i春秋时间

转载

weixin_30701575 于 2019-09-11 14:10:00 发布 221 收藏
文章标签： php
原文链接：http://www.cnblogs.com/wosun/p/11505957.html

打开题目就是一段php代码

```
<?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);
}
```

大致的意思是

设置头请求为。。。。。。

然后说了句废话，天下武功唯快不破

再设置cookie中的token为hello

高亮显示文件

然后是一个if结构

如果cookie中的token等于hello就让txt等与flag.php的连接

filename等于 一个md5加密的随机txt

然后再把filename存入txt中

休息十秒

删除foname文件

我们访问这个网站的时候，在网站目录里面会随机生成一个文件包含flag.php的内容，但是我们只有10秒的时间取访问它，10秒过后会自动删除,文件的名字是随机的，我们需要猜到文件名就可以了

这里使用御剑扫描

先制作字典

字典生成脚本

```
import hashlib
import requests
file = open("data.txt",'w+')
for i in range(1,1001):
  m = hashlib.md5()
  m.update(str(i).encode())
  mid = m.hexdigest()
  url = 'u/'+mid+'.txt'
  file.write(url+'\n')
file.close()
```

再打开御剑，将data.txt放入御剑的文档中

选择批量扫描后台，在右侧添加我们的字典

然后在刷新题目网页的10s内将其复制url，粘贴，开始扫描

再访问200响应的文件即可获得flag

转载于:https://www.cnblogs.com/wosun/p/11505957.html