

Forum:[Hack Forums](#)

Thread: [\[HOSTING:\]>_ WordPress Mass Revslider Exploiting Tool _\[/HACK WORDPRESS WEBSITES\]](#)

mObile - September 27, 2014, 8:43 pm

WordPress Slider Revolution Vulnerability Exploit:
Slider Revolution Premium WordPress Plugin that allows a remote attacker to download any file from the server.

Quote:

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

In my previous thread I help explain how easy it was to hack multiple WordPress websites through some vulnerable themes.

As you may already know the database password rarely matched the WordPress admin's password. =/

[TUTORIAL:]>_ HACK WORDPRESS WEBSITES _[/NO Experience Required!]

Quote:<https://hackforums.net/showthread.php?tid=4445583>

Here's a simple .php script Coded By AMir dZ 52 and Modified & Hosted by me help you exploit it even more. ?

Here's how it works:

First Click on "Exploit Dorks" tab and choose a dork to search on Google.

EXAMPLE:

Next click "Exploiter" tab and copy/paste multiple URL's from google and click on "Exploit" to scan for vulnerable WordPress sites. If infected it will display:

PHP Code

```
<?php
```

DB_Name:

DB_User:

DB_Pass:

DB_Host:

Now that you have the MySQL database information click on "Find DB Panel" and you can try to locate the login panel.

Currently scans:

PHP Code

```
<?php
```

```
$list = array(
```

```
    '/phpMyAdmin/',
```

'/phpmyadmin/',
'/PMA/',
'/pma/',
'/admin/',
'/wp-login.php',
'/dbadmin/',
'/DB_ADMIN/',
'/db_admin/',
'/DBA/',
'/SQLI/',
'/dba/',
'/sqli/',
'/mysql/',
'/myadmin/',
'/phpmyadmin2/',
'/phpMyAdmin2/',
'/phpMyAdmin-2/',
'/php-my-admin/',
'/phpMyAdmin-2.2.3/',
'/phpMyAdmin-2.2.6/',
'/phpMyAdmin-2.5.1/',
'/phpMyAdmin-2.5.4/',
'/phpMyAdmin-2.5.5-rc1/',
'/phpMyAdmin-2.5.5-rc2/',
'/phpMyAdmin-2.5.5/',
'/phpMyAdmin-2.5.5-pl1/',
'/phpMyAdmin-2.5.6-rc1/',

'/phpMyAdmin-2.5.6-rc2/',
'/phpMyAdmin-2.5.6/',
'/phpMyAdmin-2.5.7/',
'/phpMyAdmin-2.5.7-pl1/',
'/phpMyAdmin-2.6.0-alpha/',
'/phpMyAdmin-2.6.0-alpha2/',
'/phpMyAdmin-2.6.0-beta1/',
'/phpMyAdmin-2.6.0-beta2/',
'/phpMyAdmin-2.6.0-rc1/',
'/phpMyAdmin-2.6.0-rc2/',
'/phpMyAdmin-2.6.0-rc3/',
'/phpMyAdmin-2.6.0/',
'/phpMyAdmin-2.6.0-pl1/',
'/phpMyAdmin-2.6.0-pl2/',
'/phpMyAdmin-2.6.0-pl3/',
'/phpMyAdmin-2.6.1-rc1/',
'/phpMyAdmin-2.6.1-rc2/',
'/phpMyAdmin-2.6.1/',
'/phpMyAdmin-2.6.1-pl1/',
'/phpMyAdmin-2.6.1-pl2/',
'/phpMyAdmin-2.6.1-pl3/',
'/phpMyAdmin-2.6.2-rc1/',
'/phpMyAdmin-2.6.2-beta1/',
'/phpMyAdmin-2.6.2-rc1/',
'/phpMyAdmin-2.6.2/',
'/phpMyAdmin-2.6.2-pl1/',
'/phpMyAdmin-2.6.3/',

