- Node.JS Authentication with JWT
    - **Token คืออะไร?**

      คือรหัสชุดนึงที่เอาไว้สำหรับทดแทน session ซึ่งเอาไว้ระบุว่าคนๆนั้นคือใคร token เอามาใช้ในการทำ RESTFul API ทดแทนการทำ Web Server แบบเดิมๆ ที่เก็บในรูปแบบ session โดยตัว token จะถูกส่งไปทุกๆ request ผ่าน HTTP Headers

    - **JWT คืออะไร?**

      JWT หรือ JSON Web Token เป็นรูปแบบหนึ่งที่ใช้ในการสร้างรหัส token จากข้อมูล JSON Data แล้วทำการเข้ารหัสด้วย Base64Url Encoded ลักษณะดังนี้

```
eyJ0eXAiOiJKV1tiLCJhbGciOiJIUzI1Nis9.eyJpZCI6IjU3NzRhMjM1Zm
I1OTdlMWIxMWY3YzY3ZiIsImVtYWlsIjoiY2hhaUBuZXh0enkuY29tIiwic2
NvcGUiOiJVU0VSIiwiaWF0IjoxNDY3NzgzMTgyLCJleHAiOjE0Njc4Njk40
DJ9.CGXxDtTJD0LBpY7oTbm-ZWB1o6J7isu09ZNk1Q2uTc0
```

ซึ่งจะเห็นได้ว่า JWT จะมีจุดขั้นไว้ นั่นคือ <base64url-encoded header>.<base64url-encoded payload>.<base64url-encoded signature> ประกอบด้วย 3 ส่วนดังนี้

1. Header : (คือข้อมูล metadata ของ token ซึ่งบอกว่า เป็น type และใช้ algorithm อะไร) ประกอบด้วย 2 ส่วน คือ type เป็น JWT และ hash algorithm ที่ใช้ เช่น HMAC SHA256

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

เมื่อนำข้อมูล header มาเข้ารหัสด้วย Base64Url encoded ก็จะได้ข้อมูลประมาณ

```
eyJ0eXAiOiJKV1tiLCJhbGciOiJIUzI1Nis9
```

2. Body หรือ Payload หรือ Claims : ข้อมูลทั้งหมดที่เราเอาไว้ sign token ประกอบไปด้วยข้อมูล information ของคนๆนั้น เช่น id, name มีทั้งที่เป็น Private หรือ Public Data ข้อมูล JSON ของ payload

```
{
  "sub": "1",
  "name": "Chai Phonbopit",
  "role": "admin",
  "exp": 1402374336,
  "iat": 1402338336
}
```

- `sub`: subject เอาไว้สำหรับ authenticate user (เช่น user Id)
- `exp`: คือเวลาหมดอายุของ token
- `iat`: Issued at timestamp บอกว่า token สร้างเมื่อไหร่

3. Signature : ส่วนสำคัญของข้อมูล เป็นการรวมกันของ Header และ Body ใช้ algorithm และ secret key ในการ sign

ตัวอย่างของการ gen signature คือ

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  secretKey)
```

ดูตัวอย่างได้ที่: https://github.com/Piinfany/JWT-project