

Forum:[Hack Forums](#)

Thread: [\[TUT\] Local file inclusion without NULL-byte.](#)

AntiPaste - February 7, 2012, 11:32 am

Index0x00 - Introduction

0x01 - Summary

0x02 - Exploitation

0x03 - Ending words

0x00 - Introduction

Greetings.

Basically what I'm about to demonstrate is a vulnerability in PHP versions up to and including 5.2.8 with Suhosin patch 0.9.6.3. The vulnerability allows for local file inclusion without the well-known, and patched, NULL-byte injection and affects at least the following functions: `fopen`, `include_once`, `require_once`, `file_put_contents` and `file_get_contents`.

This tutorial will not have a vast technical explanation on what's happening behind the scenes. If you're interested in that, you can read the full vulnerability write up at <http://www.usb.it/2009/02/08/php-file-system-attack-vectors/>.

Let's begin.

0x01 - Summary

First off, a brief summary of the vulnerability.

PHP truncates paths used by filesystem functions, by default, into 4096 bytes. Thus by filling the buffer, we basically remove whatever is left at the end of the path sent as an argument to the function. This is what NULL-byte injection achieves as well, but differently. NULL-byte injection relies on C-based language's way of handling NULL-bytes as the end of a string, this vulnerability is a flaw in PHP itself, a design error.

The ideal way to fill the buffer is with `"/." strings and this is the string this tutorial will be using.`

0x02 - Exploitation

To start with, let's find ourselves an LFI vulnerable site.

<http://www.becrux.com/index.php?page=projects> just happens to be vulnerable to LFI in the page-parameter, as adding any character to the end of the URL [\[1\]](#) produces this error:

Code Warning: include(pages/projects!/index.php) [function.include]: failed to open stream: No such file or directory in /web/htdocs/www.becrux.com/home/index.php on line 111

Hurray! Now, let's try to include an arbitrary file from the filesystem on with the notorious NULL-byte injection [\[2\]](#).

Alas, NULL-byte is escaped and we simply get another error instead of a successful exploitation:

Code Warning: include(pages/./style/style.css\0/index.php) [function.include]: failed to open stream: No such file or directory in /web/htdocs/www.becrux.com/home/index.php on line 111

Now's the time to crack out our filesystem path truncation attack.

We start off with an invalid directory, for example `"a/"`.

Then we add our path traversal, pointing to the file that we want to include like this

".././style/style.css". The first "../" is for our invalid directory, don't forget that.
The path looks like this now: "a/../../style/style.css"

Here comes the exploit.
We add 2027 times the string "/" to the end of the path which will fill up the buffer and get rid of the ".php" at the end.

You end up with an URL like this: [\[3\]](#)

Success, we have included an arbitrary file on the server!

0x03 - Ending words

I hope this tutorial made any sense and / or was of use to anyone reading it. I'd appreciate feedback and corrections on it where applies.

Also, sorry for the bad example, however becrux.com refuses to include /etc/passwd due to a chroot.

Error667 - February 7, 2012, 12:17 pm

Will check this, thanks for this mate.

QuantumTunnel - February 7, 2012, 12:18 pm

Nice tutorial mate. Thanks for spending the time to create this tutorial much appreciated. :)

MajorFail - February 7, 2012, 12:49 pm

Nice tut! Edit: didn't read the tut properly, you already mentioned the 4096 buffer size. But it might be handy to point out that some server have a bigger buffer. :)

AntiPaste - February 7, 2012, 1:02 pm

(Feb 7, 2012 01:49 PM)MajorFail Wrote: [\[CITE\]](#) Nice tut! Edit: didn't read the tut properly, you already mentioned the 4096 buffer size. But it might be handy to point out that some server have a bigger buffer. :)

The default setting is 4096 and it can only be changed during compile time if I remember correctly, not to mention that it's not a well known setting. Thus 99% (100% made up statistic) of the servers have the default buffer of 4096.

? e x - February 7, 2012, 1:05 pm

good tut bro, what about etc/passwd ?

AntiPaste - February 7, 2012, 1:10 pm

(Feb 7, 2012 02:05 PM)Linuxer Wrote: [\[CITE\]](#) good tut bro, what about etc/passwd ?

You should be able to figure that out.

Just change the ".././style/style.css" part of the tutorial to ".././.././.././.././.././etc/passwd".

I explained why I didn't do that in section 0x03.

virus_in_town - February 7, 2012, 1:21 pm

This was great tutorial atleast for me ! it gave me new way to think liked the way you explained thanks alot for this. Keep the good work bro.

Das_Virus - November 6, 2012, 2:22 pm

How do you get the path? i mean how do you know that style.css is in .././style/style.css

Is there any way to list all files?

BeggFoMercy - November 6, 2012, 2:31 pm

Impressive work , Well written , keep it up <3

133720 - November 6, 2012, 6:42 pm

Great! P0st Dude

I learning advance in LFI

Thanks for tut

AntiPaste - November 6, 2012, 10:32 pm

(Nov 6, 2012 03:22 PM)Das_Virus Wrote: [\[CITE\]](#) How do you get the path? i mean how do you know that style.css is in ../../style/style.css

Is there any way to list all files?

