowukong/p/13657062.html