

原创

Fly_鹏程万里 于 2018-02-28 11:43:15 发布 1878 收藏 2

分类专栏: # 南京邮电大学CTFwriteup 【CTF】

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/Fly_hps/article/details/79397949

版权



[南京邮电大学CTFwriteup](#) 同时被 2 个专栏收录

5 篇文章 0 订阅

订阅专栏



【CTF】

30 篇文章 26 订阅

订阅专栏

1、easy

题目提示:

easy!

50

密文: bmN0Znt0aGZxZ2lzX2Jhc2U2NF9lbnNvZGV9

这题做不出来就剁手吧! [/blog.csdn.net/Fly_hps](https://blog.csdn.net/Fly_hps)

思路:

这是一个加密解密型试题, 根据其特点可知是采用base64加密的, 所以可以直接使用base64在线解密即可。

1. 在线搜索一个base64在线解密网站。

推荐链接: <http://base64.xpcha.com/>



2、KeyBoard

题目提示:



思路:

题目中多次强调“看键盘，看键盘，看键盘”，所以可以确定题目中给定的字母序列的编写与键盘密切相关，根据给定的字母序列于空格可以依次在键盘上找到相应的解密“字母”

解题步骤:

- Ytfvbhn 对应“a”
- Tgbgy 对应“r”
- Hjuygbn 对应“e”
- Yhnmki 对应“u”
- Tgvhn 对应“h”
- Uygbnjm 对应“a”
- Uygbn 对应“c”
- Yhnijm 对应“k”

从上至下依次连接起来可以得到答案：“areuhack”

提交(注意格式: nctf{areuhack})即可!

3、base64 全家桶

题目提示:



可知需要经过base64、base32、base16解密才行，所以我们直接使用Python跑一下就OK:

代码如下:

```
>>> import base64
>>> print base64.b16decode(base64.b32decode(base64.b64decode('R1pDVE1NW1hHUTNETU
4yQOdZWkRNTUpYR00zREtNWIdHTTJES1JSV0dJM0RDt1pUR1kyVEdNWIRHSTJVTU5SUkdaQ1RNTkJWSV
kzREVOUIJHNFpUTUSKVEdFWIRNTJF')))
netf(base64_base32_and_base16)
>>>
```

http://blog.csdn.net/Fly_hps

4、n次base64

题目提示:



打开链接:

```
Vn0vd2QyUX1VWGxWV0d4V1YvZDRWMV13WkRSWFJteFZVMjA1VjAxV2JETlhhMk0xVnpKS1NHVkrVRbUZ
VnxzM1ZtcEj1Rl15U2tWYVJHaG9UV1Z3V1ZacVFtR1RNBpEpJm10aldHSkdjSEJXYTFvaFpWVmFkRTF
VWxStnF6R1Fwa2QvYzJGc1NuUnhSenxWVnpOT00xcFZXbUZrUjA1R1drW1NUbUpGY0VvV2JURXdZVEZ
U0Z0c1pHcFNWR3hoV1d4U11yUnNXbGRYY1hSWFRWaENSbPpYZUhkV01ERkZVbFJDVjAxZVYvU1dha3B
VnpGT2RWYnNXbWshY1hob1ZtMXdUMk15Umtka1JtU11ZbGhtV0ZSV2FF1N1RnBZW1Voa1YwMUVSa1p
YkZKRfZqSkdjbUV6YUzAaGExcG9WakJhVdJ0dFJrZPhiV2hzWwXob2IXwRnWGRVTVZWNVYtdGtWMMWR
YUZsWnJGWhZMYphZE0N1JteFNiSEJjaV2xVb2ExWXdlVYVZTYTFwV11rWktSR1pxU2tabFZsSlpZVVP
VTFKv2N1bFdWRUpoWkRkT2MyTkZhr3BTYkVvVvZteG9RMWRzV25KwGJHUnFwakZHTkZaSGRHdFdiVXB
Vjj4U1dtSkhhR1JXtUZwVfZqRntkRkp0ZUZkaVZrbzFwbXELTkZReFdsAFRiRnBxVWxkU11WU1ZXbnR
YkZweFVtMUDUMkpGv2xw1ZwchJWVEZLVjJOSWJGZFDsVXBvVntSS1QyUkdTbkpUml0cFZqIn9VWnR
VW55Uk1XUkhWMjVTVGxaR1NsaFVWbVEwVjBaYVdHUkhkRnhITUhCS1ZsZDRjMWR0U2toaFJsS1hUVVp
VkZacVNrZFNiRkpb6V1cxc1UwMHhSalpXYVtd1ZUR1Z1RnR1U2s1WFJYQnhWVzB4YjFZeFVsaE9Wenx
Wwtad2VgVnRNVWRVtWtR1YyeHdXbFpXY0hKV1ZFVWkxWVpHY21KR1pHbFhSVXBXVn10U1MxVXhXWGh
YnxaV11saENWRWxyYm5kV1ZscDBaVWM1VWexWFVucFdNV2h2VjBkS1JrNVdVbFZXTITJoSVZHdGFjMk5
WkhSalIyaHBVbGhcZDFkV1Zt0VNVNnAaVTJ4V1YyRXhTbUZhVjNSaFYwWndSbFpZYUZkT1ZrcdVWR3h
VDJGV1Nu1UBWRVTVYVFc1b1d6bHF1a1psUm1SW1drYTFWMyPzY0ZWWFZsSkhaREZrUjJKSVRtaFm1bXh
VkZaYwQyVkdWb1Jsu0dScFVqndWV15ZEhkV01ERnhVbXRVvJFaRldreFdNVnBIWTXs1IxcEdaRTV
UlhCS1ZtMTBVMU14V1hoWFdHagHVMFpVnxscldrdGpSbHB4VkcwNWEySkhVbnBYTTFKVFYyepPkMkp
```

