

Forum:[Hack Forums](#)

Thread: [\[TUT\]How To Change Admin Password in Wordpress From DB & Hack the websites](#)

Twilight - January 3, 2013, 11:45 am

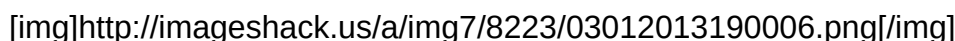
Hi Guys Today i'm showing you how to hack other websites on the same server of your uploaded shell that use WordPress script

1st of all you have to upload the Symlink tool

if you don't know this tool visit this [thread](#)

2nd after using the symlink tool (bypassing server protection) you will have the permission to explore the server websites

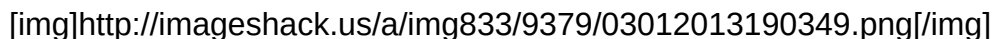
`http://[your site]/sym/root/`



go to the adress bar on you explorer and write

`http://[your site]/sym/root/home/etc/passwd`

to explore the server users



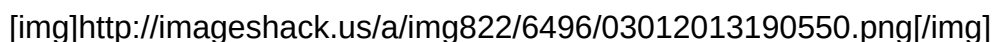
now go to bing.com

and put [ip:184.142.162.79 powered by wordpress] the server ip

to target the websites on this server that uses the wp script

i have as a target this website ==> <http://dgmates.com/>

i will try to find the user and try to explore it on my web browse



so the user is [dgmates]

now on the adress bar add

Quote:[home/dgmates/public_html/]

afte

Quote:[http://\[your site\]/sym/root/](http://[your site]/sym/root/)

the full link will be like this

Quote:[http://\[your site\]/sym/root/home/dgmates/public_html/](http://[your site]/sym/root/home/dgmates/public_html/)

now go to [wp-config.php] and click on it

[img]<http://imageshack.us/a/img248/6290/03012013190645.png>[img]

and you will see the database information

[img]<http://imageshack.us/a/img10/1803/03012013191107.png>[img]

LevelUp - January 3, 2013, 12:02 pm

Chances of them finding a shell: Meh

Chances of them noticing you've changed the password: Oh dear god..

Twilight - January 3, 2013, 12:03 pm

3rd go to your shell and click on SQL Manager

enter the information that you have got from the wp-config.php

PHP Code

```
<?php
```

```
/** The name of the database for WordPress */
```

```
define('DB_NAME', 'DBname');
```

```
/** MySQL database username */
```

```
define('DB_USER', 'VictimUser');
```

```
/** MySQL database password */
```

```
define('DB_PASSWORD', 'VictimPass');
```

```
/** MySQL hostname */
```

```
define('DB_HOST', 'localhost');
```

and click connect

[img]<http://imageshack.us/a/img441/4314/03012013191303.png>[img]

you will have something like that

[img]<http://imageshack.us/a/img11/615/03012013191435.png>[img]

at the end of home table you will see [wp_users] click on it

[img]<http://imageshack.us/a/img803/219/03012013192657.png>[img]

and you will see this

[img]http://imageshack.us/a/img210/3757/03012013193043.png[/img]

on [Table wp_users] the first ID user_login must be the admin

Code first ID = 1

User login = pain

go to Action and click Edit

[img]http://imageshack.us/a/img14/7209/03012013193841.png[/img]

you need to make a hash md5

go here

<http://www.miraclesalad.com/webtools/md5.php>

and generate your md5 Hash

for example :

your string = hkfrm

the hash md5 will be = 23db8571d53cefee83138ea095016bb9

i will use my hash now and change the ex hash on the wp DB

[img]http://imageshack.us/a/img705/2140/03012013194859.png[/img]

change it and save by clicking on confirm

[img]http://imageshack.us/a/img543/6964/03012013200115.png[/img]

again confirm with yes

before changing the hash save it first because we need change it back ,when we upload a shell (if we want to upload a shell)

now go to your target website

[http://\[target-site\]/wp-admin/](http://[target-site]/wp-admin/)

and i will log using

user login = pain

password = hkfrm (i have generate a hash md5 for this string)

[img]http://imageshack.us/a/img823/4391/03012013200306.png[/img]

so we have logged to the dashboard

[img]http://imageshack.us/a/img835/3839/03012013200342.png[/img]

now if you want hack the site just go to

appearance => editor =====> chose the file Index.php

then put your defacement index codes in php

and click update file

[img]http://imageshack.us/a/img845/7461/03012013201103.png[/img]

congratulation the website has been officially defaced

If you enjoyed this tutorial please leave a comment and say thanks I spent time making this ;)

if you want to get the tools used on my TUT leave a comment

rvltr - January 3, 2013, 12:26 pm

if you had half a brain you would atleast make a note of the original pass then change it back once youve got a shell up on the site.

Ainubbluez - January 3, 2013, 12:39 pm

@OP

T'es français ?? :) moi oui ^^

TwilighT - January 3, 2013, 12:39 pm

(Jan 3, 2013 01:26 PM)rvltr Wrote: [\[CITE\]](#) if you had half a brain you would atleast make a note of the original pass then change it back once youve got a shell up on the site.

yes you can do that even if you don't have a brain :p

or you can add another user that have the same permission to the admin :)

(Jan 3, 2013 01:39 PM)Ainubbluez Wrote: [\[CITE\]](#) @OP

T'es français ?? :) moi oui ^^

nn chui un algerien :) c'est pour ça j'utilise la langue française ;)

rvltr - January 3, 2013, 12:48 pm

(Jan 3, 2013 01:39 PM)TwilighT Wrote: [\[CITE\]](#) yes you can do that even if you don't have a brain :p

or you can add another user that have the same permission to the admin :)

nn chui un algerien :) c'est pour ça j'utilise la langue française ;)

correction sir.

adding another user with the same perms is just another way to get caught, and a much easier way to get yourself caught and noticed.

you are best off changing the existing pass to your own, upping a shell, then changing the pass back, you have less of a chance of your infiltration being exposed this way.

[UÇK] - January 3, 2013, 12:48 pm

hauahu symlink ahuah is simple! i know all methods!

but nice tut! :)

Noah™ - January 3, 2013, 1:05 pm

(Jan 3, 2013 01:48 PM)#rdp Wrote: [\[CITE\]](#) hauahu symlink ahuah is simple! i know all methods! but nice tut! :)
by the looks of you. You know about 2 methods all involving tools doing the John for you. Faggot

Twilight - January 4, 2013, 1:28 am

(Jan 3, 2013 01:48 PM)rvltr Wrote: [\[CITE\]](#) correction sir.
adding another user with the same perms is just another way to get caught, and a much easier way to get yourself caught and noticed.

you are best off changing the existing pass to your own, upping a shell, then changing the pass back, you have less of a chance of your infiltration being exposed this way.

maybe you are right but when you have shell on the server it's done you can inject the whole server to return another time ,and this website don't care about being caught because you have the config information and you can inject a shell from PHPMyAdmin ;)

(Jan 3, 2013 01:48 PM)#rdp Wrote: [\[CITE\]](#) hauahu symlink ahuah is simple! i know all methods! but nice tut! :)
okay symlink it is simple but he want work right at all time ;)