'/phpMyAdmin-2.6.3-rc1/',
'/phpMyAdmin-2.6.3/',
'/phpMyAdmin-2.6.3-pl1/',
'/phpMyAdmin-2.6.4-rc1/',
'/phpMyAdmin-2.6.4-pl1/',
'/phpMyAdmin-2.6.4-pl2/',
'/phpMyAdmin-2.6.4-pl3/',
'/phpMyAdmin-2.6.4-pl4/',
'/phpMyAdmin-2.6.4/',
'/phpMyAdmin-2.7.0-beta1/',
'/phpMyAdmin-2.7.0-rc1/',
'/phpMyAdmin-2.7.0-pl1/',
'/phpMyAdmin-2.7.0-pl2/',
'/phpMyAdmin-2.7.0/',
'/phpMyAdmin-2.8.0-beta1/',
'/phpMyAdmin-2.8.0-rc1/',
'/phpMyAdmin-2.8.0-rc2/',
'/phpMyAdmin-2.8.0/',
'/phpMyAdmin-2.8.0.1/',
'/phpMyAdmin-2.8.0.2/',
'/phpMyAdmin-2.8.0.3/',
'/phpMyAdmin-2.8.0.4/',
'/phpMyAdmin-2.8.1-rc1/',
'/phpMyAdmin-2.8.1/',
'/phpMyAdmin-2.8.2/',
'/sqlmanager/',
'/mysqlmanager/,'

'/p/m/a/',
'/PMA2005/',
'/pma2005/',
'/dev/',
'/phpmanager/',
'/php-myadmin/',
'/phpmy-admin/',
'/webadmin/',
'/sqlweb/',
'/websql/',
'/webdb/',
'/mysqladmin/',
'/mysql-admin/',
'/mya/',
'/PhpMyAdmin/',
'/phpmyadmin/',
'/myadmin/',
'/mysql/',
'/sql/',
'/server/',
'/db/',
'/database/',
'/databases/',
'/adm/',
'/configuration/',
'/configure/',
'/administrator/',

'/login/',
'/moderator/',
'/controlpanel/',
'/adminpanel/',
'/admincontrol/',
'/fileadmin/',
'/data/',
'/postgresql/',
'/oracle/',
'/mssql/',
'/msaccess/',
'/sysadmin/',
'/serverdata/',
'/webadmin/',
'/admins/',
'/Database_Administration/',
'/WebAdmin/',
'/useradmin/',
'/sysadmins/',
'/admin1/',
'/system-administration/',
'/administrators/',
'/pgadmin/',
'/directadmin/',
'/staradmin/',
'/ServerAdministrator/',
'/SysAdmin/,'

'/administer/',
'/LiveUser_Admin/',
'/sys-admin/',
'/typo3/',
'/panel/',
'/xlogin/',
'/smblogin/',
'/phpldapadmin/',
'/server_admin/',
'/database_administration/',
'/system_administration/',
'/ss_vms_admin_sm/',
'/adminarea/',
'/MySQL/',
'/mysql_admin/',
'/server_data/',
'/DB/',
'/DB1/',
'/DB2/',
'/DB3/',
'/DB4/',
'/DB5/',
'/DB6/',
'/DB7/',
'/DB8/',
'/DB9/',
'/DB0/',

'db1/',
'db2/',
'db3/',
'db4/',
'db5/',
'db6/',
'db7/',
'db8/',
'db9/',
'db0/',
'mysql5/',
'mysql4/',
'root/',
'apache/',
'php/',
'Apache/',
'Php/',
'apach/',
'apachepanel/',
'WEBSERVERS/',
'DATABASE1/',
'DATABASE2/',
'DATABASE3/',
'DATABASE4/',
'DATABASE5/',
'DATABASE6/',
'DATABASE7/',

```
'/DATABASE8',  
  
'/DATABASE9',  
  
'/WEBDATA',  
  
'/WEB_DATA',  
  
'/webservers',  
  
'/database1',  
  
'/database2',  
  
'/database3',  
  
'/database4',  
  
'/database5',  
  
'/database6',  
  
'/database7',  
  
'/database8',  
  
'/database9',  
  
'/webdata',  
  
'/web_data',  
  
);
```

Some other added features to help you along.

