

Forum:[Hack Forums](#)

Thread: [\[TUT\]\[PIC\] UPload shell in mybb and wordpress and Hack via simlink \[TUT\]](#)

nck0099 - March 7, 2013, 5:47 am

Hie Hf it is my first tut here i hope it will help some noobs :

Lets Start:

Here I will use my site just to show you how u can upload shell in mybb sites:

Go to the admin panel :site.com/admin:

[IMG]<http://imageshack.us/a/img839/1459/70609712.jpg>[/IMG]

username:ImNotGoing To show here

pass:yourpass

Now we are inside the mybb control panel:

[IMG]<http://imageshack.us/a/img856/6643/90927372.jpg>[/IMG]

Now go to >>Themes and Style

and import this xml file:

Code <http://hackerstown.com/hackerstownxml.zip>

[IMG]<http://imageshack.us/a/img195/2928/84269503.jpg>[/IMG]

and click on [b]Import Theme:[/b]

[IMG]<http://imageshack.us/a/img213/8443/53553497.jpg>[/IMG]

you will see this page:

[IMG]<http://imageshack.us/a/img594/8862/89605231.jpg>[/IMG]

One your xml file imported successfully go to the main page and click on usercp and click on edit option:

[IMG]<http://imageshack.us/a/img152/3519/36470787.jpg>[/IMG]

and now select your uploaded xml:

[IMG]<http://imageshack.us/a/img594/3377/69434754.jpg>[/IMG]

now you will see this up loader:

[IMG]<http://imageshack.us/a/img22/7540/20628871.jpg>[/IMG]

upload your shell and browse :

[IMG]<http://imageshack.us/a/img547/7914/58809002.jpg>[/IMG]

Lets do some Hacking With symlink:

Click on symlink :

[IMG]<http://imageshack.us/a/img827/5995/128ss.jpg>[/IMG]

you will see the list of all the website hosted on the same server :

[IMG]<http://imageshack.us/a/img690/4166/45665620.jpg>[/IMG]

select your target website :

I'm selection a wordpress site :

click on symlink at the right side to the domain name:

you will see something like this:

[IMG]<http://imageshack.us/a/img59/4708/62702259.jpg>[/IMG]

now click on wp-config.php /*it is for wordpress */

you will see the database name , username ,host and pass in wp-config.php note the details and click on tools over the upper side of your shell you will see a page something like this:

[IMG]<http://imageshack.us/a/img826/4498/51674594.jpg>[/IMG]

Fill it with the details u got from wp-config.php

it will change the password of the admin panel:

Once your password has been changed login into the admin panel here:

target_site_.com/wp-admin

and now go to the Appearance and edit theme:

[IMG]<http://imageshack.us/a/img823/1232/41726899.jpg>[/IMG]

select theme Im selecting twentytwelve now edit 404 Template
(404.php) and paste your shell here:

[IMG]<http://imageshack.us/a/img811/3885/60586358.jpg>[/IMG]

and now browse your shell here:

Quote:target_site_.com/wp-content/themes/twentytwelve/404.php

I hope you understand have any question regarding security pm me.

In next tut i will show u how you can prevent your site from simlink:

Thankyou

Frankstein - March 7, 2013, 5:53 am

Nice tutorial but old, however its good to demonstrate for noobs how shell uploading works

01001 - March 7, 2013, 7:47 am

I appreciate you efforts but to upload a shell, first we have to get access to ADMIN PANEL. :P

Codevade - March 7, 2013, 7:50 am

(Mar 7, 2013 08:47 AM)01001 Wrote: [\[CITE\]](#) I appreciate your efforts but to upload a shell, first we have to get access to ADMIN PANEL. :P Well yes. But his tutorial comes into play when you're only able to exploit a target via SQLI at which point you can query to add another admin to MyBB and proceed to upload a shell.

VipVince - March 7, 2013, 8:08 am

I prefer to symlink manually. You tend to learn more rather than relying on a click click from a tool made by somebody else.

Codevade - March 7, 2013, 8:20 am

(Mar 7, 2013 09:08 AM)VipVince Wrote: [\[CITE\]](#) I prefer to symlink manually. You tend to learn more rather than relying on a click click from a tool made by somebody else. Indeed. Once you understand something and how it works. You have much more control over what you're doing when done manually.

h41fd0ll4r - March 7, 2013, 8:59 am

Symlinking manually is nothing more than a few commands. Rather just have a script that'll get it done faster tbh.

nck0099 - March 7, 2013, 9:08 am

(Mar 7, 2013 09:08 AM)VipVince Wrote: [\[CITE\]](#) I prefer to symlink manually. You tend to learn more rather than relying on a click click from a tool made by somebody else.
you know i can post some detailed tut about symlink but i can not post more than 15 pics so?... btw it is just for nobs only lots of tut abt smlnk already posted here

7snovic - March 7, 2013, 1:30 pm

very gud ;) thnx bro

respect =)??????????????

tux1 - March 8, 2013, 7:01 am

Nice tutorial, thanks alot for sharing!