**1. JWT là gì?**

**JWT (JSON Web Token)** là một chuẩn **mã hóa thông tin dạng JSON**, thường được sử dụng để **xác thực và trao đổi thông tin an toàn** giữa các hệ thống.

**Cấu trúc của JWT gồm 3 phần chính (ngăn cách bởi dấu .):**

Header.Payload.Signature

* **Header**: Chứa thông tin loại token (JWT) và thuật toán ký (như HS256).
* **Payload**: Chứa dữ liệu (claims) như userId, role, exp (hạn sử dụng), v.v.
* **Signature**: Là kết quả mã hóa từ Header + Payload bằng secret key.

**2. Access Token và Refresh Token là gì?**

**Access Token**

* Dùng để **xác thực người dùng mỗi lần gọi API**.
* Có **thời hạn ngắn** (vài phút đến vài giờ).
* Nếu hết hạn -> cần dùng refresh token để lấy cái mới.

**Refresh Token**

* Dùng để **lấy access token mới** khi access token cũ hết hạn.
* Có **thời hạn dài hơn** (thường là vài ngày hoặc vài tuần).
* Bảo mật hơn, nên thường **lưu ở server hoặc HttpOnly cookie**.

**Lợi ích khi dùng cả hai:**

* Hạn chế rủi ro nếu access token bị lộ (vì thời gian ngắn).
* Không cần đăng nhập lại nhiều lần (vì có refresh token).