

Forum:[Hack Forums](#)

Thread: [File Upload Issue \(Found Image Backdoor\)](#)

Numinous - August 22, 2017, 11:48 pm

Please look at this code - <https://gyazo.com/f292c173dbebccde90b1a8b4cd02b7ea>

whcih i found in one of the web server and that site is using some FILE UPLOAD functionality and someone uploaded a valid .GIF file and when i extracted that gif file with the help of Notepad and then i found a file upload backdooring code in the middle of the file.

So my question is, how a hacker can execute this backdooring code even that file upload code is very much secured.

Payload - August 22, 2017, 11:54 pm

The code will be executed when the image is loaded. Have a look at some other examples to understand how this works.

<https://hackerone.com/reports/135072>
<https://secgeek.net/bookfresh-vulnerability/>

Numinous - August 23, 2017, 12:06 am

I already read that links, and i tried to open that .GIF file in my browser and it actually displays a image but i'm unable to execute that PHP code.

I tried all best possible ways like .gif.php, .php.gif, .gif.php2, .gif.php3, .php etc

Payload - August 23, 2017, 12:11 am

(Aug 23, 2017 12:06 AM)Numinous Wrote: [\[CITE\]](#) I already read that links, and i tried to open that .GIF file in my browser and it actually displays a image but i'm unable to execute that PHP code.

I tried all best possible ways like .gif.php, .php.gif, .gif.php2, .gif.php3, .php etc
Use ASCII encoding, you are probably saving the file UTF-8

Send a paste, i'm too lazy to type it out.

Charger - August 24, 2017, 7:08 am

If you send proper headers they shouldn't be able to execute it.

How did it get uploaded?

Ceanko - August 24, 2017, 8:57 am

Not enough information really, but this should help you: [ForceType](#).

Like Charger said, headers. Although I suggest you still fix the issue at the root; checking if an image is valid.