发现许许多多的base密文，而且提示要用n次base64，所以我们可以多次base64解密，直到得到flag:



5、骚年来一发吗？

题目提示：



可以获取的信息：

这是一个php加密函数

密文已知：密文：iEJqak3pjlaz0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas

加密函数已知。

接下来我们要做的就是解密，那么根据加函数的功能我们进行逆向其过程就OK：

```

5
6
7 <?php
8
9 function decode($str){
10     $string=base64_decode(strrev(str_rot13($string)));
11     for($_0=0;$_0<strlen($str);$_0++){
12         $_c=substr($str,$_0,1);
13         $_=ord($_c)-1;
14         $_c=chr($_);
15         $_=$_.$c;
16     }
17     $str=strrev($_);
18     return $str;
19 }
20
21 $str='iEJqak3pjlaz0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas';
22 echo decode($string);
23
?>

```

之后在本地访问该php文件即可：

```

/* 标题phpinfo()：[flag:nctf{gzip_base64_hhhhhh}] */
Notice: Undefined variable: string in D:\phpStudy\WWW\project01\1.php on line 31
Notice: Undefined variable: string in D:\phpStudy\WWW\project01\1.php on line 19
Notice: Undefined variable: _ in D:\phpStudy\WWW\project01\1.php on line 26
Notice: Undefined variable: st in D:\phpStudy\WWW\project01\1.php on line 27

```

6、异性相吸

题目提示：

异性相吸

300

同性真爱，异性相吸都是假的！
(题目要求，我是直的)

解压缩文件里的内容

TIPS:

- 1.xor
- 2.hex2binary
- 3.len(bin(miwen))==len(bin(mingwen))

biubiubiu...

http://blog.csdn.net/Fly_hps

下载文件到本地，并且将解压之后的文件移至Kali中，之后编写脚本如下，根据给定的解密与加密关系进行解密：

```
f_a=open('mi.txt','rb')
f_b=open('ming.txt','rb')

a=""
b=""

a="".join(f_a.readlines())
b="".join(f_b.readlines())

s=''
for i,j in zip(a,b):
    s+=chr(ord(i)^ord(j))
print s
```

http://blog.csdn.net/Fly_hps

The screenshot shows a terminal window in Kali Linux. The user runs 'ls' and lists files including '1.py', 'ming.txt', 'mi.txt', 'VMwareTools-10.0.6-3595377.tar.gz', 'vmware-tools-distrib', 'wingide5_5.0.9-1_i386.deb', 'Nessus', 'OpenVAS.sh', '框架使用方法', 'output', '下载', 'libc.so', and 'pwn500'. The user then runs './1.py' which fails with a 'bash: ./1.py: usr/bin/python: 坏的解释器: 没有那个文件或目录' error. Finally, the user runs 'python 1.py' which outputs the flag: 'flag:nctf{xor_xor_xor_biubiubiu}'. A watermark 'http://blog.csdn.net/Fly_hps' is visible in the bottom right.

7、Md5

题目提示：

python大法好！
这里有一段丢失的md5密文
e9032???da???08????911513?0???a2
要求你还原出他并且加上nctf{}提交
已知线索明文为：TASC?O3RJMV?WDJKX?ZM
题目来源：安恒杯
http://blog.csdn.net/Fly_hps

直接使用Python循环遍历进行查找即可！代码如下：

```
import md5
import string
for i in string.uppercase:
    for j in string.uppercase:
        for k in string.uppercase:
            a='TASC'+i+'O3RJMV'+j+'WDJKX'+k+'ZM'
            b=md5.md5(a).hexdigest()
            if(b[0:5]=='e9032'):
                print b
```

```
root@kali:~# ls
CalcActivationCode.py  MD5.py          VMwareTools-10.0.6-3595377.tar.gz
data                  Nessus          vmware-tools-distrib
Desktop              OpenVAS.sh     wingide5_5.0.9-1_i386.deb
Downloads            output         框架使用方法
libc.so              pwn500        下载
root@kali:~# python MD5.py
e9032994dabac08080091151380478a2
root@kali:~#
```

http://blog.csdn.net/Fly_hps

之后得到flag:nctf{e9032994dabac08080091151380478a2}