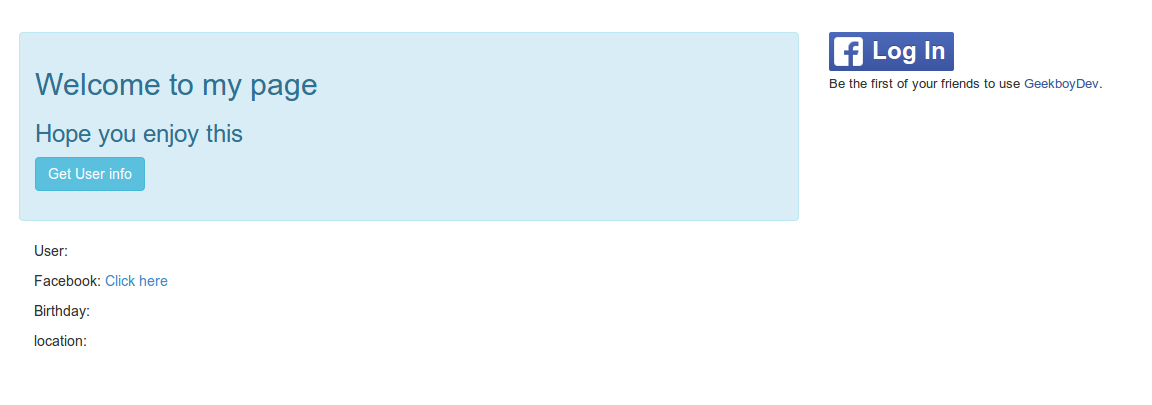
**TÌM HIỂU VỀ OAUTH**

**Use case**

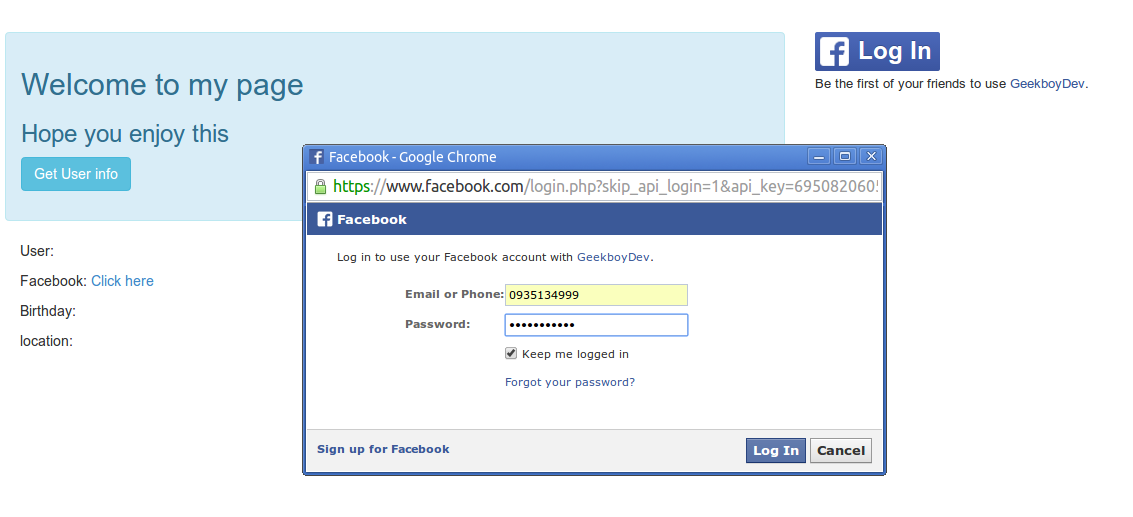
*Find Me* là một web application cho phép người dùng tìm kiếm địa chỉ nhà của bạn bè mình thông qua bản đồ Google Maps. *Find Me* không có tính năng đăng ký tài khoản người dùng mà cho phép người sử dụng tài khoản Facebook để hoạt động.

Các thông tin về tài khoản của người dùng đều do Facebook quản lý. Find me không thể truy cập đến các thông tin này nếu không được sự cho phép của người dùng. Để làm được điều này, Facebook và Find me đã sử dụng Oauth để có thể có quyền truy cập đến thông tin người dùng trên facebook.

