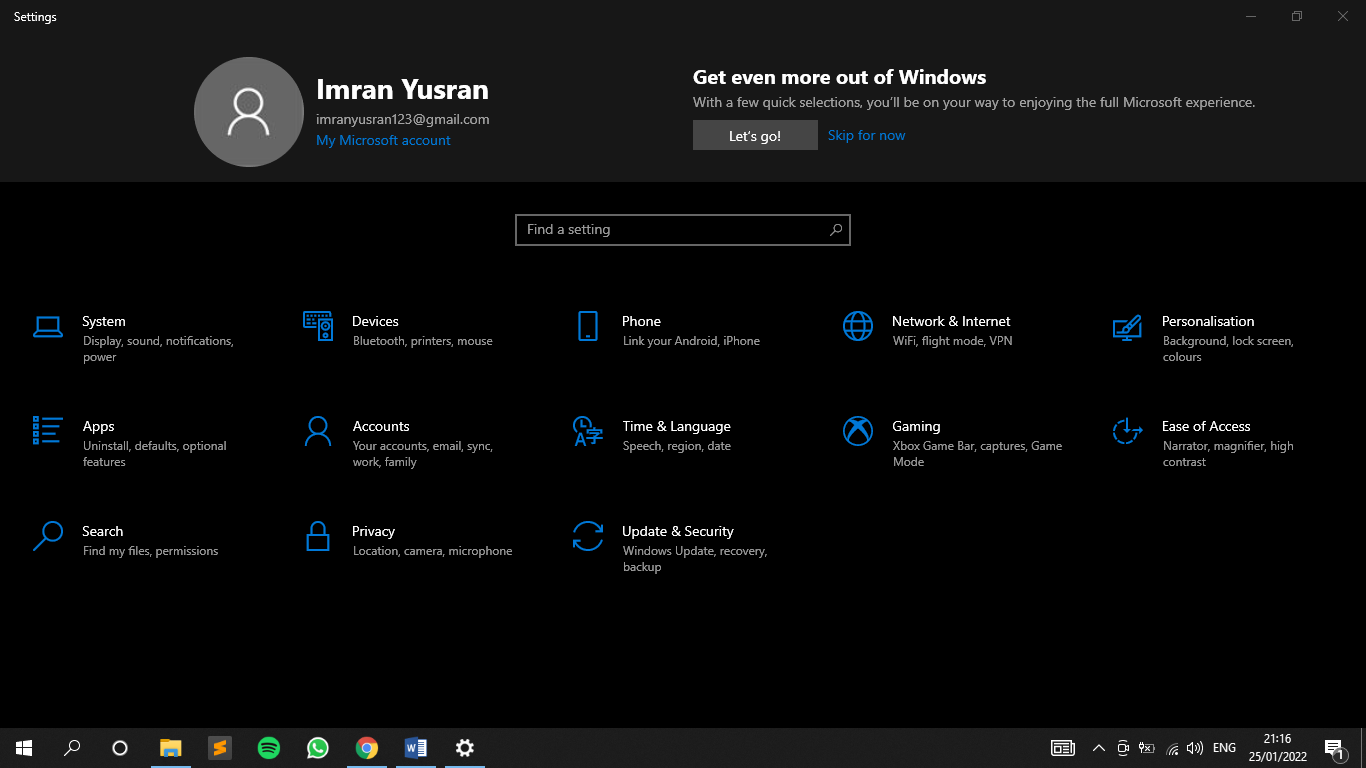
1. Cara membatasi aktifitas user tertentu di operating system pada windows 10 :
2. Masuk ke Windows Settings

Langkah pertama klik pada tombol Start (Icon Windows) lalu klik tombol Settings (Icon Gear).

