1/JWT là viết tắt của JSON Web Token - một chuẩn mã hóa dữ liệu dạng JSON được sử dụng để xác thực và trao đổi thông tin an toàn giữa các bên trong một hệ thống.

JWT là một chuỗi gồm ba phần được mã hóa dưới dạng Base64, được ngăn cách bằng dấu chấm.

Các phần của JWT bao gồm:

**Header (tiêu đề):** là một đối tượng JSON chứa thông tin về thuật toán mã hóa được sử dụng cho token và loại của token.{

“typ” (type) chỉ ra rằng đối tượng là một JWT

“alg” (algorithm) xác định thuật toán mã hóa cho chuỗi là HS256 }

Payload (nội dung): là một đối tượng JSON chứa các thông tin liên quan đến người dùng và các quyền của họ, ví dụ như tên, email, quyền truy cập vào các tài nguyên, v.v.

Phần payload sẽ chứa các thông tin mình muốn đặt trong chuỗi Token như username , userId , author , … ví dụ:

{

"user\_name": "admin",

"user\_id": "1513717410",

"authorities": "ADMIN\_USER",

"jti": "474cb37f-2c9c-44e4-8f5c-1ea5e4cc4d18"

}

Signature (chữ ký): là một chuỗi mã hóa bằng thuật toán được chỉ định trong phần header và sử dụng để đảm bảo tính toàn vẹn của dữ liệu.

+Signature được tạo bằng cách sử dụng thuật toán mã hóa và kết hợp header, payload và một khóa bí mật duy nhất để tạo ra một chuỗi ký tự đại diện cho token.

Khi một người dùng đăng nhập vào hệ thống, hệ thống sẽ tạo ra một JWT và trả về cho người dùng.

+Người dùng sẽ gửi JWT này kèm với các yêu cầu tiếp theo đến server.

+Server sẽ xác thực tính hợp lệ của token bằng cách giải mã và xác minh chữ ký, và sau đó sử dụng các thông tin trong phần payload để xác định quyền truy cập của người dùng.

+Nếu token không hợp lệ hoặc đã hết hạn, server sẽ từ chối yêu cầu và yêu cầu người dùng đăng nhập lại.