Reflections về JWT

***1.Json Web Token là gì?***

- JSON Web Token (JWT) là một tiêu chuẩn mở (RFC 7519) định nghĩa một cách nhỏ gọn và an toàn để truyền tải thông tin giữa các bên một cách an toàn dưới dạng 1 đối tượng JSON . Các thông tin này được xác thực và có độ tin cậy cao vì nó có chứa chữ ký số (digital signature).

1. ***Khi nào nên sử dụng JWT?***

- Khi người dùng đã đăng nhập vào hệ thống thì những request tiếp theo của người dùng gửi lên sẽ phải bao gồm JWT token.

- Nếu JWT token đó có quyền thì người dùng mới được truy cập các dịch vụ, tài nguyên và tương tác với cơ sở dữ liệu.

- JSON Web Tokens là cách tốt nhất để trao đổi thông tin giữa các bên một cách an toàn.

-  JWT cho phép tất cả các đặc tính này áp dụng cho API Authentication và thường được đặt trong HTTP Authorization headers.

*=>Sử dụng JWT là cách tốt để áp dụng cơ chế bảo mật đối với các dịch vụ API RESTful mà có thể được sử dụng để truy cập vào cơ sở dữ liệu của bạn.*

1. ***3 thành phần của JWT***

- **Header**:

Header bao gồm hai phần chính: loại token (mặc định là JWT - Thông tin này cho biết đây là một Token JWT) và thuật toán đã dùng để mã hóa (HMAC SHA256 - HS256 hoặc RSA).

- **Payload**:

Payload chứa các claims. Claims là một các biểu thức về một thực thể (chẳng hạn user) và một số metadata phụ trợ. Có 3 loại claims thường gặp trong Payload: reserved, public và private claims.

- ****Signature:****

Do bản thân Signature đã bao gồm cả header và payload nên Signature có thể dùng để kiểm tra tính toàn vẹn của dữ liệu khi truyền tải.

*4.******JSON Web Tokens hoạt động như thế nào?*****

- Trong quá trình xác thực, người dùng đăng nhập thành công bằng cách sử dụng các thông tin của họ (email or username, password), JSON Web Token sẽ được trả lại và phải được lưu lại dưới local (thường là trong local storage, nhưng có lúc cookie cũng có thể được sử dụng) thay vì cách truyền thống là tạo ra một session trên server và trả lại cookie.

- Bất cứ khi nào người dùng muốn truy cập vào route hoặc tài nguyên cần có quyền, họ phải gửi JWT trong ****Authorization**** header sử dụng Bearer schema như sau: Authorization: Bearer <token>