crypto-writeup

原创

song-10 于 2019-07-19 22:56:04 发布 248 收藏
分类专栏： MOCTF 文章标签： moctf crypto

- 数据库密码

题目描述：

数据库密码经由md5加密后存储，md5字串长度为32个字符（128位），但题目中给的是35位仔细观察发现，字母Q、X、V并不是md5值所包含的字母，去除后刚好32个字符（128位），修改后的字串在网站上在线解密，得到flag：

- rot大法好

题目描述：

rot大法好

50

题目如下：}rQbpar_gbE{sgpbz

没有什么特殊的，直接rot13解密：

```
Python 3.7.0b1 (v3.7.0b1:9561d7f, Jan 31 2018, 07:26:34) [MSC v.1900 64 bit (AMD
64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
============== RESTART: D:\TOOLS\PythonScripts\crypto\rot13.py ==============
ciphertext:}rQbpar_gbE{sgpbz
}eDocne_toR{ftcom
```

解密后发现是逆序，倒过来就是flag：

```
>>> '}eDocne_toR{ftcom'[-1::-1]
'moctf{Rot_encoDe}'
>>>
```

- 奇怪的汉字

题目描述：

奇怪汉字

50

flag格式moctf{xxxxx}题目如下：2099年，年轻的江先生因为实在没钱
于是将自己的魔法棒带到当铺出售，但当铺老板却给了他一张纸，上面
这样写道：由口中 由由夫 由由口 由由口 由中由

明显的当铺密码（题目描述也有提示），在线解密：

本题汉字不是很多，数值也可以直接数出来，将得到的数转码即得到flag：

```
>>> list1=[102,117,110,110,121]
>>> for i in list1:
        print(chr(i),end='')


funny
```

- 就是这个feel

题目描述：

恰恰 恰恰恰 恰绑恰绑 恰 绑绑恰绑{恰恰绑 恰恰恰 恰恰恰 恰绑绑}

疑似摩斯电码，将恰转变为1（-），绑转变为0（.),尝试脚本解一下：

```
#!/usr/bin/python
# -*- coding: UTF-8 -*-
def decode(a):
    plain_text=''
    s = a.split(" ")
    dict = {
            '.-':'A','-...':'B','-.-.':'C','-..':'D','.':'E','..-.':'F','--.':'G','....':'H',
            '..':'I','.---':'J','-.-':'K','.-..':'L','--':'M','-.':'N','---':'O','.--.':'P',
            '--.-':'Q','.-.':'R','...':'S','-':'T','..-':'U','...-':'V','.--':'W','-..-':'X',
            '-.--':'Y','--..':'Z','.----':'1','..---':'2','...--':'3','....-':'4','.....':'5',
            '-....':'6','--...':'7','---..':'8','----.':'9','-----':'0','..--..':'?','-..-.':'/',
            '-.--.-':'()','-....-':'-','.-.-.-':'.'
            };
    for item in s:
        plain_text+=dict[item]
    return plain_text
str1='11 111 1010 1 0010 110 111 111 100'
cipher_text=''
for i in str1:
    try:
        if i==' ':
            cipher_text+=i
        else:
            if i=='1':
                cipher_text+='-'
            elif i=='0':
                cipher_text+="."
    except Exception as err:
        print(err)
print(decode(cipher_text).lower())
```

得到flag（加上{}）即可：

```
Python 3.7.0b1 (v3.7.0b1:9561d7f, Jan 31 2018, 07:26:34) [MSC v.1900 64 bit (AMD
64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
============== RESTART: D:\TOOLS\PythonScripts\crypto\Morse.py ==============
moctfgood
>>>
```

- 贝斯族谱

```
Vm0weGQxSXlSblJWV0d4WFlUSm9WRll3WkRSV01XeHlXa1pPYUZKc1NsWldSM1JQVmpGS2RHVkVRbFZXYkhCUVdWZHplRll4VG5OWGJGcFh
```