?Hosted Link:

Quote:<http://www.dogankagit.com/toksel/revpress.php>

Good Luck and Thanks for viewing my thread. ?

Hooded Robin - September 27, 2014, 9:03 pm

no shouts when i posted a py exploit script for this vuln on your other original posting :(

PS - you can turn it into a very high success rate for WP admin panel compromise, if you follow some good advice from here:

<http://blog.spiderlabs.com/2014/09/leveraging-lfi-to-get-full-compromise-on-wordpress-sites.html>

(use your brain and you can see how this vuln and this writeup relate.....hint hint wink wink, not just

for LFI)

Zlatane Ibrahimovique - September 27, 2014, 9:18 pm

Great contribution Sir!

Thanks for this :)

*****W0lf***** - September 28, 2014, 1:37 am

Thanks for sharing this useful site-tools Sir!

Hunger - September 28, 2014, 11:34 am

Thanks for sharing this OP, useful tool :D

Nitai - September 28, 2014, 12:49 pm

Thanks for sharing this tool, HQ Member !

Bibl - September 28, 2014, 5:35 pm

I love it i love it i love it very HQ :DDDDDD

Drøm - September 28, 2014, 5:45 pm

Yeah, they can download files from the server but what damage is that going to cause. Except they would only have the ability to rip a template or plugin but I can't see this as a massive threat tbh.

Nigga From Africa - September 28, 2014, 10:07 pm

(Sep 28, 2014 05:45 PM)Canterbury Bulldogs Wrote: [\[CITE\]](#) Yeah, they can download files from the server but what damage is that going to cause. Except they would only have the ability to rip a template or plugin but I can't see this as a massive threat tbh.

Download the config

Find the pma and boom db access.

Drøm - September 28, 2014, 11:28 pm

(Sep 28, 2014 10:07 PM)Death0x Wrote: [\[CITE\]](#) Download the config

Find the pma and boom db access.

Depends on what kind of version of WP you're using.

Nigga From Africa - September 29, 2014, 1:21 am

(Sep 28, 2014 11:28 PM)Canterbury Bulldogs Wrote: [\[CITE\]](#) Depends on what kind of version of WP you're using.

It all depends on if you can find the phpmyadmin login.

You dont really know what you're talking about do you?

Drøm - September 29, 2014, 1:36 am

(Sep 29, 2014 01:21 AM)Death0x Wrote: [\[CITE\]](#) It all depends on if you can find the phpmyadmin login.

You dont really know what you're talking about do you?

Didn't you here? It was silently patched which means the creator of the "vulnerable plugin" patched it without prior notice when he noticed his plugin had a PHP vuln.

I do know what I am talking about since I read my news before coming to conclusions.

With cpanel accounts Mysql logins will always require said user to be logged onto their actual Cpanel account.

I have used Cpanel alot. And I am an ex hacker.

Nigga From Africa - September 29, 2014, 2:24 am

(Sep 29, 2014 01:36 AM)Canterbury Bulldogs Wrote: [\[CITE\]](#) Didn't you here? It was silently patched which means the creator of the "vulnerable plugin" patched it without prior notice when he noticed his plugin had a PHP vuln.

I do know what I am talking about since I read my news before coming to conclusions.

With cpanel accounts Mysql logins will always require said user to be logged onto their actual Cpanel account.

I have used Cpanel alot. And I am an ex hacker.

Okay no you have no idea what you're talking about.

Im on phone so just brief.

You use the vuln to download a config file.

Config file have database info.

If remote login is enabled just connect

If not you search for phpmyadmin login.

If you're an ex hacker i assume all you could do was use havij.

Drøm - September 29, 2014, 2:53 am

(Sep 29, 2014 02:24 AM)Death0x Wrote: [\[CITE\]](#) Okay no you have no idea what you're talking about.

