

Forum:[Hack Forums](#)

Thread: [\[BlackHat Administrators:\]> _ WordPress Hacking: Training Course _ \[/NO Experience Req.\]](#)

mObile - March 31, 2015, 8:22 pm

[img]<http://i.minus.com/iqBEIolXKoZd0.gif>[/img]

[img]<http://www.techexquisite.com/wp-content/uploads/2015/03/WordPress-plugins.png>[/img]

[img]<http://i.minus.com/iqBEIolXKoZd0.gif>[/img]

Last year I posted this thread.

Quote:[\[TUTORIAL:\]> _ HACK WORDPRESS WEBSITES _ \[/NO Experience Required!\]](#)

A method used to hack vulnerable WordPress websites that uses the popular revolution slider plugin.

Here's some details about the WordPress Slider Revolution Vulnerability Exploit:

Quote:

<http://blog.sucuri.net/2014/09/slider-revolution-plugin-critical-vulnerability-being-exploited.html>

To be honest i did not explain the FULL details on how to fully exploit this vulnerability because it was somewhat private so I thought I would teach some of you this method from my online training course thread.

Quote:[\[BlackHat Administrators:\]> _ WordPress Hacking: \[ONLINE\] Training Course _ \[/LEET/UB3R\]](#)

Enough time has passed and I've had this tutorial laying around so I'd thought I'd share it with everyone. ?

You do not need ANY experience in website hacking to do this, just follow my step-by-step instructions and you will get to experience the rush of hacking into a website/server. (if you don't already)

NOTE: I wrote this tutorial months ago so some the demonstration sites in this tutorial may have been patched. =/

Hacking is illegal, so taking the risk is entirely up to you, I take no responsibility.

Ok before we began you need to protect your IP# from being logged by the server your about to hack into, for this were gonna need a proxy/VPN (Virtual Private Network) I'd suggest using Tor if you have it, if not I would use Hotspot Shield. (it's free)

Quote: <https://www.hotspotshield.com/>

IP Test:

Quote:<http://whatismyipaddress.com/>

To Test your IP, Turn on your proxy/VPN and refresh the page above, if your IP# changes your good. If not try again until it does.

[img]http://i.minus.com/iqBEIolXKoZd0.gif[/img]

Ok now that you changed your IP# Let's do this shit. ?

Tutorial:

1.) If you are a member on my website hacking tool box, open the "Mass Revslider Exploiting Tool"

Quote:<https://hackforums.net/showthread.php?tid=3911852>

Hosted link for non members:

Quote:[Mass Revslider Exploiting Tool](#)

USAGE OVERVIEW:

Quote:<https://hackforums.net/showthread.php?tid=4465534>

2.) Click on "Exploiter" and enter this website URL and then click "Exploit Button":

PHP Code

<?php

<http://www.maaleadumim.org/>

Ok see the DB Host:

PHP Code

<?php

<mysql.maaleadumim.org>

That's the backend to the database on this site.

3.) Go to:

PHP Code

<?php

<mysql.maaleadumim.org>

And login with the provided login information.

4.) Ok we are now logged in through the phpmyadmin database. From here we need to find where the administrators login information is, to do that under Database click on [maaleadumim_org\(15\)](#) and locate [wp_cfsau2_users](#) and click Browse.

5.) Next click Edit next to admin name and copy the password hash in a notepad because you're gonna need it later.

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

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

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

7.)Ok now that, that's done, let's login at:

PHP Code

```
<?php
```

<http://www.maaleadumim.org/wp-login.php>

Enter admin and your password to login to Dashboard.

8.)Awesome job! You're doing great! 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/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 Go and logout. Now everything is back to normal, but he now have our shell on the site. ?

Want More..?

To find more sites using this vulnerable plugin, enter one of these dorks in google search. Some are private so please do not share outside of group.

PHP Code

```
<?php
```

inurl:wp-content

inurl:wp-content/themes/

inurl:wp-content inurl:revslider

inurl:wp-content intext:revslider.php

inurl:wp-content intext:revslider_front.php

inurl:wp-content intext:revslider.php site:il

inurl:/themes/WP-Smartcheck

inurl:/themes/stendhal

inurl:/theme/templates/sliders

inurl:/themes/RoyalOak

inurl:/themes/celestino2

inurl:/plugins/dnd-shortcodes

inurl:/themes/incrediblewp

inurl:/themes/celestino

inurl:/plugins/meteor-extras

inurl:/themes/bazar

inurl:/themes/cheope

inurl:/themes/aziza

inurl:/themes/LaBomba

inurl:/themes/Studiofolio

inurl:/themes/Jupiter

Then gather a few URL's and enter them in to the Mass Revslider Exploiting Tool

When you find one with a DB Host: mysql.URL you should be able to login, if you see localhost you could try to connect to the server from your shell, via SQL Browser. This does not work on every server.

