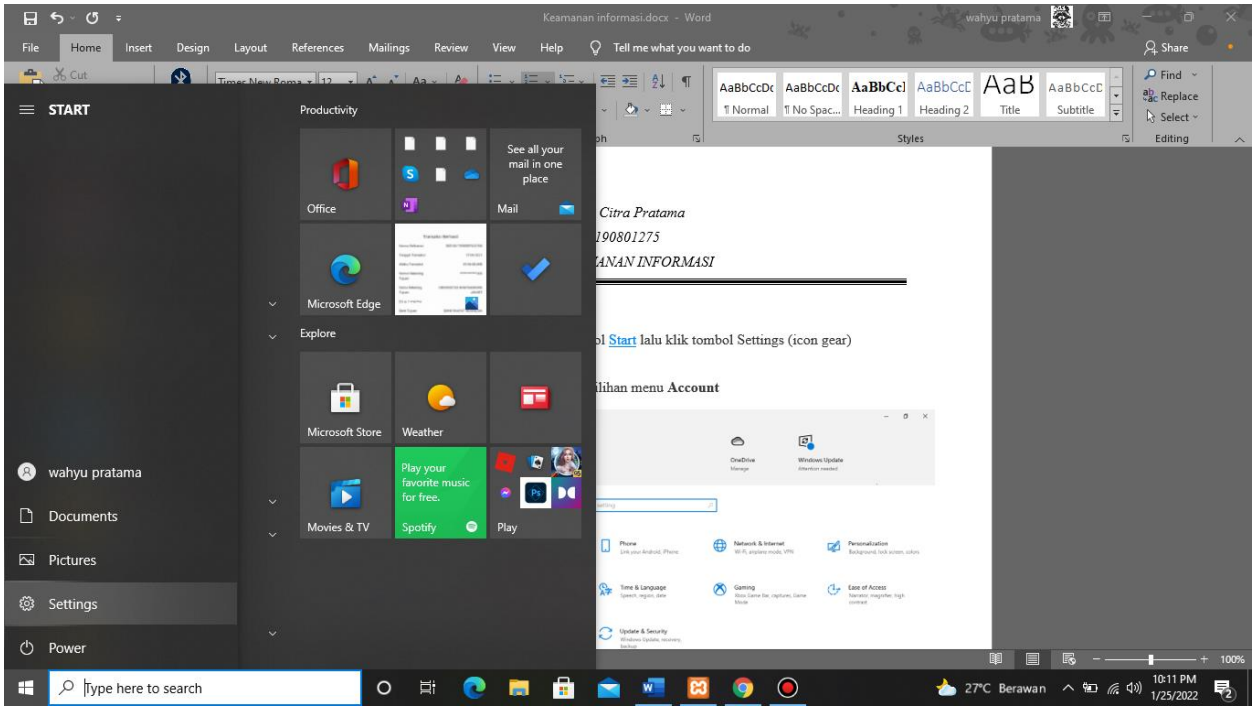
Wahyu Citra Pratama

20190801275

UAS KEAMANAN INFORMASI

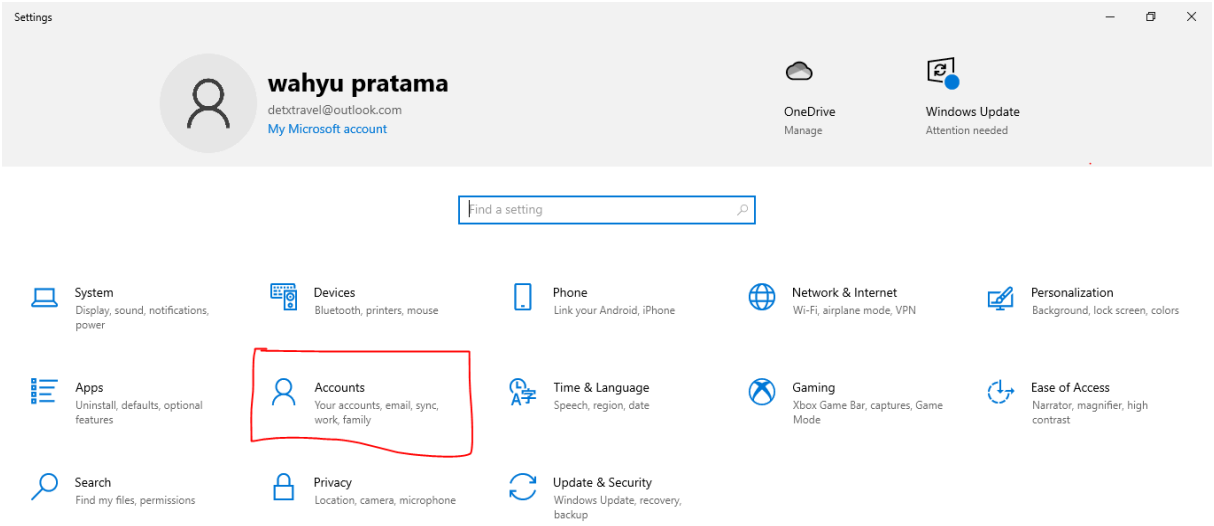
---

1. **1. Masuk ke Windows Settings**
   Langkah pertama klik pada tombol Start lalu klik tombol Settings (icon gear)



