

Forum:[Hack Forums](#)

Thread: [apache deny access to a folder failed](#)

heropage - October 29, 2013, 7:24 pm

my site just got hacked.

I have a site where user can upload photo.
in my httpd.conf file.

I use

Quote:<Directory /var/www/html/photo>

Order Deny,Allow

Deny from All

</Directory> to block access to photo folder directly.

It works fine for most users.

But for some reason, some hacker still be able to access this folder.

He uploaded a gif file which contains php codes and execute it

<http://mysite/photo/123.gif>

and my site get hacked.

I guess he use some software to bypass apache.

Also weird thing is : I can not find the log from the apache access log.

But I can see it in the error log, because there are some php warning error .

Quote:[error] [client 113.1.1.1] PHP Warning: Unexpected character in input: '\x01' (ASCII=1)
state=0 in /var/www/html/photo/123.gif : eval()'d code on line 1, referer: site.com

So 2 things:

1) how to block the photo folder completely. it looks like if user use browser, he got blocked. but if he use some software, he can access. any software can do this?

2)how come there is not server log in access_log? any software can do this?

L?c???? - October 29, 2013, 7:25 pm

He shelled your site sir, if you need help pm me.

SHADOW REALM - October 29, 2013, 11:41 pm

I remember someone posting somewhere that changing your HTTP method from GET/POST to something like KJAFD (Using Tamperdata) could bypass either the .htpasswd or .htaccess. Dont quote me on it as I can't remember 100% and I can't seem to find the thread

heropage - October 30, 2013, 10:05 am

(Oct 29, 2013 11:41 PM)SHADOW REALM Wrote: [\[CITE\]](#) I remember someone posting somewhere that changing your HTTP method from GET/POST to something like KJAFD (Using Tamperdata) could bypass either the .htpasswd or .htaccess. Dont quote me on it as I can't remember 100% and I can't seem to find the thread

i don't think Tamperdata can bypass htpasswd or htaccess

phlower - October 30, 2013, 11:39 am

(Oct 29, 2013 11:41 PM)SHADOW REALM Wrote: [\[CITE\]](#) I remember someone posting somewhere that changing your HTTP method from GET/POST to something like KJAFD (Using Tamperdata) could bypass either the .htpasswd or .htaccess. Dont quote me on it as I can't remember 100% and

I can't seem to find the threadchanging it to anything can possibly bypass it
<https://hackforums.net/showthread.php?tid=3392310>

SHADOW REALM - October 30, 2013, 10:45 pm

(Oct 30, 2013 11:39 AM)phlower Wrote: [\[CITE\]](#) changing it to anything can possibly bypass it
<https://hackforums.net/showthread.php?tid=3392310>

That's what I was thinking of and by the looks of that thread it seems your vuln. Test it just to see if you are though

heropage - October 31, 2013, 6:40 am

(Oct 30, 2013 10:45 PM)SHADOW REALM Wrote: [\[CITE\]](#) That's what I was thinking of and by the looks of that thread it seems your vuln. Test it just to see if you are though

live http header can only bypass .htaccess which use

Quote:<LimitExcept GET POST>

Order Allow,Deny

Deny from all

</LimitExcept>

it doesn't work if .htaccess use something like

Quote:AuthName Login

AuthType Basic

require valid-user

tehunseen - October 31, 2013, 6:44 am

What if you create a .htaccess file in the /var/www/html/photo/ directory which contains "deny from all"?

Also PM me your upload script, I can patch the vulnerability.

cheatson - October 31, 2013, 11:58 am

Check your site for local file inclusion vulns mate!

<https://hackforums.net/showthread.php?tid=3837733>

heropage - October 31, 2013, 7:40 pm

(Oct 31, 2013 11:58 AM)cheatson Wrote: [\[CITE\]](#) Check your site for local file inclusion vulns mate!
<https://hackforums.net/showthread.php?tid=3837733>

i think it's a good direction!

my site is a clipshare video site.

it has inclusion vulns.

But BTW, I inject a php into a jpg file, and it looks like it doesn't run the php codes.

I have tried edjpgcom and Exif editor.

I also tried this

Quote:copy google.gif /b + phpinfo.php /a phpinfo.gif the image still not running php codes.