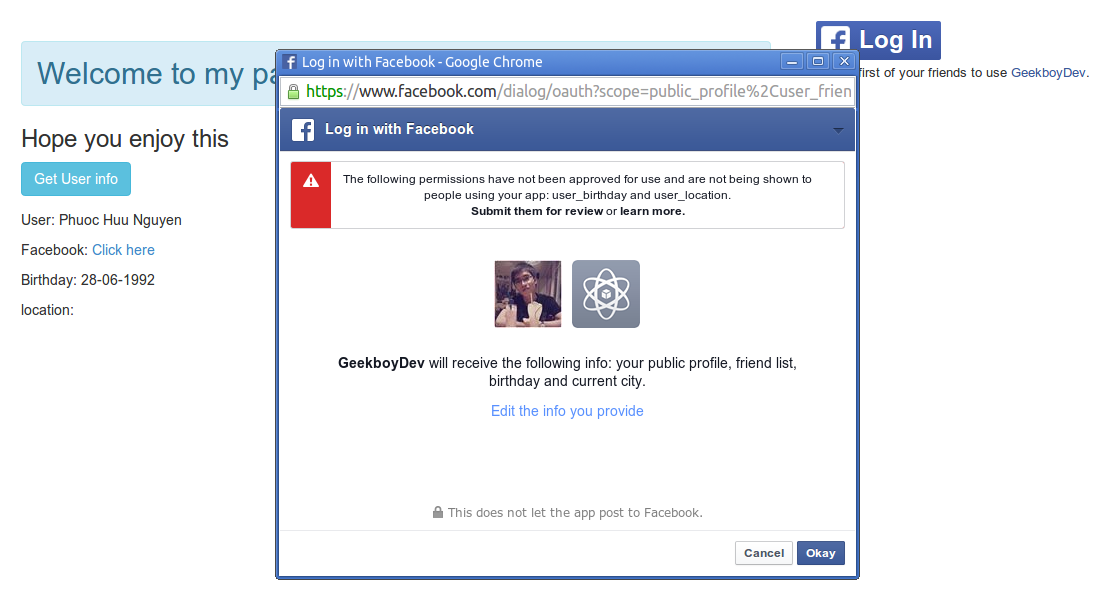
Khi người dùng lần đầu truy cập vào Find me, để có thể sử dụng các tính năng Find me cung cấp, người dùng cần phải đăng nhập thông qua Facebook. Find me sẽ cung cấp sẵn cho người dùng một button đăng nhập với Facebook.



Khi người dùng nhấp vào button Login, Find me sẽ gửi một Request access thông qua SDK và hiển thị form đăng nhập Facebook cho người dùng.

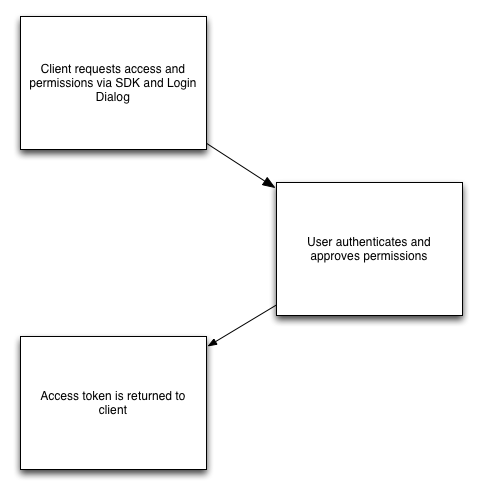


Khi người dùng đăng nhập thành công, Facebook sẽ hiển thị bảng thông báo yêu cầu người dùng cấp phép để Find me có thể lấy thông tin người dùng từ Facebook.



