

Forum:[Hack Forums](#)

Thread: [Resetting WP password via SQLi vuln ?](#)

kuramiqko - May 30, 2020, 7:16 am

Hey guys, I would like to ask someone experienced with wordpress, lets say I have access to an database(s) with wordpress sites, and I can see the wp_users table with passwords and everything, is there any way to reset the password via the Forgotten password and then access reset token via the database which I have gained access via SQL injection vulnerability ?

Thanks for the help !

!!*-Ir0nMan™*-!! - May 30, 2020, 9:52 am

(May 30, 2020 07:16 AM)kuramiqko Wrote: [\[CITE\]](#) Hey guys, I would like to ask someone experienced with wordpress, lets say I have access to an database(s) with wordpress sites, and I can see the wp_users table with passwords and everything, is there any way to reset the password via the Forgotten password and then access reset token via the database which I have gained access via SQL injection vulnerability ?

Thanks for the help !

it was possible before but now reset key is hashed as well. If you can alter the sql records then it is possible otherwise not.

kuramiqko - May 30, 2020, 12:48 pm

(May 30, 2020 09:52 AM)!!*-Ir0nMan™*-!! Wrote: [\[CITE\]](#) it was possible before but now reset key is hashed as well. If you can alter the sql records then it is possible otherwise not. I googled around and it said it was hashing the user activation key or I did not understand right ? If is that so, can I just hash the encryption key and get the reset code ?

!!*-Ir0nMan™*-!! - May 31, 2020, 2:02 pm

(May 30, 2020 12:48 PM)kuramiqko Wrote: [\[CITE\]](#) I googled around and it said it was hashing the user activation key or I did not understand right ? If is that so, can I just hash the encryption key and get the reset code ?

the time u finish cracking the hash it will expire.

frank3nstien - May 31, 2020, 7:44 pm

This is how reset token works on Wordpress

Code `check_password_reset_key( string $key, string $login )`
this token is generated by hashing a random string. when token is generated it is stored in the users table in the user_activation_key column and Only the most recently generated token is stored, The token is also removed from the database once used.

If you are looking to send these token using sqli, you can generate them by trying

Code `get_password_reset_key()`
This function accepts a WP_User object as its argument

MahonStoN_ - June 6, 2020, 3:51 am

try to alter the sql records as the guy above me said already.