***Tìm hiểu cơ chế xác thực OAuth2***

1. **OAuth2 là gì?**

Là giao thức xác thực và ủy quyền phổ biến được sử dụng để cho phép người dùng truy cập tài nguyên của 1 dịch vụ hoặc ứng dụng bên thứ 3 mà không cần chia sẻ trực tiếp thông tin đăng nhập. OAuth2 sẽ dùng các mã token để xác thực và ủy quyền người dùng

1. **Cơ chế của OAuth2**

* **Resource Owner (Chủ sở hữu tài nguyên):** Người dùng muốn sở hữu tài nguyên mà ứng dụng muốn truy cập
* **Resource Server (Máy chủ tài nguyên):** Là server lưu trữ tài nguyên do người dùng chia sẻ
* **Client (Ứng dụng):** Ứng dụng muốn truy cập tài nguyên của người dùng
* **Authorization Server (Máy chủ ủy quyền):** Máy chủ cung cấp dịch vụ xác thực và ủy quyền cho người dùng và ứng dụng bằng cách tạo ra các mã token

1. **Quá trình hoạt động của OAuth2**

* Client yêu cầu xác thực và ủy quyền từ người dùng
* Người dùng cấp quyền cho client và chuyển hướng tới Authorization Server
* Authorization Server xác thực danh tính của người dùng và yêu cầu xác nhận quyền truy cập từ người dùng
* Người dùng cung cấp xác nhận quyền truy cập
* Authorization Server cung cấp mã ủy quyền cho client
* Client gửi mã ủy quyền đến Authorization Server để yêu cầu mã truy cập
* Authorization Server xác thực mã ủy quyền và cung cấp mã truy cập cho client
* Clien sử dụng mã truy cập tài nguyên từ người dùng từ Resource Server

1. **Các loại Grant type của OAuth2**

* **Authorization Code Grant:** Đây là grant type phổ biến nhất trong OAuth2. Client yêu cầu người dùng xác thực và cấp quyền truy cập, 1 mã ủy quyền được cấp cho client, client sử dụng mã ủy quyền để đổi lấy mã truy cập từ Authorization Server
* **Implicit Grant:** Được sử dụng khi client trực tiếp nhận mã truy cập từ Authorization Server thông qua phản hồi của người dùng, không cần trao đổi mã ủy quyền. Implicit Grant thường được sử dụng trong các ứng dụng đơn giản và client-side
* **Resource Owner Password Credentials Grant:** Loại grant type này cho phép ứng dụng yêu cầu người dùng cung cấp tên đăng nhập và mật khẩu trực tiếp từ client, client lấy thông tin để đổi mã truy cập Authorization Server -> Không được khuyến khích sử dụng , vì nó yêu cầu client lưu trữ và xử lý thông tin đăng nhập của người dùng
* **Client Credentials Grant:** Loại grant type này cho phép ứng dụng yêu cầu mã truy cập từ Authorization Server bằng cách xác thực bằng thông tin đăng nhập và mật khẩu của chính ứng dụng, thay vì thông tin đăng nhập của người dùng. Thường dùng trong việc xác thực và ủy quyền giữa các ứng dụng trong môi trường server-to-server
* **Refresh Token Grant:** Khi mã truy cập hết hạn , client có thể sử dụng mã làm mới (refresh token) để lấy 1 mã truy cập mới mà không cần yêu cầu người dùng xác thực lại. Refresh Token Grant cho phép ứng dụng trao đổi mã làm mới để lấy mã truy cập mới từ Authorization Server