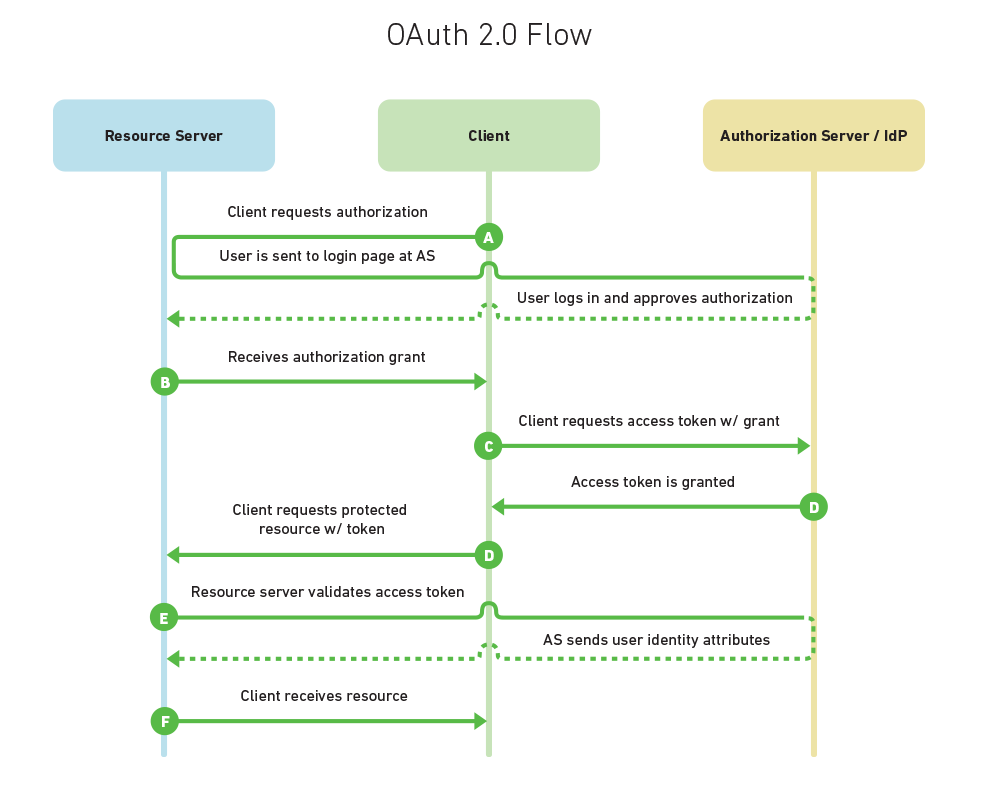
Khi người chấp nhận cấp quyền cho Find me, Facebook sẽ ung cấp cho người một access token. Ta có thể hiểu access token giống như một chìa khóa, bao gồm một số quyền hạn mà người dùng cho phép cho Find me truy cập thông tin mình trên Facebook.

**Mô tả qui trình**



**Giới thiệu Oauth 2**

**Sơ đồ hoạt động**



**Các thành phần tham gia**

* **Resource Server (Service Provider)** - this is the web-server you are trying to access information on.
* **Client** - this is how the user is interacting with the Resource Server. This could be a browser-based web app, a native mobile app, a desktop app, a server-side app
* **Authorization Server (Identity Provider)** - this is the server that owns the user identities and credentials. It's who the user actually authenticates and authorizes with. - là máy chủ chứa sở hữu thông tin của người dùng.

**The workflow**

A - a user opens their web-browser and goes to Findme.com. This website doesn't handle authentication itself, so the user is redirected to the Authorization Server with a request for authorization. The user is presented with a login form and is asked if they want to approve the Resource Server (Findme.com) to act on their behalf. The user logs in and they are redirected back to Findme.com.

B - Findme.com receives an **authorization grant code** as a part of the redirect and then passes this along to the client.

C - the Client then uses that authorization grant code to request an access token from the Authorization Server.

D - if the authorization grant code is valid, then the Authorization Server grants an access token. The access token is then used by the client to request resources from the Resource Server (Findme.com).

E - Findme.com receives the request for a resource and it receives the access token. In order to make sure it's a valid access token it sends the token directly to the Authorization Server to validate. If valid, the Authorization Server sends back information about the user.

F - having validated the user's request Findme.com sends the requested resource back to the user.