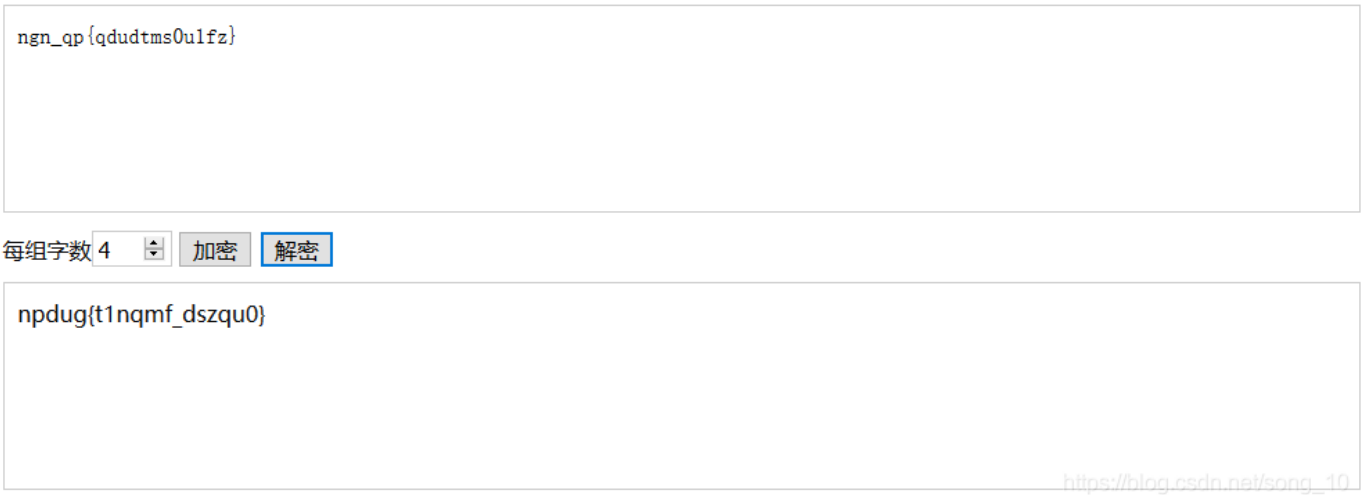
多次base64加密，解密即可：

```
import base64
flag='VjFjd2VHRXlVbGRhTTNCVFltMVNjMVJVUW1GamJIQkhXa1pPVGxJd2NGcFdSbWhyWVRGYVJsZHVVbUZXZWxJelZVWkZPVkJSUFQwP
while True:
    try:
        flag=base64.b64decode(flag)
    except Exception as err:
        print(flag)
        break
```

解密后得到的并不是最终的flag：

```
Python 3.7.0b1 (v3.7.0b1:9561d7f, Jan 31 2018, 07:26:34) [MSC v.1900 64 bit (AMD
64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
========== RESTART: C:\Users\Nop\Desktop\test.py ==========
b'ngn_qp{qdudtms0u1fz}'
>>>
```

像是栅栏密码，尝试解密：



得到形式于flag格式一致的字串，在移位解密，得到flag：

```
input_str=input('plaintext: ')
key=1
while key<27:
    str1=input_str
    flag=''
    for i in range(len(str1)):
        try:
            if not (65<=ord(str1[i])<=90 or 97<=ord(str1[i])<=122):
                flag+=str1[i]
            else:
                flag+=chr(97+(ord(str1[i])-97-key)%26)
        except Exception as err:
            print(err)
    key+=1
    print(key,flag)
```

```
Python 3.7.0b1 (v3.7.0b1:9561d7f, Jan 31 2018, 07:26:34) [MSC v.1900 64 bit (AMD
64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
========== RESTART: D:\TOOLS\PythonScripts\crypto\凯撒密码.py ==========
==
plaintextnpdug{tlnqmf_dszqu0}
2 moctf{slmple_crypt0}
3 lnbse{rllokd_bqxos0}
4 kmard{qlknjc_apwnr0}
5 jlzqc{pljmib_zovmq0}
6 ikypb{olilha_ynulp0}
7 hjxoa{nlhkgz_xmtko0}
8 giwnz{mlgjfy_wlsjn0}
9 fhvmy{llfiex_vkrim0}
10 egulx{klehdw_ujqhl0}
11 dftkw{jldgcv_tipgk0}
12 cesjv{ilcfbu_shofj0}
13 bdriu{hlbeat_rgnei0}
14 acqht{gladzs_qfmdh0}
15 zbpgs{flzcyr_pelcg0}
16 yaofr{elybxq_odkbf0}
17 xzneq{dlxawp_ncjae0}
18 wymdp{clwzvo_mbizd0}
19 vxlco{blvyun_lahyc0}
20 uwkbn{aluxtm_kzgxb0}
21 tvjam{zltwsl_jyfwa0}
22 suizl{ylsvrk_ixevz0}
23 rthyk{xlruqj_hwduy0}
24 qsgxj{wlqtpi_gvctx0}
25 prfwi{vlpsoh_fubsw0}
26 oqevh{ulorng_etarv0}
27 npdug{tlnqmf_dszqu0}
>>>
```


- 贝斯族谱升级版

```
R1pDRE1SUldHTTNUSU5SV0c1QkRNUkJUR0UzRElOUlVHWkJUTU5KVklZM0RHTlpTRzQ0VE9NQlhHUVpUQU4yRQ==
```

base64、32、16分别解密即可得到flag：

```
from base64 import *
flag='R1pDRE1SUldHTTNUSU5SV0c1QkRNUkJUR0UzRElOUlVHWkJUTU5KVklZM0RHTlpTRzQ0VE9NQlhHUVpUQU4yRQ=='
while True:
    try:
        flag=b64decode(flag)
    except Exception as err:
        print(err)
    try:
        flag=b32decode(flag)
    except Exception as err:
        print(err)
    try:
        flag=b16decode(flag)
    except Exception as err:
        break
print(flag)
```

```
Python 3.7.0b1 (v3.7.0b1:9561d7f, Jan 31 2018, 07:26:34) [MSC v.1900 64 bit (AMD
64)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
========== RESTART: C:\Users\Nop\Desktop\test1.py ==========
Incorrect padding
Incorrect padding
b'moctf{m1ddle_crypt0}'
```

- 卡哇伊

题目描述：

卡哇伊

50

你瞅我可爱吗?

