

Forum:[Hack Forums](#)

Thread: [Wordpress Pass hashed, twice encryption](#)

naografix2 - April 10, 2015, 10:30 am

Hey !

I found an error with SQL Injection on the wordpress.

I found the table : wp_users and found the username and the password

But i think it encrypted twice because i have this :

\$P\$BdXICQzLr5ZLZAmrGokJ/clo6J1hDd1

Who can decode this for me ?

Thx !

IDK - April 10, 2015, 4:12 pm

umm ? " encrypted twice " I look like a normal wp hash to me

naografix2 - April 10, 2015, 4:26 pm

(Apr 10, 2015 04:12 PM)Random Nigga Wrote: [\[CITE\]](#) umm ? " encrypted twice " I look like a normal wp hash to me

Dunno, because i cant find the pass with md5 decode, well... i'm not sure it's a md5 hash :/

LittleBobbyTables - April 10, 2015, 4:29 pm

It's not an MD5 hash for sure.

Do you have a character set?

Or at least a length

Forezza - April 10, 2015, 4:31 pm

This is a normal Wordpress hash. I'll just clear a few things up for you.

1. Hashes cannot be decoded / decrypted, they're cracked. These decrypter sites are just large databases of hashes that you can cross compare with. You cannot do this with wordpress hashes because they contain salts.
2. Wordpress hashes are in simple terms, multiple iterations of MD5 hashes + salts with a few more steps added on. This makes them far slower to crack.

naografix2 - April 10, 2015, 4:41 pm

(Apr 10, 2015 04:31 PM)Forezza Wrote: [\[CITE\]](#) This is a normal Wordpress hash. I'll just clear a few things up for you.

1. Hashes cannot be decoded / decrypted, they're cracked. These decrypter sites are just large databases of hashes that you can cross compare with. You cannot do this with wordpress hashes because they contain salts.
2. Wordpress hashes are in simple terms, multiple iterations of MD5 hashes + salts with a few more steps added on. This makes them far slower to crack.

Ho okay ! Thx for this informations <3

But well, how can i find/crack the Password with/without this hash. Because i found the username, and i just found this Password.

How can i connect in this website in wp-admin page ?

Brute force ? ^^

HeXagone - April 10, 2015, 6:00 pm

you got the hash using Sql i don't know if it is still working but here is what you have to do :

get the email of the admin

go to wp-login.pph page and click on forgot password

enter the email and click on get new password

get the user_activation_key

wp-login.php?action=rp&key=resetkey&login=username

replace username and resetkey you got above.

hope it works

HeXagone

Soulo - April 10, 2015, 6:30 pm

(Apr 10, 2015 06:00 PM)HeXagone Wrote: [\[CITE\]](#) you got the hash using Sql i don't know if it is still working but here is what you have to do :

get the email of the admin

go to wp-login.pph page and click on forgot password

enter the email and click on get new password

get the user_activation_key

wp-login.php?action=rp&key=resetkey&login=username

replace username and resetkey you got above.

hope it works

HeXagone

This was patched in October of 2013...

<https://core.trac.wordpress.org/changeset/25696>

naografix2 - April 11, 2015, 3:49 am

(Apr 10, 2015 06:30 PM)Soulo Wrote: [\[CITE\]](#) This was patched in October of 2013...

<https://core.trac.wordpress.org/changeset/25696>

Arf, so it's impossible to have the wordpress Password with the hash ./ !