

Forum:[Hack Forums](#)

Thread: [\[Website\] LFI: Local file inclusion? what is it? and a simple proof of concept #3](#)

slober - April 18, 2020, 4:01 pm

[Web] LFI: Local file inclusion on a website#33

A few days ago I did a CTF challenge with a few buddies of me and this was one of the easier ones. It mainly focussed on a super simple LFI vulnerabilities

LFI stands for Local file inclusion.

Simply put you can inject local files in the webserver and if the webserver runs as root you can pretty much call a lot of files ?.

The counterpart of LFI is RFI which stands for remote file inclusion same principle applied here only this time you aren't including a local file but a remote one such as webshell or an exploit.

In this example, we've used the local one.

How can this happen?

well, most of the time it's due to sloppy or rushed code writing a quick example or POC and well not updating it...

PHP Code

```
<?php
```

```
if ( isset ( $_GET["name"] ) ) {  
    include ( $_GET["name"]);  
}
```

```
?>
```

If I ran this code on my webserver I would most likely have a bad day in the near future.
What's happening?

Well, when the get param name is set (has a value) it will include that value in its code.
That would mean if I have a text file called superduper-awesome-secrets.txt I could view it on said webpage.

That wouldn't be a good thing to happen right?

Yes, it does still happen out in the wild maybe not that often or this obvious but well it is out there.

How would this be beneficial to us?

Let me bounce that question back with another one which file on a Linux system could contain (unencrypted) passwords?

Code /etc/passwd

/etc/shadow

How can you figure out that you're dealing with a possible LFI vulnerability (in a CTF environment)

well add "./" in front of your get request
try playing with the request changing the input and see what happens.

once you're getting something similar like picture 2 you could possibly be dealing with an LFI vulnerability.

All we have to do now is add a bunch of ../../ and /etc/passwd or /etc/shadow at the end

What is the meaning of ../?

../ will go up a directory

Once you've got the credentials you can spawn up an ssh shell and you're pretty much inside...
all you need to do now is find the flags or escalate your privileges.

In this chapter in our capture the Flag campaign we didn't need a shell. We did need to capture two flags the root flag and the user flag. so we only needed the user name (hence etc/passwd to get the username) and well the root username is root so that was pretty easy. the flag locations where
Code ../../../../jhonyc/user.flag and

../../../../root/root.flag

For those that still had that lingering question ?

Ahh, it brought back memories indeed.

If you have a raspberry pi you can try this out! It's very easy to try this and it should give you some basic insight about LFI and security in general. don't be sloppy when you're coding and don't rush it.

This kind of vulnerabilities are so much fun ?

UPDATE #1:

Reason: Interesting addition by ??@???:

Spoiler ([Click to View](#))

(Apr 18, 2020 04:33 PM)??@??? Wrote: [\[CITE\]](#) There are other ways to Pop a shell with LFI such as PHP wrappers , proc/self/environ etc :) (Apr 18, 2020 05:06 PM)slober Wrote: [\[CITE\]](#) Thank you added some extra reading material at the end of the tutorial this server wasn't susceptible to these attacks it used a get parameter so PHP wrappers (like php://file) were out of the question expect isn't enabled by default so we couldn't use that (expect:// LFI) we didn't try proc/self/environ (tried it after you've mentioned it) and we didn't really need it

In this chapter (1 of 5 that day and this one was the most simple) in our capture the Flag campaign we didn't need a shell. We did need to capture two flags the root flag and the user flag. so we only needed the user name (hence etc/passwd to get the username) but the way or machine was set up would never spawn a shell

nevertheless, I've added the reading materials as this was just a small introductory ?

Extra:

If you want to explore LFI more you could look into it this was a basic example just for funsies.

There are so much more ways to pop up shells you could, for example, execute PHP code use different kind of PHP-wrappers and other file locations such as proc/self/environ

These three sites will go so much more in-depth on this topic I really advise these if you want to know more about it.

<https://www.aprive.co.uk/blog/local-file-inclusion-lfi-testing/>
<https://highon.coffee/blog/lfi-cheat-sheet/>
<https://book.hacktricks.xyz/pentesting-web/file-inclusion>

??¢??? - April 18, 2020, 4:33 pm

There are other ways to Pop a shell with LFI such as PHP wrappers , proc/self/envIRON etc :)

slober - April 18, 2020, 5:06 pm

(Apr 18, 2020 04:33 PM)??¢??? Wrote: [\[CITE\]](#) There are other ways to Pop a shell with LFI such as PHP wrappers , proc/self/envIRON etc :)

Thank you added some extra reading material at the end of the tutorial this server wasn't susceptible to these attacks it used a get parameter so PHP wrappers (like php://file) were out of the question "expect" isn't enabled by default so we couldn't use that (expect:// LFI) we didn't try proc/self/envIRON (tried it after you've mentioned it and it shouldn't have worked the way the machine was set up) We didn't really need it in the end

In this chapter (1 of 5 that day and this one was the most simple) in our capture the Flag campaign we didn't need a shell. We did need to capture two flags the root flag and the user flag. so we only needed the user name (hence etc/passwd to get the username) but the way or machine was set up would never spawn a shell

nevertheless, I've added the reading materials as this was just a small introductory ?

??¢??? - April 18, 2020, 6:12 pm

(Apr 18, 2020 05:06 PM)slober Wrote: [\[CITE\]](#) Thank you added some extra reading material at the end of the tutorial this server wasn't susceptible to these attacks it used a get parameter so PHP wrappers (like php://file) were out of the question "expect" isn't enabled by default so we couldn't use that (expect:// LFI) we didn't try proc/self/envIRON (tried it after you've mentioned it and it shouldn't have worked the way the machine was set up) We didn't really need it in the end

In this chapter (1 of 5 that day and this one was the most simple) in our capture the Flag campaign we didn't need a shell. We did need to capture two flags the root flag and the user flag. so we only needed the user name (hence etc/passwd to get the username) but the way or machine was set up would never spawn a shell

nevertheless, I've added the reading materials as this was just a small introductory ?
I appreciate you writing this thread and you did an excellent job.

Also, did you try the Log File Contamination method? If you know the location of the log file and can access it, this is a very good method

If you a file upload somewhere on the website, you can chain it with
php?page=zip://path/to/file.zip%23shell

php://input&cmd=ls. (Change the HTTP Request method to post and send the shellcode in the POST Data)

Brief - *January 1, 2023, 7:50 pm*

Love this tutorial. Well explained.

Forex Advice - *April 6, 2023, 4:17 am*

Nice tutorial , very cool !