拿到的文件是一堆字符（AAencode）：

```
ﾟωﾟ/= /｀ｍ´）/ ~┻━┻   //*´∇｀*/ ['_']; o=(ﾟｰﾟ)  =_=3; c=(ﾟΘﾟ) =(ﾟｰﾟ)-(ﾟｰﾟ); (ﾟДﾟ) =(ﾟ
Θﾟ)= (o^_^o)/ (o^_^o);(ﾟДﾟ)={ﾟΘﾟ: '_' ,ﾟωﾟ/ : ((ﾟωﾟ/==3) +'_') [ﾟΘﾟ] ,ﾟｰﾟ/ :(ﾟωﾟ/+
'_')[o^_^o -(ﾟΘﾟ)] ,ﾟДﾟ/:((ﾟｰﾟ==3) +'_')[ﾟｰﾟ] }; (ﾟДﾟ) [ﾟΘﾟ] =((ﾟωﾟ/==3) +'_') [c^_^o];(ﾟДﾟ)
['c'] = ((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)-(ﾟΘﾟ)];(ﾟДﾟ) ['o'] = ((ﾟДﾟ)+'_') [ﾟΘﾟ];(ﾟoﾟ)=(ﾟДﾟ) ['c']+(ﾟД
ﾟ) ['o']+(ﾟωﾟ/ +'_')[ﾟΘﾟ]+ ((ﾟωﾟ/==3) +'_') [ﾟｰﾟ] + ((ﾟДﾟ) +'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ ((ﾟｰﾟ==3) +'_')
[ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [(ﾟｰﾟ) - (ﾟΘﾟ)]+(ﾟДﾟ) ['c']+((ﾟДﾟ)+'_') [(ﾟｰﾟ)+(ﾟｰﾟ)]+ (ﾟДﾟ) ['o']+((ﾟｰ
==3) +'_') [ﾟΘﾟ];(ﾟДﾟ) ['_'] =(o^_^o) [ﾟoﾟ] [ﾟoﾟ];(ﾟεﾟ)=((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟДﾟ) .ﾟДﾟ/
+((ﾟДﾟ)+'_') [(ﾟｰﾟ) + (ﾟｰﾟ)]+((ﾟｰﾟ==3) +'_') [o^_^o -ﾟΘﾟ]+((ﾟｰﾟ==3) +'_') [ﾟΘﾟ]+ (ﾟωﾟ/ +'_') [
Θﾟ]; (ﾟｰﾟ)+=(ﾟΘﾟ); (ﾟДﾟ)[ﾟεﾟ]='\\'; (ﾟДﾟ).ﾟΘﾟ/=(ﾟДﾟ+ ﾟｰﾟ)[o^_^o -(ﾟΘﾟ)];(oﾟｰﾟo)=(ﾟω
ﾟ/ +'_')[c^_^o];(ﾟДﾟ) [ﾟoﾟ]='\"';(ﾟДﾟ) ['_'] ( (ﾟДﾟ) ['_'] (ﾟεﾟ+(ﾟДﾟ)[ﾟoﾟ]+ (ﾟДﾟ)[ﾟεﾟ]+(
Θﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (ﾟΘﾟ))+ ((ﾟｰﾟ) +
(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ (o^_^o)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟｰ
ﾟ)+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ (ﾟｰﾟ)+ ((o^_^o) +(o^_^o))+ (ﾟДﾟ)[ﾟεﾟ]+(ﾟΘﾟ)+ ((ﾟｰﾟ) + (o^_^o))+|
```


在线解密：

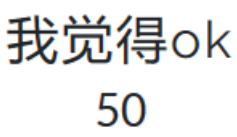
jjencode与aaencode解密

```
moctf{Do_YOu_Th1nk_1_Am_Cut3?};
```

全局变量名称： jjencode解密 aaencode解密 普通解密/Decrypt

- 我觉得ok

题目描述：



flag先发给你好不好

拿到的同样是一堆字符（ook编码）：

Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook.↵
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.↵
Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.↵
Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook. Ook. Ook. Ook.↵
Ook. Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook!↵
Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook!↵
Ook! Ook! Ook! Ook! Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook.↵
Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook.↵
Ook. Ook? Ook. Ook? Ook! Ook. Ook? Ook. Ook. Ook! Ook. Ook? Ook. Ook. Ook.↵
Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook!↵
Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook!↵
Ook! Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook!↵
Ook? Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook.↵
Ook? Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook!↵
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook.↵
Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook? Ook! Ook! Ook! Ook! Ook! Ook! Ook!↵
Ook! Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook!↵
Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook!↵
Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook? Ook. Ook? Ook!↵
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook!↵
Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook? Ook! Ook! Ook. Ook?↵
Ook! Ook! Ook! Ook! Ook! Ook! Ook? Ook. Ook? Ook! Ook. Ook? Ook! Ook! Ook!↵
Ook! Ook! Ook. Ook? Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook. Ook! Ook?↵

在线解码：