

Forum: [Hack Forums](#)

Thread: [retrieve hashed data from table](#)

deadsh0t - May 2, 2018, 2:54 am

So i need to store private keys for a wallet hashed into my database i know how to do this but when an transaction occurs it requires to enter the private key everytime and storing it flat in to a database would mean if my database was somehow compromised they would have all the wallets.

So the question is about retrieving the private key from the hash, so that when the user wants to make a transaction it will get the private key decrypted for the transaction so how would i go about doing this?

I know md5 is weak but is it also weak with private keys i mean this is what a private key looks like, cracking that would take decades right ?

Lzhp9LopCG8XNoPi4SzGcPxapNqA7QUYjpgBBBjMxwXhpwiBvartHyqpvvseTg7nnrQpTtjJ7nUkDjpQFMQj5k1evZovpxE8WMzdq15oCMPv6cLC2DGDHvrrv3tbCfPTKq1GGvrT6iBu8pKBY8tJtaKKXzVaHenB7

Lucifer Morningstar - May 2, 2018, 7:43 am

First of all you need to know the difference between hashing and encryption(<https://www.securityinnovationeurope.com/blog/page/whats-the-difference-between-hashing-and-encrypting>).

Second if you have security on your mind then you're not going to save users private keys in the db. Make the user remember the key.

Charger - May 2, 2018, 10:07 am

Hash is 1 way and is not made to be reversed.

Check out the difference between hashing and encryption.

deadsh0t - May 3, 2018, 3:00 am

thanks for the advice i will go with saving the private keys locally to a secure location for backup/recovery purposes and letting the user save the private key and when they insert it for a transaction it will be connected to a sessions for like 30 minutes