【2020年第二届“网鼎杯”网络安全大赛 白虎组】 Crypto b64

转载

你们这样一点都不可耐 于 2020-08-03 21:27:05 发布 521 收藏

分类专栏： CTF 文章标签： 加密解密 python md5 爬虫 后端

原文链接：https://writeup.ctfhub.com/Challenge/2020/%E7%BD%91%E9%BC%8E%E6%9D%AF/%E7%99%BD%E8%99%8E%E7%BB%84/57c13864.html

> 张三看到了一个神秘的字符串，似乎是base64。该题可能有多解，请尝试多次提交，flag格式flag{UUID}

```
密文:uLdAuO8duojAFLEKjIgdpfGeZoELjJp9kSieuIsAjJ/LpSXDuCGduouz

泄露的密文:pTjMwJ9WiQHfvC+eFCFKTBpWQtmgjopgqtmPjfKfjSmdFLpeFf/Aj2ud3tN7u2+enC9+nLN8kgdWo29ZnCrOFCDdFCrOFoF=
泄露的明文:ashlkj!@sj1223%^&*Sd4564sd879s5d12f231a46qwjkd12J;DJjl;LjL;KJ8729128713
```

CTFHub提供的解题思路和脚本

```
换表base64，将给出对应关系记下来，发现flag密文中['E', 'G', 'I', 's', 'X', 'z']，这六个字符没有映射关系。

然后有['+', '/', '1', '5', '7', '6', '9', '8', 'A', 'C', 'H', 'K', 'J', 'P', 'R', 'V', 'e', 'f', 'n', 'u', 'w', 'v'] 这么多位字符也没有被映射。

所以爆破这两个列表中的映射关系

然后根据flag的格式，uuid，来判断结果。
```

```python
# -*- coding: utf-8-*-
from base64 import *
from string import *

def check(s):
    for i in s:
        if i not in "flag{-1234567890abcdef}":
            return False
    return True

flag = 'uLdAuO8duojAFLEKjIgdpfGeZoELjJp9kSieuIsAjJ/LpSXDuCGduouz'
a='pTjMwJ9WiQHfvC+eFCFKTBpWQtmgjopgqtmPjfKfjSmdFLpeFf/Aj2ud3tN7u2+enC9+nLN8kgdWo29ZnCrOFCDdFCrOFoF='
b='YXNobGtqIUBzajEyMjMlXiYqU2Q0NTY0c2Q4NzlzNWQxMmYyMzFhNDZxd2prZDEySjtESmpsO0xqTDtLSjg3MjkxMjg3MTM='
alpha = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789abcdefABCDEF+/'
FLAG=''

print("fail words")
for i in flag:
    if i in a:

        index = a.index(i)
        FLAG+=b[index]
    else:
        FLAG+='!'
        print i,
print "\nFLAG cipher"
print FLAG
#'ZmxhZ3sxZTNhMm!LN!0xYz!yLT!mNGYtOWIyZ!!hNGFmYW!kZj!xZTZ!'

print "alternative words"
aw=""
for i in alpha:
```

```
    if i not in b:
        aw += i
print aw

'@#$%^&'
table = 'ACHJKPRVefnuvw156789efAC+/'
print("for z")
for i in table:
    if b64decode("ZTZ"+i)[-1] == '}':
        FLAG = FLAG.replace("ZTZ!","ZTZ9")
        table = table.replace(i,"")
        #print FLAG

print("for G")
for i in table:
    if check(b64decode("Zj"+i+"x")) and check(b64decode("Yz"+i+"y")):
        #print b64decode("Zj"+i+"x")
        FLAG = FLAG.replace("Zj!x","Zj"+i+"x").replace("Yz!y","Yz"+i+"y")
        table = table.replace(i,"")
        #print i
        #print FLAG

print("for I and s")
for i in table:
    for j in table:
        if check(b64decode("N"+i+"0x")) and check(b64decode("Z"+i+j+"h")):
            #print b64decode("N"+i+"0x"),b64decode("Z"+i+j+"h")
            FLAG = FLAG.replace("N!0x","N"+i+"0x").replace("Z!!h","Z"+i+j+"h")
            table = table.replace(i,"").replace(j,"")
            #print i,j
            #print FLAG

print("for X and E")
for i in table:
    for j in table:
        if j == i:
            continue
        s = b64decode(FLAG.replace("Mm!l","Mm"+i+"l").replace("LT!m","LT"+i+"m").replace("YW!k","YW"+j+'k'))
        if check(s):
            print s
```

自己测试了一下

```
C:\Python27\python2.exe C:/Users/xxx/Desktop/4.py
fail words
E I G E I s X G z
FLAG cipher
ZmxhZ3sxZTNhMm!lN!0xYz!yLT!mNGYtOWIyZ!!hNGFmYW!kZj!xZTZ!
alternative words
ACHJKPRVefnuvw156789efAC+/
for z
for G
for I and s
for X and E
flag{1e3a2be4-1c02-2f4f-9b2d-a4afaddf01e6}
flag{1e3a2be4-1c02-2f4f-9b2d-a4afaedf01e6}
flag{1e3a2de4-1c02-4f4f-9b2d-a4afabdf01e6}
flag{1e3a2de4-1c02-4f4f-9b2d-a4afaedf01e6}
flag{1e3a2ee4-1c02-5f4f-9b2d-a4afabdf01e6}
flag{1e3a2ee4-1c02-5f4f-9b2d-a4afaddf01e6}

Process finished with exit code 0
```

作者：CTFHub

代码来源：

https://writeup.ctfhub.com/Challenge/2020/%E7%BD%91%E9%BC%8E%E6%9D%AF/%E7%99%BD%E8%99%8E%E7%BB%84/57c13864.html

以下是个人的注释

```
a=密文
uLdAuO8duojAFLEKjIgdpfGeZoELjJp9kSieuIsAjJ/LpSXDuCGduouz

b=泄露的密文
pTjMwJ9WiQHfvC+eFCFKTBpWQtmgjopgqtmPjfKfjSmdFLpeFf/Aj2ud3tN7u2+enC9+nLN8kgdWo29ZnCrOFCDdFCrOFoF=

c=泄露的明文base64加密
ashlkj!@sj1223%^&*Sd4564sd879s5d12f231a46qwjkd12J;DJjl;LjL;KJ8729128713的base64加密
也就是
YXNobGtqIUBzajEyMjMlXiYqU2Q0NTY0c2Q4NzlzNWQxMmYyMzFhNDZxd2prZDEySjtESmpsO0xqTDtLSjg3MjkxMjg3MTM=
```