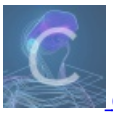
南京邮电大学攻防平台密码题 writeup

原创

南方还是花房 于 2018-10-16 23:50:30 发布 793 收藏 2

分类专栏： crypto 文章标签： ctf

本文链接：https://blog.csdn.net/m1785717/article/details/83099436



南京邮电大学攻防平台

easy!

密文：bmN0Znt0aGlzX2lzX2Jhc2U2NF9lbmNvZGV9

base64解密：`nctf{this_is_base64_encode}`

KeyBoard

密文：ytfvbhn tgbgy hjuygbn yhnmki tgvhn uygbnjm uygbn yhnijm

题目提示了键盘，所以根据密文在键盘上的位置可以笔画出flag:`nctf{areuhack}`

base64全家桶

密文：R1pDVE1NWlhHUTNETU4yQ0dZWkRNTUpYR00zREtNWldHTTJES

1JSV0dJM0RDTlpUR1kyVEdNWlRHSTJVTU5SUkdaQ1RNTkJWSVk

zREVOUlJHNFpUTU5KVEdFWlRNTjJF

提示base64全家桶，考虑base64、base32、base16，将密文依次进行上述顺序解密，得到flag:`nctf{base64_base32_and_base16}`

n次base64

很长的密文，提示是经过多次base64加密得到，手动解密也可以，我用Python解的，代码如下：

```
import base64
import re
with open('base64.txt', 'r') as text:
    base_decode = text.read()
    while bool(re.search('{', base_decode))==False:
        base_decode = base64.b64decode(base_decode)
    print base_decode
```

其中base64.txt是密文文件

运行结果：`nctf{please_use_python_to_decode_base64}

5. 骚年来一发吗

   这道题给了自定义的PHP加密

```
function encode($str){
        $_o = strrev($str);
        for($_0=0;$_0<strlen($_o);$_0++){
                $_c = substr($_o,$_0,1);
                $__ = ord($_c)+1;
                $_c = chr($__);
                $_= $_.$_c;
        }
        return str_rot13(strrev(base64_encode($_)));
}
```


   加密结果为：

   密文：iEJqak3pjlaZ0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas

   用php进行逆向解密，代码如下：

```php
<?php
function decode($str){
 $str=base64_decode(strrev(str_rot13($str)));
 for($_0=0;$_0<strlen($str);$_0++){
  $_c=substr($str,$_0,1);
  $__= ord($_c)-1;
  $_c=chr($__);
  $_=$_.$_c;
 }
 $_=strrev($_);
 return $_;
}
echo decode('iEJqak3pjIaZ0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas');

?>
```

解得flag: `nctf{rot13_and_base64_and_strrev}`

mixed_base64
加密方式如下：

```
import random
from base64 import *
result={
    '16':lambda x:b16encode(x),
    '32':lambda x:b32encode(x),
    '64':lambda x:b64encode(x),
    }

flag=b"nctf{**********}"
for i in range(10):
    a=random.choice(['16','32','64'])
    flag=result[a](flag)

with open("code.txt","wb") as f:
    f.write(flag)
```


code.txt是密文文件，显然将明文进行10次随机base64/base32/base1加密，可以观察密文形式进行解密，解密路径唯一
解得flag: `nctf{random_mixed_base64_encode}`

MD5
明文：TASC?O3RJMV?WDJKX?ZM
md5()加密：e9032???da???08???911513?0???a2
可以看到明文中有一些残缺地方等待补全，可以通过密文展示的字符进行暴力破解。
代码如下：

```
import hashlib
import re

def get_md5_value(src):
    myMd5 = hashlib.md5()
    myMd5.update(src)
    myMd5_Digest = myMd5.hexdigest()
    return myMd5_Digest


def get_str():
    minwen = "TASC?O3RJMV?WDJKX?ZM"
    minwen_1 = list(minwen)
    s = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789"
    s1 = list(s)

    for i in s1:
        for j in s1:
            for k in s1:
                minwen_1[4] = i
                minwen_1[11] =j
                minwen_1[17] = k
                str =''.join(minwen_1)
                md5 = get_md5_value(str)
                if md5[:6] == "e90329" and md5[-2:] == "a2" and md5[8:10] == 'da' and md5[13:15] == '08' and md5
[19:25] == '911513':
                    print md5
                    print "success!"+str
                    exit(0)

get_str()
```

得到flag:

e9032994dabac08080091151380478a2

success! `TASCJO3RJMVKWDJKXLZM`

其实这里考虑不周全，替代的列表应该是全部可打印的字符。看到一个写得更好一点的代码，这里贴出来：

```
# coding:utf8

    import hashlib
    #miwen:e9032___da___08____911513_0___a2
    #mingwen:TASC_O3RJMV_WDJKX_ZM
    str1 = "TASC"
    str2 = "O3RJMV"
    str3 = "WDJKX"
    str4 = "ZM"

    def get_md5_value(src):
        myMd5 = hashlib.md5()
        myMd5.update(src)
        myMd5_Digest = myMd5.hexdigest()
        return myMd5_Digest

    res = [' ', '!', '"', '#', '$', '%', '&', "'", '(', ')', '*', '+', ',', '-', '.', '/', '0', '1', '2', '3', '
4', '5', '6', '7', '8', '9', ':', ';', '<', '=', '>', '?', '@', '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', '[', ']', '^', '_', '`', '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', '{', '|', '}', '~ ']


    for i in res:
        for j in res:
            for k in res:
                str = str1+i+str2+j+str3+k+str4
                #print str+" "
                md5 = get_md5_value(str)
                #print md5+" "
                if md5[:6] == "e90329" and md5[-2:] == "a2" and md5[8:10] == 'da' and md5[13:15] == '08' and md5
[19:25] == '911513':
                    print "Success ! The plaintext is : " + str
                    exit(0)
```

1. List item

`