

Forum:[Hack Forums](#)

Thread: [wp-admin/admin-ajax.php exploit](#)

Skidy - March 13, 2015, 9:14 am

I've got a URL that displays a 0 when I go to this :

[www.examplewebsite.com/wp-admin/admin-ajax.php](#) | What is the exploit for this?

Delevingne - March 13, 2015, 9:15 am

I think it displays boolean(false) which equals to 0, because you are not administrator. I'm not sure tho.

Skidy - March 13, 2015, 9:17 am

(Mar 13, 2015 09:15 AM)D A L O Wrote: [\[CITE\]](#) I think it displays boolean(false) which equals to 0, because you are not administrator. I'm not sure tho.

yeah, I've tried the method where you put:

wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php and download their database but it doesn't work. Any other way of getting access?

(Mar 13, 2015 09:15 AM)D A L O Wrote: [\[CITE\]](#) I think it displays boolean(false) which equals to 0, because you are not administrator. I'm not sure tho.

in the source code it has this:

```
Code      <input type="submit" name="wp-submit" id="wp-submit" class="button button-primary
button-large" value="Log In" />
          <input type="hidden" name="redirect_to" value="https://example.org.uk/wp-admin/" />
          <input type="hidden" name="testcookie" value="1" />
```

This is on the login page.. Could I try and set the value to 1???

(Mar 13, 2015 09:15 AM)D A L O Wrote: [\[CITE\]](#) I think it displays boolean(false) which equals to 0, because you are not administrator. I'm not sure tho.

Oh and

```
Code /* <![CDATA[ */
var imgmap =
{"ajaxurl":"https://example.org.uk/wp-admin/admin-ajax.php","pulseOption":"first_time","admin_log
ged":"","alt_dialog":"1"};
/* ]]> */
```

So, could I do anything with this?

runnerup - March 13, 2015, 10:00 am

Try and find out what plugins the site is using then find exploits for those plugins.

[http://wppluginchecker . earthpeople . se/](#)

Sorry about the spaces I'm not allowed to post links.

Skidy - March 13, 2015, 10:03 am

(Mar 13, 2015 10:00 AM)runnerup Wrote: [\[CITE\]](#) Try and find out what plugins the site is using then find exploits for those plugins.

[http://wppluginchecker . earthpeople . se/](#)

Sorry about the spaces I'm not allowed to post links.

Any ideas on exploiting plugins?? How would I exploit them?

[img]http://screenshu.com/static/uploads/temporary/e1/tl/ia/i2kov9.jpg[/img]

Any exploits from those?

SIM-209986 - March 13, 2015, 11:36 am

Use wpscan in Kali Linux. Does the job. but make sure to update the database first.

Skidy - March 13, 2015, 11:58 am

(Mar 13, 2015 11:36 AM)?????. Wrote: [\[CITE\]](#) Use wpscan in Kali Linux. Does the job. but make sure to update the database first.

What do you mean update the database? And is there no way of using wpscan on Windows?

11ssx1 - March 13, 2015, 1:06 pm

(Mar 13, 2015 11:58 AM)benny_boy Wrote: [\[CITE\]](#) What do you mean update the database? And is there no way of using wpscan on Windows?

Try wpscan in kali .

or just search for it in win version .

may google be with you :)