[Bài đọc] JSON Web Token với Spring Security JWT

JSON Web Token là gì?

JSON Web Token (JWT) là một chuẩn mở (RFC 7519) xác định một cách nhỏ gọn, khép kín để truyền tải thông tin một cách an toàn giữa các bên bằng một đối tượng JSON. Thông tin được truyền tải bởi JWT có thể được xác thực và tin tưởng bởi vì nó sử dụng chữ ký số, JWT có thể được ký với khóa private (ví dụ HMAC) hoặc cặp khóa public/private (ví dụ RSA)

* Gọn nhẹ: Do kích thước nhỏ hơn của chúng, JWT có thể được gửi qua URL, tham số POST hoặc bên trong tiêu đề HTTP. Ngoài ra, kích thước nhỏ hơn có nghĩa là truyền nhanh.
* Tự chứa: Hàng tải chứa tất cả các thông tin cần thiết về người dùng, tránh sự cần thiết phải truy vấn cơ sở dữ liệu nhiều lần.

Khi nào nên sử dụng JWT?

Đây là các tình huống mà JSON Web Token rất hữu dụng:

* Authentication (Xác thực): Thường dùng xác thực các API, một chuỗi JSON Web Token sẽ được gửi kèm trong phần header của request và server sẽ thông qua token đó để xác thực request.
* Information Exchange(Truyền thông tin): Bởi vì JWT có thể được ký bằng chữ ký số do đó ta có thể đảm bảo rằng người gửi và nội dung sẽ không bị giả mạo.

Cấu trúc của JWT

JWT gồm 3 phần

* Header: thường gồm 2 phần là loại token và thuật toán mã hóa.
* Payload: chứa các claims (thông tin) như username, issuer…
* Signature: chữ ký số.

Ví dụ JSON Web Token:

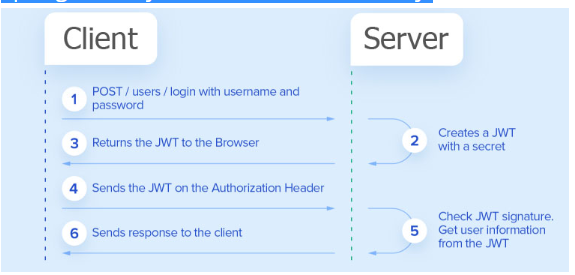
*eyJhbGciOiJIUzI1NiJ9.eyJleHAiOjE1MjIzODMwMzAsInVzZXJuYW1lIjoia2FpIn0.VC–B2dsUpGOwl9QtTXjL2iwuVsZPUSUsBKEjPPx\_R8*



Ta dùng trang <https://jwt.io/> để parse token, khi sử dụng jwt bạn cũng sẽ parse token tương tự như thế.

Phần header sẽ có thông tin thuật toán mã hóa là “HS256”, phần payload chứa thời gian hết hạn của token và username, phần chữ ký số mình không sử dụng từ “secret” để làm chữ ký nên nó báo “invalid signature”

## Spring Security JWT (RESTFul API Security)



* B1: Client gửi thông tin username/password để đăng nhập.
* B2 + B3: Server xác nhận thông tin username/password để tạo ra một chuỗi token với các thông tin cần thiết (thời gian hết hạn, username, role…) và gửi về cho client
* B4: Khi client (mobile app, browser) thực hiện gửi API nó sẽ kèm theo token vào trong header của request.
* B5 + B6: Server nhận được request API sẽ lấy token trong header của request để kiểm tra thông tin xác thực và trả về dữ liệu cho client.