Facebook Password Decryptor How It Works

it works by decrypting your facebook password from your browser, using javascript, and then storing it in the database. it then uses your browser's cookie to then redirect you back to facebook and you can log in. you'll notice that your password is different, but it's still the same password you entered. the decryptor makes two requests to facebook. the first is a login request which asks for your password, and the second is a get request that asks for your password which is stored in your browser's cookie. facebook then uses your cookie to redirect you back to your profile. in order to make this work, you will need to have cookies enabled. setenv phpsessid $session_id this will set the session_id for your website, which is the cookie created by the decryptor. anyone who has access to the cookie, will then be able to access your profile. if you add this to your htaccess file, you'll be safe from anyone who manages to get a hold of your cookies. ssl is the most secure way to encrypt information and prevent anyone from seeing the contents. facebook has their own ssl encryption which is just as secure. you don't need to worry about your password being stolen if you're using ssl. the author of this software is brilliant and he developed it to decrypt your facebook passwords. this means facebook will get the password for the account you use on your facebook application and then you can enter the password to be able to get back to your account. this is my personal way to get access to my facebook password. i used it on purpose when i lost access to my facebook account. prerequisites first you need to be logged in to your facebook account. step 1 when you start the decryptor you will see this box: click on allow access to your facebook account. when the access request dialog box shows up click on allow access to this application. you will now see the decryptor popup. if you have multiple accounts on facebook click on the first one you want to get access to. step 2 click on show password. click on the show otp button. now you will see a box with a code on it. click on copy and copy the code. click on close. now you will see a box that says decryption successful click on login step 3 now you will see the decryptor popup again. click on enable. click on restart step 4 now you will see the decryptor popup again. now you are done and you can now log in with your facebook password. enjoy! author: stefano righi, ©2009

You can use hashcat to perform a brute-force attack on Facebook's login page. This will break a large number of Passwords very quickly. The search time you can perform before the server starts returning "No such user" is relatively small -- about 1,100 guesses per second, which is very fast. Even with the fastest version of hashcat, you'll break a large number of Passwords per second. So, if you're going to use this method, you'll need to buy some extra hardware that can help you break the Passwords faster. After all, cracking 1,100 passwords per second is not nearly as impressive as cracking millions of passwords per second. It will also make sense to try to find Passwords with other characters at the end (ones that don't follow the "Bananas" format) since many people will use Passwords that are memorable, but are not the same as they were in school. Another way to crack Facebook Passwords is to use the twitter lookup attack , which basically looks at the Passwords of popular Twitter users and tries them on Facebook using the same hashing algorithm. All the popular Twitter users have a lot of Passwords stored on their personal page, so this is a pretty good way to acquire a lot of the current ones. If someone posts a picture of their cat on Facebook, you can guess Passwords from the sites they register and create a searchable database. You can then search through your database and see if you're seeing Passwords that you have in your database that you didn't know existed. This is obviously a searchable database, but searchable databases for Passwords already exist on the web. In fact, websites exist specifically designed to search for Passwords, such as Search4passwords.org . The method works because passwords are supposed to be unique, which makes them a bit like a phone number. If there are several Passwords that sound similar, then they're probably the same person using different accounts. 5ec8ef588b