Im on phone so just brief.

You use the vuln to download a config file.

Config file have database info.

If remote login is enabled just connect

If not you search for phpmyadmin login.

If you're an ex hacker i assume all you could do was use havij.

Only skids use Havij you being the skid

Remote SQL would only be available if you have access to the remote session which you wouldn't

You are horrible with knowledge on "SQL and hacking".

You are speaking nonsense now.

Nigga From Africa - September 29, 2014, 3:13 am

(Sep 29, 2014 02:53 AM)Canterbury Bulldogs Wrote: [\[CITE\]](#) Only skids use Havij you being the skid

Remote SQL would only be available if you have access to the remote session which you wouldn't

You are horrible with knowledge on "SQL and hacking".

You are speaking nonsense now.

Holy shit im fucking laughing.

Why dont you fucking try this yourself?

Hooded Robin - September 29, 2014, 8:50 am

@canterbury In addition to mysql access or random dumb re-use of credentials, the wp-config.php file also contains the auth_key & auth_salt, these can be used to bruteforce cookies to gain admin

authenticated access, which from there makes shelling the site a matter of seconds in most cases. There are a number of ways this can be helpful, so stop being such a douche

SIM-1073426 - September 29, 2014, 5:22 pm

I made a program to check just how useful this 0day is. It basically scraped Google with a dork and tried to login to SQL and the admin panel. It scanned around 300-400 pages and it could connect to 2 SQL databases and 2 with normal admin login.

SIM-1073426 - September 30, 2014, 2:21 am

(Sep 28, 2014 11:28 PM)Canterbury Bulldogs Wrote: [\[CITE\]](#) Depends on what kind of version of WP you're using.

Actually it depends on if you're using a patched version of Revslider or not. The WP version is completely irrelevant.

indonesiamaju - October 5, 2014, 3:23 am

(Sep 27, 2014 08:43 PM)mObil3_xT Wrote: [\[CITE\]](#)

WordPress Slider Revolution Vulnerability Exploit:

Slider Revolution Premium WordPress Plugin that allows a remote attacker to download any file from the server.

In my previous thread I help explain how easy it was to hack multiple WordPress websites through some vulnerable themes.

As you may already know the database password rarely matched the WordPress admin's password. =/

[TUTORIAL:]>_ HACK WORDPRESS WEBSITES_[/NO Experience Required!]

Here's a simple .php script Coded By AMir dZ 52 and Modified & Hosted by me help you exploit it even more. ?

Here's how it works:

First Click on "Exploit Dorks" tab and choose a dork to search on Google.

EXAMPLE:

Next click "Exploiter" tab and copy/paste multiple URL's from google and click on "Exploit" to scan for vulnerable WordPress sites. If infected it will display:

PHP Code

```
<?php
```

DB_Name:

DB_User:

DB_Pass:

DB_Host:

Now that you have the MySQL database information click on "Find DB Panel" and you can try to locate the login panel.

Currently scans:

PHP Code

```
<?php
$list = array(

'/phpMyAdmin/',

'/phpmyadmin/',

'/PMA',

'/pma/',

'/admin/',

'/wp-login.php',

'/dbadmin/',

'/DB_ADMIN/',

'/db_admin/',

'/DBA',

'/SQLI/',

'/dba/',

'/sqli/',

'/mysql/',

'/myadmin/',

'/phpmyadmin2/',

'/phpMyAdmin2/',

'/phpMyAdmin-2/',

'/php-my-admin/',

'/phpMyAdmin-2.2.3/',

'/phpMyAdmin-2.2.6/',

'/phpMyAdmin-2.5.1/',

'/phpMyAdmin-2.5.4/',

'/phpMyAdmin-2.5.5-rc1/',

'/phpMyAdmin-2.5.5-rc2/',
```

