

Forum:[Hack Forums](#)

Thread: [Bypassing upload file extension filter](#)

leoniss - February 18, 2020, 1:13 pm

Hello I'm trying to upload some php script but the extension filters anything that isn't images or videos. I've seen some trick by replacing the extension like .jpg.php but they're old tricks that have been patched. Is there anything new that will work?

red forman - February 18, 2020, 3:54 pm

try a different shell script.

FlySwatter - February 19, 2020, 4:13 am

The double extension (.jpg.php) only worked on mis-configured apache servers.

I don't think there is any bypass that is universal. What I would do is get a copy of the code that is blocking my upload and see how they are filtering. Long ago I saw a poorly coded wordpress plugin that filtered lowercase characters, but not uppercase characters. Another one filtered 'php', but not: phtml, .php3, .php4, .php5

It all depends on the code at the other end. See?

Money- - February 19, 2020, 4:18 am

(Feb 19, 2020 05:13 AM)FlySwatter Wrote: [\[CITE\]](#) The double extension (.jpg.php) only worked on mis-configured apache servers.

I don't think there is any bypass that is universal. What I would do is get a copy of the code that is blocking my upload and see how they are filtering. Long ago I saw a poorly coded wordpress plugin that filtered lowercase characters, but not uppercase characters. Another one filtered 'php', but not: phtml, .php3, .php4, .php5

It all depends on the code at the other end. See?

Yes it all depends on back-end of the filtering. It might be a client side filtering or it might be a back-end filtering.

Try and fuzz around to see what extensions it allows and try to manipulate your extension script later on.

If the filtering or validation is client-side which I doubt it will be, burp suite is always your friend to change extension when you intercept the request during upload.

leoniss - February 22, 2020, 8:42 am

It's a back-end filtering and obviously I don't have access to their code. I'd like to add that you can upload several filetypes, images, videos and even *.stream. I wonder if this filetype could be exploited.

<https://imgur.com/a/ZW0kWT8>

Baskarhomecontrol - February 23, 2020, 11:39 am

I know a hex way ,inbox me

RootForce - February 23, 2020, 5:52 pm

(Feb 22, 2020 09:42 AM)leoniss Wrote: [\[CITE\]](#) It's a back-end filtering and obviously I don't have access to their code. I'd like to add that you can upload several filetypes, images, videos and even *.stream. I wonder if this filetype could be exploited.

There are a few ways of achieving your goal: magic numbers or hiding php code within a legit .jpg/.stream/etc. file.

Magic numbers are used in the beginning of a file to determine what a file's type is. You can read more about it on this wiki page: "wikipedia Magic_number_(programming)#In_files". Perhaps manipulating the magic numbers can lead to a successful file upload. You can use the "img_hdr" Python module to see if your magic number manipulation was successful.

Alternatively, you could try hiding PHP code within a legitimate media file's metadata as seen in this article: "hiding-php-code-in-image-files-revisited".

I'm unable to post links to the wiki pages or articles because I don't meet the 50 post requirement. Google the information in quotes to find the links that I'm talking about.