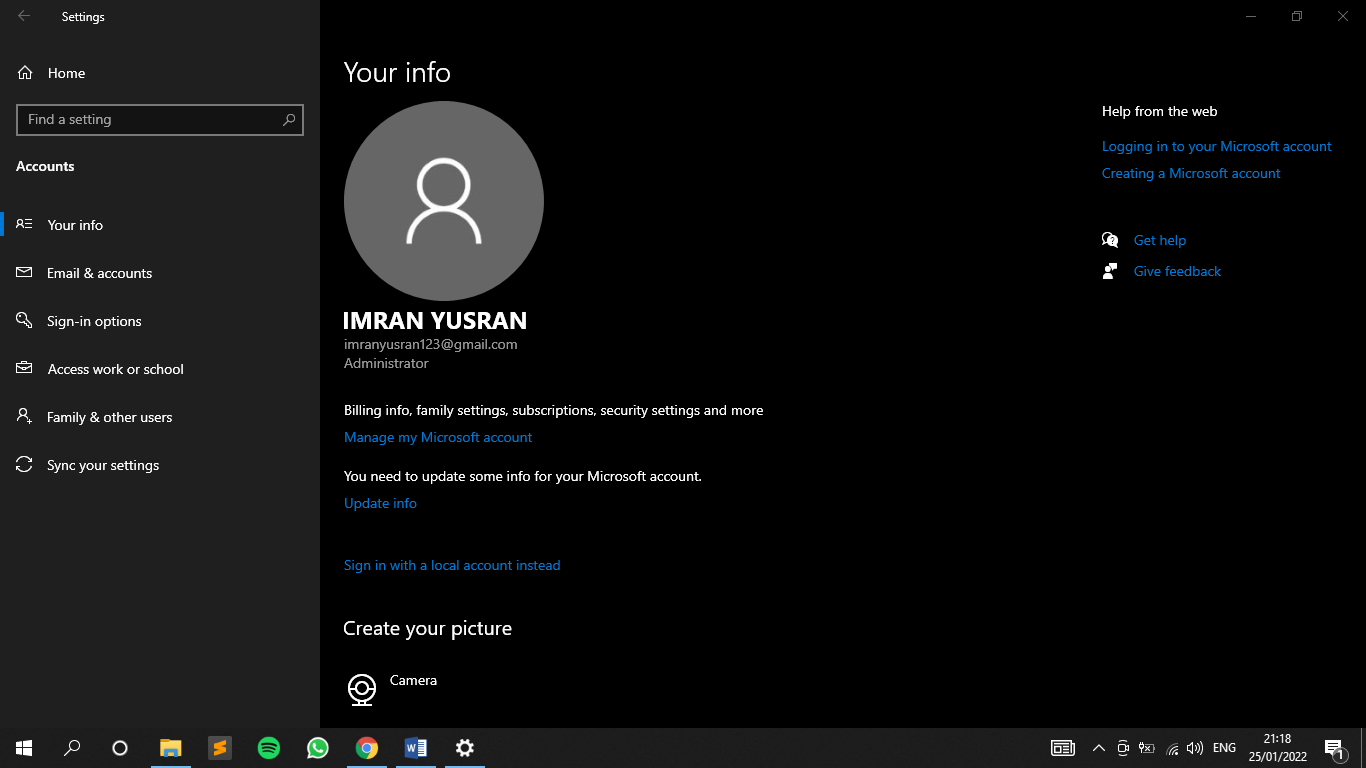
1. Pilih menu Accounts

Pada jendela Settings, klik pada pilihan menu Accounts.



1. Klik tab Family and other users

Lihat panel sebelah kiri, lalu klik tab Family and other users.