1.) Open shell and click SQL
2.) Enter the login info and the server IP. You can get the server IP by clicking on Domains 2 IP in the Exploit tool.

3.) If and when you connect, to change the password like the phpmyadmin from your shell, enter this code:

PHP Code

```
<?php  
UPDATE `DATABASE NAME`.`wp_users` SET `user_pass` = 'PASSWORD' WHERE `wp_users`.  
`.`ID` =1;
```

And edit:

DATABASE NAME = Enter Database Name here

PASSWORD = Enter your MD5 password here

Then click Execute

EXAMPLE:

I'm sure some of you don't have a uploaded shell so I'm going to host DBKiss (MySQL Connect) for you to use.

Hosted Link:

PHP Code

```
<?php
```

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

That's about all I know on this exploit, here's some vulnerable sites you can test on

PHP Code

```
<?php
```

<http://www.gromosapien.com/>

<http://stars-source.com/>

<http://hippityhopcreative.com/>

These are just a few, there are thousands, just have to put in the time to find them because I'm up to

150 shelled servers and finding more everyday, so don't say this method does not work because it works quite well for me or I would not waste my time posting this tutorial. Well that's about it, I hope you had a fun journey hacking into a web server as much as I enjoyed writing this tutorial. Thanks for reading on how easy it is to hack random WordPress websites. ?

Shout out's to all BlackHat Administrators members \m/

Yas3r - April 1, 2015, 2:26 pm

As usual you rock :D - Great Tutorial thanks

Deadbyte - April 1, 2015, 2:28 pm

Extremely HQ, thanks for posting this.

thisguy1234 - April 1, 2015, 3:18 pm

thanks mate

just wondering about the shell. How would one go about changing the password, just replace auth_pass?

cdange - April 1, 2015, 5:12 pm

Excellent tutorial! You rocks man!

Thank you

knightserv - April 2, 2015, 3:42 am

love it want to know how can i get the Tools...I cannot pm you...

Xierz - April 2, 2015, 5:08 am

Damn, this is a really good tutorial! Thanks alot mate!

Hydraulic - April 2, 2015, 5:12 am

Very high quality thread, good job and thank you for sharing this with us all.

SH?D? - April 2, 2015, 1:28 pm

can it grab www.duelingnetwork.com try for it

wranx - April 2, 2015, 1:46 pm

Great tutorial! Definitely helpful.

YouMakeMeHue - April 2, 2015, 2:26 pm

HOW THE FUCK IS THE OP NOT DEAD YET??

Judicar - April 3, 2015, 6:30 am

Link to a Mass Revslider Exploiting Tool won't work

bradjose - July 5, 2015, 11:37 pm

you bro rock :) Thanks alot mate!

cheatson - July 6, 2015, 11:55 am

Missed this of yours mobile, yet another detailed thread would expect nothing less!

Th3PonyWizard - July 6, 2015, 1:00 pm

(Jul 6, 2015 11:55 AM)cheatson Wrote: [\[CITE\]](#) Missed this of yours mobile, yet another detailed thread would expect nothing less!it takes quite a skill single-handedly killing a section

edit:spelling

moonheart08 - *July 14, 2015, 6:08 pm*

Site broke :/ shame, I wanted to do this

dunkey - *July 15, 2015, 4:45 am*

Thanks dude really HQ tut

blacksarge01 - *July 15, 2015, 7:06 am*

i need a account for that dude... And the site says, i have your IP i send it to my Email.

Mr. Corleone - *September 22, 2016, 12:22 am*

Excellent and HQ thread from you as always.

I have a question tho, the hosted linkon dogankagit does not work anymore, could you re-upload it?
Thanks!

OxaByte - *July 26, 2017, 10:17 am*

You are pro blackhat . I Appreciate your work and i am now your fan. Thanks for the tutorial.

Younis Khan - *July 26, 2017, 11:49 am*

why big bump so big oh mayne

Lextian - *May 2, 2019, 9:51 pm*

Great post and very useful to me.

tintinkool - *May 4, 2019, 12:26 pm*

wanted to check for own site. but link not working.