南邮ctf writeup

转载

agacx42680 于 2017-09-26 11:28:00 发布 155 收藏
文章标签： php python 密码学
原文链接：http://www.cnblogs.com/kele1997/p/7595853.html

misc

misc题目下载

女神

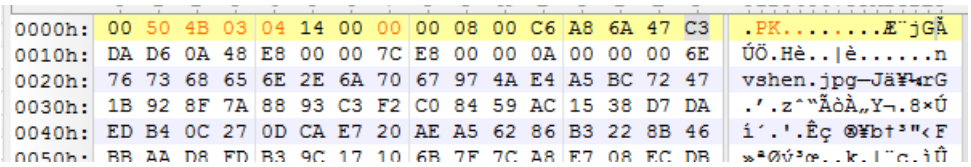
binwalk跑一跑，确实是一张图片，查看文件的详细信息，exif信息无异常，直接二进制打开,ultraedit打开之后，文件末尾发现明文flag。

图种

binwalk跑一跑，发现，中间夹了一个zip文件，dd命令提取出来，获得zip压缩包，flag是zip文件里面gif图片的最后一句话的拼音首字母。

丘比龙De女神

binwalk发现文件末尾是zip的结束标志，但是没有zip的开始标志。二进制打开找吧，在文件末尾出看到nvshen.jpg，搜索在文件中间找到nvshen.jpg，前面有一个love的单词。zip文件的开始标志应该是在这里。提取出来(ultraedit显示文件地址是16进制，dd命令默认用的地址是十进制，需要转换一下).提取出来发现文件损伤，因为zip文件没有开始标志，所以手动修复zip文件，在开头加入PK标志，把50 4B 03 04 14 00 00 00替换6C 6F 76 65 14 00 01 00



最后的flag是这个zip里面的jpg的md5值，软件获取就可以了。

密码学

easy

base64解码

keyboard

看键盘，字母的顺序构成一个图形，图形是字母，试了多次，最后成功了

base64全家桶

看样子是base64，先base64解码，然后base64不行，使用base32，base16,最后得到flag
本题主要考察base64、base32、base16的特点：

> base64中包含大写字母（A-Z）、小写字母（a-z）、数字0——9以及+/
> base32中只有大写字母（A-Z）和数字234567
> base16中只有数字0-9以及大写字母ABCDEF。

n次base64

python解base64，复制字符串，去掉回车，把'\r\n'替换掉，然后复制给字符串

```
import base64

s="字符串"
for i in range(100):
   try:
        s=base64.b64decode(s)
    except Exception as e:
        print s
        return ""
```

骚年来一发吗

php的代码反过来,想了很久，还是没想通.....，等我整理的时候自己做出来了2333333

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

print decode("iEJqak3pjIaZ0NzLiITLwWTqzqGAtW2oyOTq1A3pzqas");


?>
```

mixed_base64

丧心病狂的加密方式，随机base64 32 16 ,上python,解码的顺序一定要注意，先base16,然后base32，在之后base64,因为base16一定可以使用base64解，所以有可能密码可能被解码成乱码

```
#coding:utf-8
import base64

#读取文件先
code=open("code.txt","r").read()
while(True):
 #base16
    try:
        p=base64.b16decode(code)
        code=p
        print "base16\n"
        continue
    except:
        pass
    #base32
    try:
        p=base64.b32decode(code)
        code=p
        print "base32\n"
        continue
    except:
        pass

    #base64
    try:
        p=base64.b64decode(code)
        code=p
        print "base64\n"
        continue
    except:
        pass

    break

print code
```

异性相吸

文件读写,二进制异或操作

```
miwen=open("密文.txt","rb")
mingwen=open("明文.txt","rb")
result=open("result.txt","wb")

for i in range(len(miwen)):
    result.write(chr(ord(miwen[i])^ord(mingwen[i])))

result.close()
```

打开result.txt就查看了flag了

转载于:https://www.cnblogs.com/kele1997/p/7595853.html