Chapter 4: REST API

REST API

เป็นสถาปัตยกรรม Client-Server ที่มี **REST Web Service Server** ที่รับ HTTP request มาจาก Application Server อีกที

- method + json

API Security

1. **Logout to clear token cookie** >> ตั้ง expiration date ของ cookie และหากกด logout ให้ clear ด้วย
2. **Prevent NoSQL injection & Sanitized data**
3. **Security headers**
4. **Cross-site scripting (XSS)** >> พยายามฝัง script หรือ link การเรียกใช้ script
5. **Rate limit** >> จำกัดจำนวนการเรียกใช้งานในระยะเวลา ๆ หนึ่ง
6. **HTTP Parameter Pollution (HPP)** >> ป้องกันการใส่ parameter เข้ามาเยอะ ๆ
7. **CORS** >> ป้องกันไม่ให้มีการเรียกใช้ resource ข้าม server

OpenAPI

- **OpenAPI** >> specification (standard) ที่อธิบาย API
  - ไม่ได้ขึ้นกับภาษาใดภาษาหนึ่ง
  - ทำให้คนกับคอมพิวเตอร์เข้าใจ REST API ได้โดยไม่ต้องรู้ code ก็เข้าใจการเรียกใช้งานได้
- **Swagger** >> เครื่องมือ (tool) ที่ช่วยในการเขียน OpenAPI