'/phpMyAdmin-2.5.5/',
'/phpMyAdmin-2.5.5-pl1/',
'/phpMyAdmin-2.5.6-rc1/',
'/phpMyAdmin-2.5.6-rc2/',
'/phpMyAdmin-2.5.6/',
'/phpMyAdmin-2.5.7/',
'/phpMyAdmin-2.5.7-pl1/',
'/phpMyAdmin-2.6.0-alpha/',
'/phpMyAdmin-2.6.0-alpha2/',
'/phpMyAdmin-2.6.0-beta1/',
'/phpMyAdmin-2.6.0-beta2/',
'/phpMyAdmin-2.6.0-rc1/',
'/phpMyAdmin-2.6.0-rc2/',
'/phpMyAdmin-2.6.0-rc3/',
'/phpMyAdmin-2.6.0/',
'/phpMyAdmin-2.6.0-pl1/',
'/phpMyAdmin-2.6.0-pl2/',
'/phpMyAdmin-2.6.0-pl3/',
'/phpMyAdmin-2.6.1-rc1/',
'/phpMyAdmin-2.6.1-rc2/',
'/phpMyAdmin-2.6.1/',
'/phpMyAdmin-2.6.1-pl1/',
'/phpMyAdmin-2.6.1-pl2/',
'/phpMyAdmin-2.6.1-pl3/',
'/phpMyAdmin-2.6.2-rc1/',
'/phpMyAdmin-2.6.2-beta1/',
'/phpMyAdmin-2.6.2-rc1/',

'/phpMyAdmin-2.6.2/',
'/phpMyAdmin-2.6.2-pl1/',
'/phpMyAdmin-2.6.3/',
'/phpMyAdmin-2.6.3-rc1/',
'/phpMyAdmin-2.6.3/',
'/phpMyAdmin-2.6.3-pl1/',
'/phpMyAdmin-2.6.4-rc1/',
'/phpMyAdmin-2.6.4-pl1/',
'/phpMyAdmin-2.6.4-pl2/',
'/phpMyAdmin-2.6.4-pl3/',
'/phpMyAdmin-2.6.4-pl4/',
'/phpMyAdmin-2.6.4/',
'/phpMyAdmin-2.7.0-beta1/',
'/phpMyAdmin-2.7.0-rc1/',
'/phpMyAdmin-2.7.0-pl1/',
'/phpMyAdmin-2.7.0-pl2/',
'/phpMyAdmin-2.7.0/',
'/phpMyAdmin-2.8.0-beta1/',
'/phpMyAdmin-2.8.0-rc1/',
'/phpMyAdmin-2.8.0-rc2/',
'/phpMyAdmin-2.8.0/',
'/phpMyAdmin-2.8.0.1/',
'/phpMyAdmin-2.8.0.2/',
'/phpMyAdmin-2.8.0.3/',
'/phpMyAdmin-2.8.0.4/',
'/phpMyAdmin-2.8.1-rc1/',
'/phpMyAdmin-2.8.1/',

'/phpMyAdmin-2.8.2/',

'/sqlmanager/',

'/mysqlmanager/',

'/p/m/a/',

'/PMA2005/',

'/pma2005/',

'/dev/',

'/phpmanager/',

'/php-myadmin/',

'/phpmy-admin/',

'/webadmin/',

'/sqlweb/',

'/websql/',

'/webdb/',

'/mysqladmin/',

'/mysql-admin/',

'/mya/',

'/PhpMyAdmin/',

'/phpmyadmin/',

'/myadmin/',

'/mysql/',

'/sql/',

'/server/',

'/db/',

'/database/',

'/databases/',

'/adm/',

'/configuration/',
'/configure/',
'/administrator/',
'/login/',
'/moderator/',
'/controlpanel/',
'/adminpanel/',
'/admincontrol/',
'/fileadmin/',
'/data/',
'/postgresql/',
'/oracle/',
'/mssql/',
'/msaccess/',
'/sysadmin/',
'/serverdata/',
'/webadmin/',
'/admins/',
'/Database_Administration/',
'/WebAdmin/',
'/useradmin/',
'/sysadmins/',
'/admin1/',
'/system-administration/',
'/administrators/',
'/pgadmin/',
'/directadmin/',

