原创 Python老吕 已于 2024-03-14 00:54:54 修改 阅读量1.9k 收藏 22 点赞数 23

分类专栏： 《跟老吕学PHP》 文章标签： php 开发语言 PHP伪协议详解 PHP伪协议 phar data zip与bzip与zlib协议

PHP 《跟老吕学PHP》 专栏收录该内容 2 订阅 35 篇文章

PHP伪协议 **详解**

一、前言

1.什么是PHP伪协议?

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_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

2.什么时候用PHP伪协议?

文件包含！！！的时候，可能遇到的文件包含函数:
1、include
2、require
3、include_once
4、require_once
5、highlight_file
6、show_source
7、flie
8、readfile

Python老吕 关注 23 22 0

11、fopen (比较常见)

二、常见的php伪协议

php://input

php://input 是个可以访问请求的原始数据的只读流，获取POST请求数据的协议

当enctype="multipart/form-data" 的时候 php://input 是无效的。

php://input 伪协议 成功执行前提
php.ini 中的 allow_url_include设置为On

格式示例：

```
php
<?php
@include($_GET["file"]);
?>
```

php://filter

php://filter 是一种元封装器， 设计用于数据流打开时的筛选过滤应用。 这对于一体式（all-in-one）的文件函数非常有用，类似 readfile()、 file() 和 file_get_contents()， 在数据流内容读取之前没有机会应用其他过滤器。

在利用上很多都是与包含函数结合使用，读入或者输出获取文件源码然后编码让其不执行从而输出

php://filter 的使用：
如
php://filter/read=convert.base64-encode/resource=index.php
php://filter/resource=index.php

php://filter 伪协议组成：
read=<读链的筛选列表>
resource=<要过滤的数据流>
write=<写链的筛选列表>
php://filter/read=处理方式（base64编码，rot13等等）/resource=要读取的文件

read 对应要设置的过滤器：
常见的过滤器分字符串过滤器、转换过滤器、压缩过滤器、加密过滤器
其中convert.base64-encode ， convert.base64-decode都属于 转换过滤器

格式示例：

```
<?php
$a=($_GET["file"]);
echo(file_get_contents($a));//获取文件内容
?>
```

zip://与bzip2://与zlib://协议

zip:// 等属于压缩流的协议，通过直接压缩普通文件为zip文件，再通过zip:// 协议读取，可以直接执行php代码。压缩后的zip文件可以随意修改后缀也
协议读取。（注意是如phpinfo.txt直接压缩为zip,而不是文件夹压缩zip）

格式示例：

```
<?php
$a=($_GET["file"]);
include($a);
?>

```

Python老吕 关注 23 22 0

压缩及协议访问格式：

压缩文件为.zip后缀
zip://绝对路径/phpinfo.zip%23phpinfo.php
压缩文件为.bz2后缀
compress.bzip2://绝对路径/phpinfo.zip/phpinfo.php
压缩文件为.gz后缀
compress.zlib://绝对路径/phpinfo.zip/phpinfo.php

---

data://

data://伪协议可以通过请求提交的php代码数据配合文件包含函数可以达到代码执行效果。

data://伪协议 成功执行前提
php.ini设置allow_url_include 与allow_url_open都为On。

data://协议的格式是: data://数据流封装器,相应格式数据

格式示例：

```php
<?php
$a=($_GET["file"]);
include($a);
?>
```

---

phar://

phar://伪协议可以对zip格式压缩包进行访问解析

格式示例：

```
phar://绝对路径\phpinfo.zip\phpinfo.php
```

注意这里与zip://不同的地方是，phar访问压缩包内容是通过/访问，而zip是通过#访问

> Python老吕提醒
> 使用这些伪协议时，需要注意PHP配置和服务器环境的限制，某些协议可能因为配置或安全原因被禁用。
> 特别是在处理外部资源（如HTTP或FTP）时，需要注意安全性，确保不会暴露敏感信息或遭受注入攻击。
> 在使用 data://、phar:// 等伪协议时，应特别注意数据的验证和清洁，以避免安全漏洞。

博主Python老吕说：如果您觉得本文有帮助，辛苦您帮忙点赞、收藏、评论，您的举手之劳将对我提供了无限的写作动力！

精品付费专栏:(暂时免费，尽快订阅、收藏哦)
《跟老吕学Python编程》
《跟老吕学Python编程·附录资料》

前端:
《跟老吕学HTML》
《XHTML》
《CSS》
《JavaScript》
《Vue》

后端:
《跟老吕学C语言》

Python老吕 关注 23 22 0