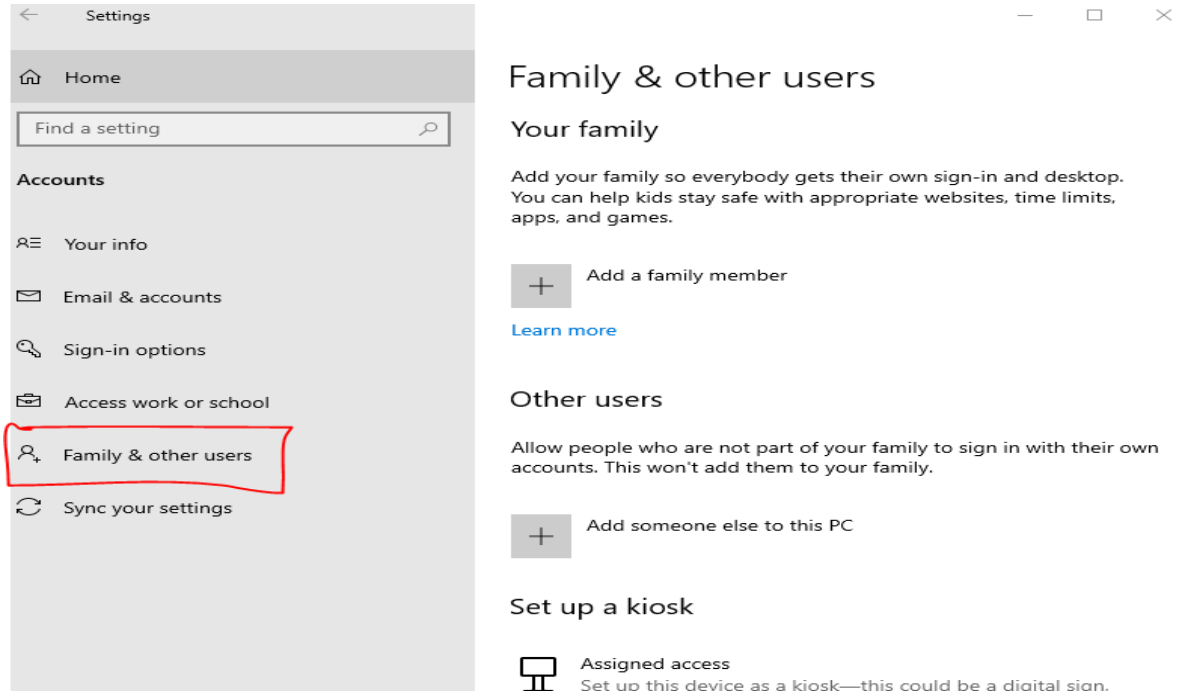
2. Pilih menu Accounts

Pada jendela Settings klik pada pilihan menu **Account**



3. Klik tab Family and other users

Panel sebelah kiri klik pada tab **Family and other users**

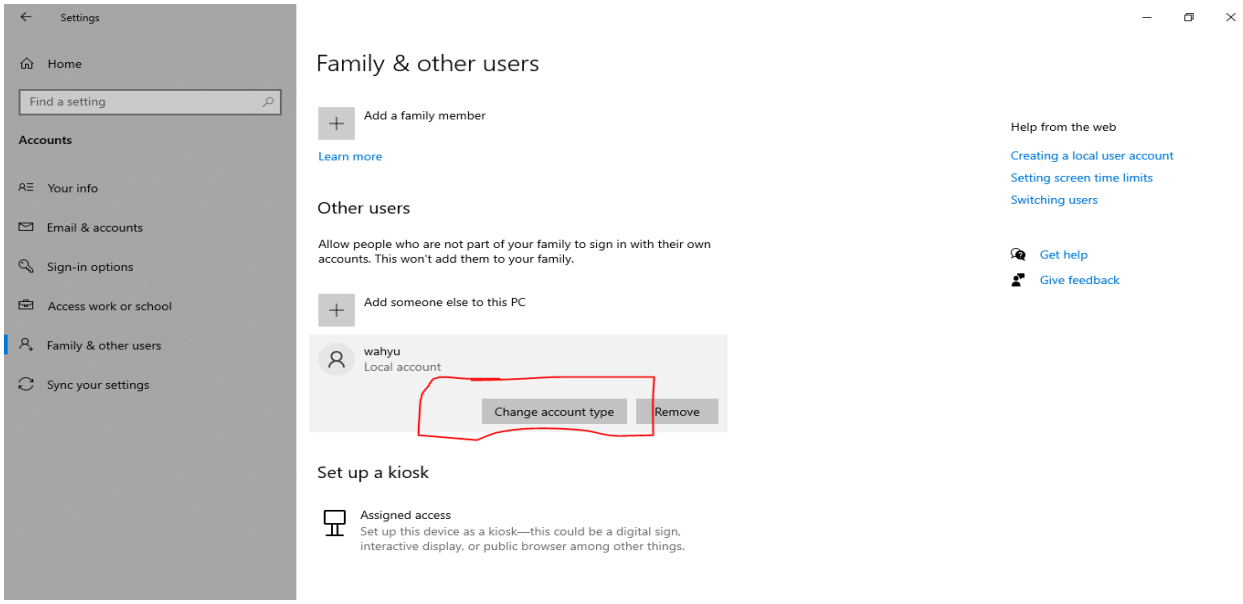


4. Pilih user yang ingin dibatasi aksesnya

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

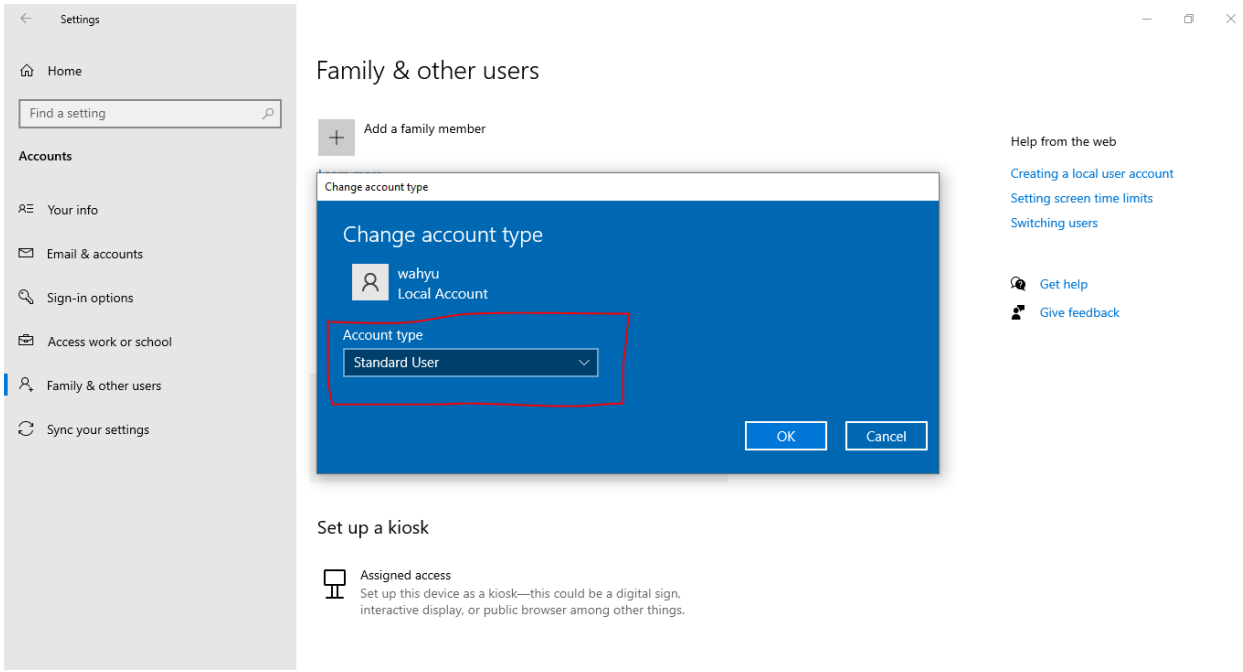
5. Klik tombol Change account type

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



6. Pilih Standard User

Terakhir pilih pada opsi **Standard User** lalu klik **OK**.



Standard User adalah pengguna dengan akses 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.

b. Buatlah sebuah code snippet untuk mengatasi SQL injection

Source Code:

```
$user = $db->prepare("SELECT * FROM users WHERE username = :username");

$user->execute([

    'username' => $username,

]);
```