Those are relative paths and I found the location from the site's source code.

The style.css was only an example.

If you can see the full path from the PHP error, it's easier to see how many directories you have to go up to get to the website's root directory.

There's no way to list all the files so you'll have to go guessing, or use files included with almost every copy of the OS.

For example, with Linux /etc/passwd, /proc/self/version etc.

chip_worm - December 10, 2012, 11:47 am

I m too far away to learn this kind of hard attack....

Illicit - December 10, 2012, 11:52 am

Nice tutorial :p Another way to do his would be like this:

<http://www.site.com/page.php?page=projects/../../etc/passwd#>

Great tutorial though I liked the HEX layout :3

AntiPaste - December 10, 2012, 12:03 pm

(Dec 10, 2012 12:52 PM)Red_Hat Wrote: [\[CITE\]](#) Nice tutorial :p Another way to do his would be like this:

<http://www.site.com/page.php?page=projects/../../etc/passwd#>

Great tutorial though I liked the HEX layout :3

This was posted more than 10 months ago as you can see. :3

People keep grave digging it though. Thanks anyways. ~

Adding the # at the end of the URL does nothing since most browsers use that as an anchor-tag.

It's not included in the request sent to the server in any way.

You probably meant adding # in it's URL encoded form (%23).

That does nothing for LFI and is most certainly not another way to do what my tutorial explains.

Mormaii - December 10, 2012, 12:06 pm

(Dec 10, 2012 01:03 PM)AntiPaste Wrote: [\[CITE\]](#) This was posted more than 10 months ago as you can see. :3

People keep grave digging it though. Thanks anyways. ~

Adding the # at the end of the URL does nothing since most browsers use that as an anchor-tag.

It's not included in the request sent to the server in any way.

You probably meant adding # in it's URL encoded form (%23).

That does nothing for LFI and is most certainly not another way to do what my tutorial explains.

Doesn't matter if it's a grave dig or not since it's a great tutorial and everyone should see it.

MajorFail - December 10, 2012, 2:57 pm

(Dec 10, 2012 12:52 PM)Red_Hat Wrote: [\[CITE\]](#) Nice tutorial :p Another way to do this would be like this:

<http://www.site.com/page.php?page=projects/../../etc/passwd#>

Great tutorial though I liked the HEX layout :3

I think your mistaking a SQLi method (# is a comment char that let's MySQL see the rest of the line as a comment), this will not work with LFI. ?

Starfall - December 10, 2012, 8:30 pm

(Nov 6, 2012 11:32 PM)AntiPaste Wrote: [\[CITE\]](#) /proc/self/version

I love calling people out on stuff like this.

/proc/self/version doesn't exist. You're thinking of /proc/version and /proc/self/environ.

AntiPaste - December 11, 2012, 3:33 am

(Dec 10, 2012 09:30 PM)Starfall Wrote: [\[CITE\]](#) I love calling people out on stuff like this.

/proc/self/version doesn't exist. You're thinking of /proc/version and /proc/self/environ.

Indeed.

I was probably thinking about both of them and brainfarted it into /proc/self/version. x.x

Thanks.<3 ~

joube - January 20, 2014, 1:20 pm

Cool I was having problem with a null byte injection filtered. Actually it also works without the invalid directory: "../../../../style/style.css" or "../../../../style/style.css/../../../../"

Putting "../../../../" instead of "../../../../" (dubble "/" for keeping the same number of chars)

Actually it does not work for me because the suffix is added before in another var:

```
$theme = 'themes/'. $my_theme . '_pref.php';  
include_once $theme;
```

Is there any way to bypass the '_pref.php' in this configuration??

21redallday12 - January 20, 2014, 4:12 pm

Nice tutorial... ,

keep it up.. .

Sciffs - January 20, 2014, 4:14 pm

Nice job, really well told, and pretty impressive

warghost - December 1, 2016, 8:48 am

good tut bro, thanks for share :)

iampayload - December 9, 2016, 12:01 am

Great work. More examples will be appreciated. Thanks

memory - December 9, 2016, 2:02 am

Just to clarify, this is using the 4096 byte exploit?

(Jun 13, 2015 05:24 AM)Tony S Wrote: [\[CITE\]](#) There was another lesser-known vulnerability present in PHP versions up to and including 5.2.8 along with Suhosin 0.9.6.3 that affected filesystem

functions.

Filesystem paths passed into these functions as arguments had a buffer size of 4096 bytes. If you were to fill the buffer with arbitrary, valid data, the path used in the syscall would be truncated. For example, if someone submitted an "email" that set the value of \$email to "asdf.php/././." (with a lot more ./'s that would eventually fill the buffer), the .txt file extension would be dropped in the syscall.

This isn't really an issue if your PHP version is up to date. You can read more [here](#) if you want to.

Source: <https://hackforums.net/showthread.php?tid=4862292&pid=46563839#pid46563839>

EDIT: Just re-read the thread again and saw you already included all of that info, thank you!

This is really neat OP, thank you for the share!

lochv37 - December 9, 2016, 6:11 pm

well done bro, kip it up.