'/staradmin/',
'/ServerAdministrator/',
'/SysAdmin/',
'/administer/',
'/LiveUser_Admin/',
'/sys-admin/',
'/typo3/',
'/panel/',
'/xlogin/',
'/smblogin/',
'/phpldapadmin/',
'/server_admin/',
'/database_administration/',
'/system_administration/',
'/ss_vms_admin_sm/',
'/adminarea/',
'/MySQL/',
'/mysql_admin/',
'/server_data/',
'/DB/',
'/DB1/',
'/DB2/',
'/DB3/',
'/DB4/',
'/DB5/',
'/DB6/',
'/DB7/',

'/DB8',
'/DB9',
'/DB0',
'/db1',
'/db2',
'/db3',
'/db4',
'/db5',
'/db6',
'/db7',
'/db8',
'/db9',
'/db0',
'/mysql5',
'/mysql4',
'/root',
'/apache',
'/php',
'/Apache',
'/Php',
'/apach',
'/apachepanel',
'/WEBSERVERS',
'/DATABASE1',
'/DATABASE2',
'/DATABASE3',
'/DATABASE4',

```
'/DATABASE5',  
'/DATABASE6',  
'/DATABASE7',  
'/DATABASE8',  
'/DATABASE9',  
'/WEBDATA',  
'/WEB_DATA',  
'/webservers',  
'/database1',  
'/database2',  
'/database3',  
'/database4',  
'/database5',  
'/database6',  
'/database7',  
'/database8',  
'/database9',  
'/webdata',  
'/web_data',  
);
```

Some other added features to help you along.

?Hosted Link:

Good Luck and Thanks for viewing my thread. ?

very good tools :)

i'll use the tools if i have the access to the site :)

Mvb101 - October 15, 2014, 9:49 am

(Sep 28, 2014 10:07 PM)DotTXT Wrote: [\[CITE\]](#) Download the config
Find the pma and boom db access.
great thought ?

didn't think about that

Dea7h - November 14, 2014, 2:13 pm

Hello please pm me my username and pass, thanks

Volcan - November 14, 2014, 6:37 pm

great job bro im waiting to see more and more from you

best regards

mats0o0o0

AMir dZ 52 - December 8, 2014, 1:06 pm

Wtfff This Shiit - _ -

this tool is real Coded By Me not you - _ - Noooooobs Everywhere !!!

dopeeboii - December 8, 2014, 2:17 pm

Can I get access to this, please :P

OBL1V10N - December 9, 2014, 12:31 pm

Well done on this post bro. ill check this out a report back

133720 - December 13, 2014, 5:47 am

Thanks for your effort bro :) I am your old friend 133720.

mahmudul006 - January 15, 2015, 6:10 am

awesome script..

but where is script download link

thanks in advance

knightserv - April 2, 2015, 4:11 am

where can i download the tools cuz i want to try it out...

knightserv - April 2, 2015, 4:13 am

awesome script..but where is script download link thanks in advance where can i download it

bradjose - July 5, 2015, 11:33 pm

give me script download link.

SliceOfAMoment - July 6, 2015, 3:35 pm

Can I get a copy of the script as well? Thanks :)

denio - July 7, 2015, 4:17 am

looking nice

can i get a copy of the script please?

dogankagit.com 'daki link çalışmıyor :(

you can found (i think) same script in youtube, you can see the link on google if u search
WordPress RevSlider File Upload and Execute Vulnerability keywords

YMIML123 - *March 13, 2016, 12:08 pm*

hi mobile i really need your help

acidgameing - *February 15, 2018, 8:17 am*

i need this omg i need this to test my website out ty

kamera - *February 16, 2018, 6:10 am*

Hi.

The download link doesn't seem to be working at the moment.