

Forum:[Hack Forums](#)

Thread: [Uploading a shell on sites error](#)

aNeek - May 2, 2020, 1:37 pm

So, my friend has tried to upload shells on sites he has permission to upload shells on.

What happens is the image will have embedded PHP code, but when he uploads, the image passes on and is uploaded fine.

But the image is uploaded, he doesn't know what to do as there's no code being executed.

The question is,

is this because the server detected the code? (very bad website, likely wouldnt detect the coode)

Or is something being done wrong

??¢??? - May 3, 2020, 9:29 am

(May 2, 2020 01:37 PM)aNeek Wrote: [\[CITE\]](#) So, my friend has tried to upload shells on sites he has permission to upload shells on.

What happens is the image will have embedded PHP code, but when he uploads, the image passes on and is uploaded fine.

But the image is uploaded, he doesn't know what to do as there's no code being executed.

The question is,

is this because the server detected the code? (very bad website, likely wouldnt detect the coode)

Or is something being done wrong

You can't just embed the code in an image without breaking the image.

Servers usually check the extension/mime-type before uploading. Anyway, if the extension is .jpg/png and you have an embedded PHP code it will never execute unless there is a specific backend code on the server that reads the image and you somehow end up breaking into that function.

If after uploading the shell, it shows a 404/500 error that usually means its being picked up by an antivirus/firewall or IDS running on the server.

aNeek - May 3, 2020, 1:37 pm

(May 3, 2020 09:29 AM)??¢??? Wrote: [\[CITE\]](#) You can't just embed the code in an image without breaking the image.

Servers usually check the extension/mime-type before uploading. Anyway, if the extension is .jpg/png and you have an embedded PHP code it will never execute unless there is a specific backend code on the server that reads the image and you somehow end up breaking into that function.

If after uploading the shell, it shows a 404/500error that usually means its being picked up by an antivirus/firewall or IDS running on the server.

Appreciate the help.

