

JWT:

1. 伺服器端在收到登入請求後驗證使用者
2. 伺服器端產生和回傳一組帶有資訊，且僅能在伺服器端被驗證的 Token
3. Token 被回傳後，存取在「客戶端」（大多存在瀏覽器的 Storage 當中）
4. 往後客戶端向伺服器端發送請求時，皆附帶此 Token 讓伺服器端驗證
5. 若伺服器端在請求中沒有找到 Token，回傳錯誤；若有找到 Token 則驗證

JWT 組成

JWT 是一組字串，透過（.）切分成三個為 Base64 編碼的部分：

Header：含 Token 的種類及產生簽章（signature）要使用的雜湊演算法

Payload：帶有欲存放的資訊（例如用戶資訊）

Signature：編譯後的 Header、Payload 與密鑰透過雜湊演算法所產生

安裝:  
$ npm install jsonwebtoken

載入:  
const jwt = require('jsonwebtoken');

產生:  
jwt.sign(payload, secretOrPrivateKey, [options, callback]);

Option 非必填 但能設定很多選項  
Ex: algorithm: 設定產生簽章要使用的雜湊演算法（預設： HS256）

expiresIn: 設定 Token 多久後會過期（自動在 Payload 新增 exp）

noTimestamp: 設定產生 JWD 時不會自動在 Payload 中新增iat時間

客戶端請求帶入JWT

Authorization: 'Bearer ' + token

伺服器取得

const token = req.header('Authorization').replace('Bearer ', '')

console.log(token)