

Forum:[Hack Forums](#)

Thread: [General web-hacking tips & tricks](#)

Meowie - October 4, 2015, 5:23 am

Well, i'm bored as fuck and I want to be a cool kid, so i'm making this thread.

Here, i'll list some random tips & tricks i've learned from tutorials, books, guides, CTFs, writeups, etc.

This thread will help you if you're new, and probably even if you aren't.

Please excuse any mistakes since English is not my first language.

////////////////////////////////////

1. Getting a full path

Spoiler ([Click to View](#))

Most of us have been in a situation where you have an SQLi with file priv, you can read all you want, write all you want, but can't get the full path of the site.

Something you can try is going around the site and changing GET/POST parameters from strings to arrays using [].

There are several php functions that will give back an error when supplied with an array (trim for example) instead of a string.

Example: gay.com/notvulnerable.php?search[]=123

(note: if errors are disabled, this won't help)

Another common way is to look for a phpinfo file. Chances are you won't find this on big sites, but if you're targetting some small site, give this a go.

I recommend using DirBuster on Windows & dirb on Linux to look for phpinfo files. I'll drop links for both of these at the bottom of this post.

Yet another way to get the full path is to check common log files. What I usually do is look at what version of nginx/apache/whateverthefuck its running and look up the default log directory, then try to read the access & error logs. With a bit of luck, you'll get them and you'll have your FPD in there.

If the site is running on a shared hosting, you can try finding other sites that run on the box via several tools like yougetsignal, bing and the like.

Once you find some, you can try and get an FPD on them. The more sites, the higher the chance.

Most of the time, the path you'll get is something like this: /srv/www/vhosts/site.com/public_html

From here, you can replace site.com with the site you're targetting, and there's your full path.

And last one for this bunch would be subdomains. You have no idea how many people make subdomains thinking they'll be the only ones to know about them and end up getting hacked. There are several tools to bruteforce subdomains, but I mostly use fierce.pl and knock. A bonus is sometimes the dns server may be misconfigured and you can get a list of ALL the subdomains without bruteforcing.

////////////////////////////////////

2. Bypassing is_numeric

Spoiler ([Click to View](#))

Say you're hacking a website. You know what CMS it's running, you have the source. You find a potential SQLi, but it's being passed to an `is_numeric` check first.

Let's say this is the code:

```
Code $cocks = $_GET['image'];
```

```
$id = $_GET['id'];
```

```
if(!is_numeric($cocks) || !is_numeric($id)){  
    die('Please enter a valid id/image.');
```

```
}
```

```
$zeroday = mysql_query('SELECT concat('.$cocks.', _image) as path FROM images WHERE id =  
'.$id.);
```

```
$path = mysql_result($q, 0);
```

...It looks impossible to bypass, but it's not.

The way to bypass it is hex encoding. Yeah, hex encoding.

If we set `$_GET['image']` to `0x6e656b6f` (which is "neko", hex encoded) it will bypass the `is_numeric` check, and MySQL will decode it and insert it in the query.

Now to automate this, all you have to do is hex encode your parameter. Easy.

////////////////////////////////////

3. A lesser known way to exploit LFI

Spoiler ([Click to View](#))

Note: This works on older versions of PHP. Not sure which version patches it, but it should work on `<=5.3.x`

Here's the situation you're in:

You have an LFI.

`/proc/self/environ` and `/proc/self/fd(1/2/3)` don't work.

None of the php wrappers work.

You can't find the logs the server is storing.

It's using `require` instead of `include`, so you can't read the code of the included files.

The site isn't running on a shared hosting.

There are no places to upload a file.

You found the `phpinfo` file.

What would you do in this situation?

Most people would probably give up, but there is hope.

Yesterday I read a book on exploiting an LFI when you've found a `phpinfo` file.

What it was is basically that whenever you submit a file, php accepts it and stores it in the temp directory with a random name till the request is over.

When the request is over, it gets deleted. This happens in less than 3 seconds.

Now, where does `phpinfo` come into this? Well, whenever you submit a request to `phpinfo`, it shows you all the parameters you've set, and that includes submitting the file. It shows you the temporary file name.

What you need to do is submit a php file to `phpinfo`, get the filename and run it through the LFI before PHP manages to delete it.

Quite the job, don't you think? Well, that's why we have scripts for these kinds of jobs.

I'll leave links to several scripts to exploit this.