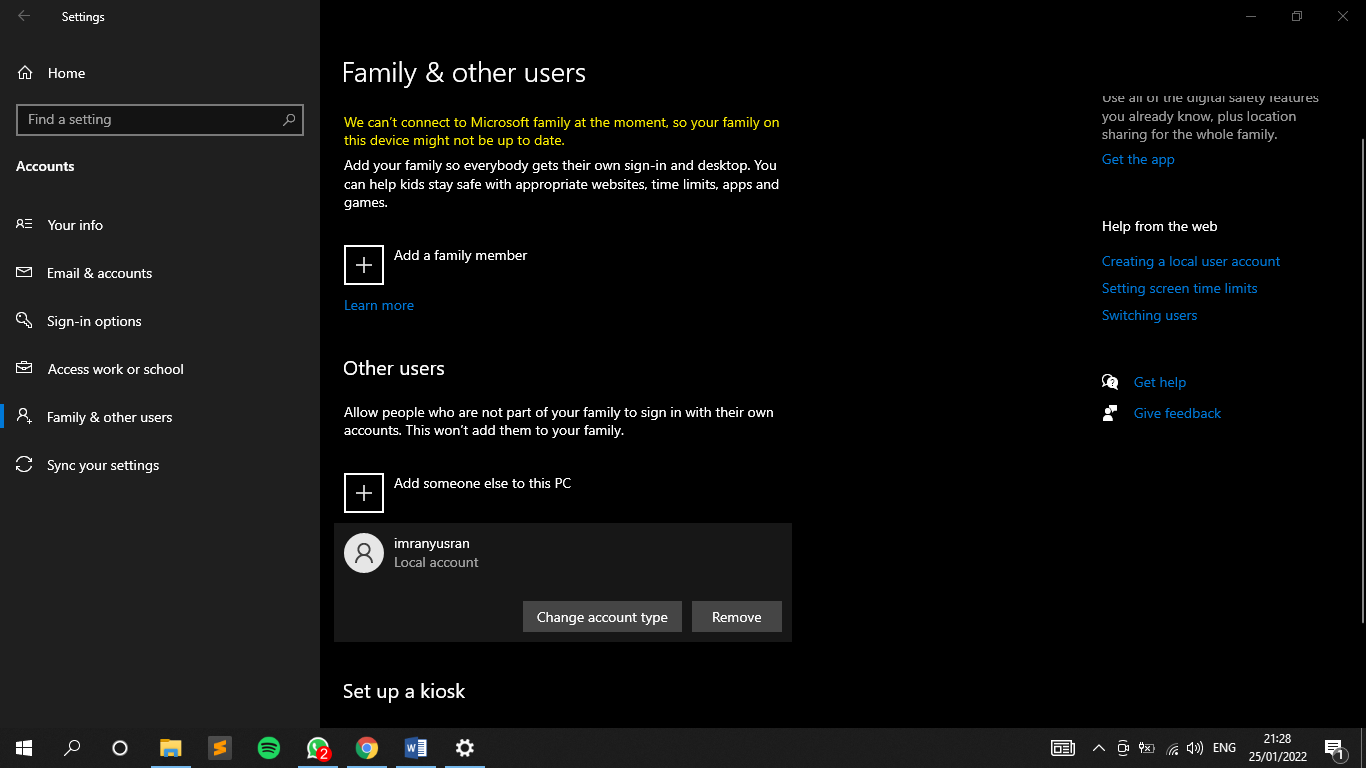


1. Pilih user yang ingin dibatasi aksesnya

Perhatikan pada panel sebelah kanan, di sana akan terlihat daftar user yang ada di Windows 10 kita. Lalu klik user yang ingin dibatasi aksesnya.

