**Khái niệm JWT**

**JWT (JSON Web Token)** là tiêu chuẩn mở (RFC 7519) để truyền tải thông tin an toàn giữa các bên dưới dạng JSON. JWT được sử dụng chủ yếu cho **xác thực và ủy quyền** trong ứng dụng web/mobile.

**Cấu trúc JWT**

JWT gồm **3 phần** phân tách bởi dấu chấm (.):

Header.Payload.Signature

xxxxx.yyyyy.zzzzz

**Ví dụ JWT mẫu:**

text

eyJhbGciOiJIUzI1NiJ9.eyJuYW1lIjoiSm9lIENvZGVyIn0.5dlp7GmziL2QS06sZgK4mtaqv0\_xX4oFUuTDh1zHK4U

**1. Header**

Chứa thông tin về loại token và thuật toán mã hóa:

{

"alg": "HS256", *// Thuật toán*

"typ": "JWT" *// Loại token*

}

**2. Payload**

Chứa các **claims** (thông tin người dùng):

{

"sub": "1234567890",

"name": "John Doe",

"admin": true

}

**3. Signature**

Được tạo bằng: HMACSHA256(header + payload, secret) để đảm bảo tính toàn vẹn.

**Ưu điểm vs Nhược điểm**

| **Ưu điểm** | **Nhược điểm** |
| --- | --- |
| Gọn nhẹ, tiết kiệm tài nguyên | Giới hạn 8KB (HTTP Header) |
| Bảo mật với chữ ký số | Không thể thu hồi token |
| Tương thích đa ngôn ngữ | Header/Payload có thể đọc được |
| Không cần lưu trên server | Rủi ro nếu cấu hình sai |

**Các trường hợp sử dụng phổ biến**

1. **Authentication** - Xác thực người dùng sau đăng nhập
2. **Authorization** - Phân quyền truy cập tài nguyên
3. **Single Sign-On (SSO)** - Đăng nhập một lần, dùng nhiều ứng dụng
4. **API Authorization** - Bảo vệ và phân quyền API
5. **Microservices Communication** - Giao tiếp giữa các service
6. **Information Exchange** - Trao đổi dữ liệu an toàn