Also, on Windows, there is another easier method just like this, but I'll just leave a link to that since I haven't really tested it myself.

////////////////////////////////////

That's about it for now, because i'm a lazy fuck.

I'll keep adding more to this thread when I feel like it.
Peace.

References & links

Code Dirbuster - sourceforge.net/projects/dirbuster/

dirb - dirb.sourceforge.net/

YouGetSignal - yougetsignal.com/tools/web-sites-on-web-server/

Fierce.pl - aldeid.com/wiki/Fierce

Knock - github.com/guelfoweb/knock

LFI with PHPInfo - packetstormsecurity.com/files/104825/LFI-With-PHPInfo-Assistance.html

LFI with PHPInfo - insecurity.net/?p=687

Script to exploit the LFI - github.com/D35m0nd142/Kadabra/blob/master/phpinfo.py

There is also a built-in module in fimap for the exploit.

Elliotstanleybrown - October 4, 2015, 5:27 am

Thanks Man I Just Got some stuff from a website :D

TheSlap - October 4, 2015, 5:40 am

Nice trick for bypassing `is_numeric()`, hopefully some skiddles can learn a few things by utilizing some of the tips in this tutorial.

(Oct 4, 2015 05:27 AM)Elliotstanleybrown Wrote: [\[CITE\]](#) Thanks Man I Just Got some stuff from a website :D

I hope your comment isn't in reference to his tutorials because there is no fucking way you read it & put it to use in 4 minutes.

> Reasons to hate the W&F hacking section on this shit tier forum.

Aakash_Choudhary - October 4, 2015, 6:30 am

Nice tips and tricks for Beginners.

Nothing new for me but this is very good for those who don't know.

By the way there are lots of functions other than `phpinfo` for exploiting LFI

Thanks.keep it up.Good work. Waiting for more.

?

Meowie - October 4, 2015, 6:40 am

(Oct 4, 2015 06:30 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) Nice tips and tricks for Beginners.

Nothing new for me but this is very good for those who don't know.

By the way there are lots of functions other than `phpinfo` for exploiting LFI

Thanks.keep it up.Good work. Waiting for more.

?

I didn't list all of the ways of exploiting LFI lol.

Most of the time, it's different for every site.

Aakash_Choudhary - October 4, 2015, 7:22 am

I would like if you also include this site as reference which can help beginners :->

Code <http://stackoverflow.com/questions/3115559/exploitable-php-functions>Thanks

Meowie - October 4, 2015, 8:08 am

(Oct 4, 2015 07:22 AM)Aakash_Choudhary Wrote: [\[CITE\]](#) I would like if you also include this site as

reference which can help beginners :->

Thanks

Fuck editing the thread anymore.

I have to use htmlentities to encode "/proc/ self/envIRON" every time because CF detects it and doesn't let me post.

hahdbwoannniabs - October 4, 2015, 9:10 am

Another way to find the full path is to load the /etc/passwd file and see the users' home directories in hope that the target website's directory will be in there somewhere. And also there are config files you can look in (other than the apache/nginx/whatever configs) that will sometimes have a full path. Furthermore, you left out tampering with the session for FPD. You can insert any illegal characters (usually anything that isn't a letter or number) in your PHPSESSID (or whatever the cookie name is) and it will throw you an error containing the full path if you're lucky.

Also, is_numeric is gay and uncommon, most non-retarded people will use intval() if they know what they're doing.

Other than that, nice thread.

Meowie - October 4, 2015, 9:26 am

(Oct 4, 2015 09:10 AM)_anthrax Wrote: [\[CITE\]](#) Another way to find the full path is to load the /etc/passwd file and see the users' home directories in hope that the target website's directory will be in there somewhere. And also there are config files you can look in (other than the apache/nginx/whatever configs) that will sometimes have a full path. Furthermore, you left out tampering with the session for FPD. You can insert any illegal characters (usually anything that isn't a letter or number) in your PHPSESSID (or whatever the cookie name is) and it will throw you an error containing the full path if you're lucky.

Also, is_numeric is gay and uncommon, most non-retarded people will use intval() if they know what they're doing.

Other than that, nice thread.

I just felt lazy.

As for the session, you can even just clear it.

Like, remove all of its contents and it will error out.

Viktory - November 2, 2015, 7:56 am

another few ways to get a fpd is to make the server timeout by sending a massive request, or by using a dork to find any config files the admin might have forgot to delete after setting up the website.