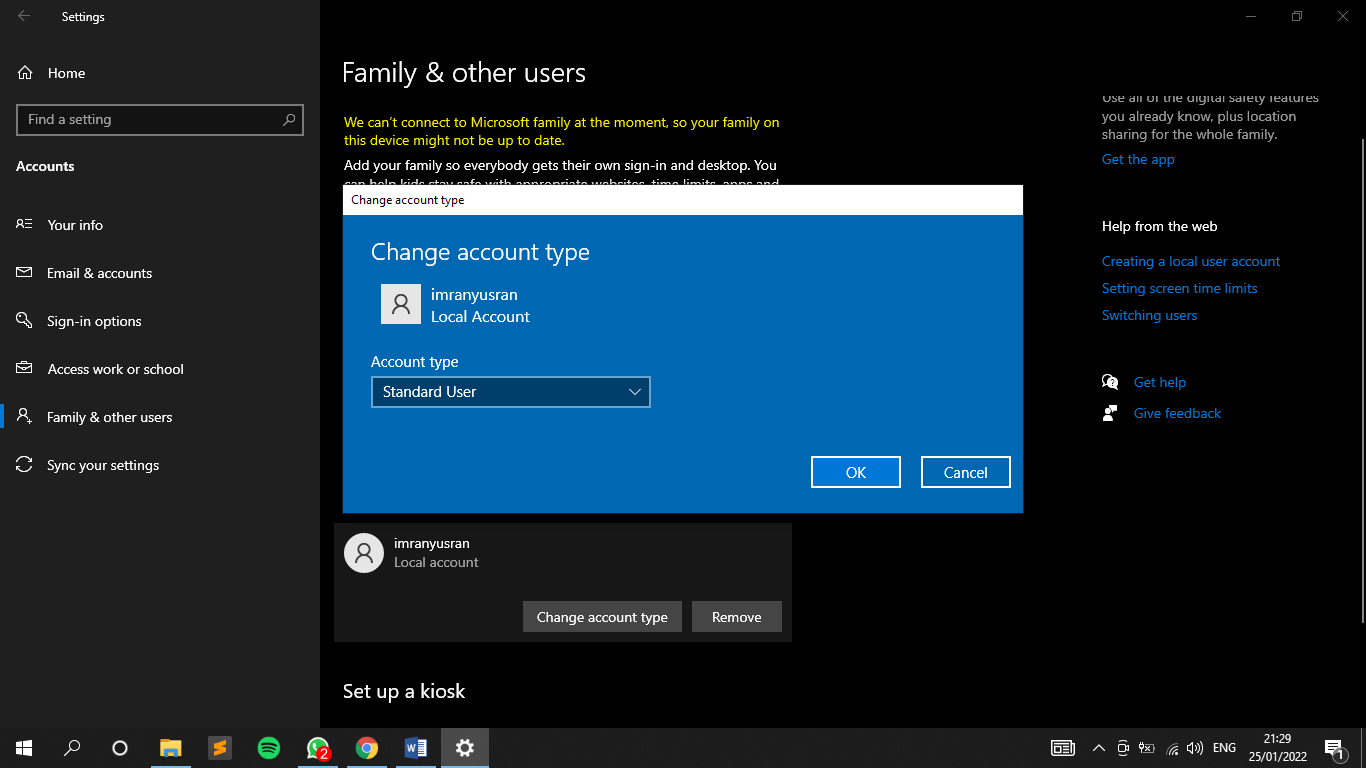
1. Klik tombol Change account type

Selanjutnya klik pada tombol Change account type yang ada di bawahnya.



1. Pilih Standard User

Terakhir pilih pada opsi Standard User, lalu klik OK.



Standard user merupakan pengguna dengan akses yang terbatas. User jenis ini bisa menggunakan semua program yang ada, menyimpan file pada folder user maupun partisi data, namun tidak bisa mengubah pengaturan komputer maupun menginstall aplikasi baru.

1. Code snippet untuk mengatasi SQL injection.

Ada beberapa cara yang bisa kita lakukan untuk mengatasi serangan SQL injection, kita bisa membuat script anti SQL injection dengan memanfaatkan fungsi bawan dari PHP yaitu mysql\_real\_escape atau mysql\_real\_escape\_string. Cara penggunaanya adalah sebagai berikut :

$id = mysql\_real\_escape\_string($\_GET['id']);

Selain cara di atas, ada beberapa tips aplikatif yang bisa kita gunakan untuk mengamankan web anda dari serangan SQL injection, berikut ini adalah tips nya :

1. Batasi panjang input box (jika memungkinkan), dengan  
   cara membatasinya di kode program, jadi si cracker pemula akan bingung sejenak melihat input box nya gak bisa diinject dengan perintah yang panjang.
2. Filter input yang dimasukkan oleh user, terutama penggunaan tanda kutip tunggal (Input Validation).
3. Matikan atau sembunyikan pesan-pesan error yang keluar dari SQL Server yang berjalan.
4. Code snippet untuk melakukan SQL injection.

Berikut merupakan contoh sederhana dari teknik serangan SQL Injection. SQL statement dinamis umumnya dikonstruksi pada saat eksekusi dilakukan, misalkan contoh berikut ditulis dalam bahasa pemrograman .NET dimana parameter input harus diisikan oleh pengguna

Query = "SELECT \* FROM users WHERE username = ' " +request.getParameter("input")+ " ' " ;

Maka baris kode tersebut akan menjalankan perintah query SQL sebagai berikut :

SELECT \* FROM users WHERE username = ‘input’

1. Code snippet untuk sanitasi data :
2. Mevalidasi Input : if (is\_numeric($id) == true) { ... }
3. Menyiapkan Kueri : $q = "SELECT username FROM users WHERE id = :id";
4. Membuat Pernyatan : $sth = $dbh->prepare($q);
5. Mengikat Paramater : $sth->bindParam(':id', $id);
6. Menjalankan Kueri : $sth->execute();
7. Mengambill Hasilnya : $result = $sth->fetchColumn();
8. Berikut sebuah form insiden beserta isi dari form tersebut :
9. Validasi form action

if (isset($\_POST['username'])) { ... }

1. Query

SELECT \* FROM users WHERE username = :username

1. Mempersiapkan dan memvalidasi query

$user = $db->prepare("SELECT \* FROM users WHERE username = :username"); $user->execute([ 'username' => $username, ]);

1. Validasi data tersedia

if ($user->rowCount()) { ... }

1. Eksekusi

$result = $user->fetch(PDO::FETCH\_OBJ);

1. Menampilkan hasil

echo 'Username: ' . $username . '<br>';

echo 'Nama: ' . $result->firstname . ' ' . $result->lastname;