Salah satu cara mencegah SQL Injection yaitu menggunakan quiery yang berparameter yang mudah. Query berparameter memaksa membedakan mana yang perintah query dan data yang dimasukkan oleh user. Hal ini memudahkan database untuk membedakan input dari user dan perintah database.

Jika penyerang memasukkan perintah query, maka sistem akan menganggapnya input dari user dan sebagai perintah sql yang tidak benar. Maka database tidak akan menjalankan perintah sql tersebut. Semua yang diinputkan oleh user dianggap oleh database sebagai data dari user bukan sebuah perintah sql.

c. Buatlah sebuah code snippet untuk melakukan SQL injection Source Code:

```
$user = $db->query("SELECT * FROM users WHERE username = '{$username}'");
```

Code tersebut adalah query untuk memanggil data setelah mengisi username di form. Jika data tersedia maka akan tampil seperti berikut:

Form:

Unsername : Wahyu Submit

Hasil/data yang ditampilkan:

Unsername : wahyu pratama

Jika source code seperti di atas maka bisa dilakukan SQL Injection dengan query seperti berikut:

'; DROP TABLE threads; --

Code tersebut untuk menghapus table yang bernama threads. Jika tereksekusi maka table tersebut akan terhapus.

d. Buatlah sebuah code snippet untuk sanitasi data sebuah form insiden beserta isi dari form tersebut

1. Validasi Form Action

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

2. Query

SELECT * FROM users WHERE username = :username

3.Mempersiapkan dan memvalidasi query

$user = $db->prepare("SELECT * FROM users WHERE username = :username");

$user->execute([

'username' => $username,

]);

Validasi Data Tersedia

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

Eksekusi

$result = $user->fetch(PDO::FETCH_OBJ);

6. Menampilkan Hasil

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