

淺談 Session 與 JWT 差異



集點送紅利 / Hiro · Follow

7 min read · Feb 14, 2020



70



前言

在剛觸碰後端時，很常為了會員驗證的 Session 而苦惱不久對吧？前陣子我第一眼看到 JWT 的時候，一丟 Google 發現有人用 JWT 來代替 Session，繼續查下去又發現有人說不要這樣做，所以 JWT 到底是啥？可以用在哪？

目錄

- 認證與授權
 1. 認證
 2. 授權
- Session 是什麼
 1. 小故事
 2. 運作原理
 3. 與 Cookie 差在哪？
- JWT 又是什麼
 1. Base64Url
 2. head
 3. payload
 4. signature
 5. 運作原理
 6. 使用時機

認證與授權

在介紹 Session 與 JWT 前，我們要來談談這兩個單字。以辦信用卡來舉例，通常辦卡前銀行會確認你的收入是否穩定，再來決定是否發行信用卡給你，因此可以分為：

認證

讓銀行知道你的收入是否穩定。

授權

收入通過標準，銀行發行信用卡給你。

Session 是什麼

Session 基於 Cookie，指的是在網路上的「狀態」。被用在身份驗證上是較常見的。

小故事

不知道大家有沒有用 Booking.com 訂房過，他有個機制是你在兩年內訂房超過幾次就可以升級 Genius 會員，還分了很多階級有不同的優惠折扣。

所以當我輸入完帳密登入後，Booking 會先去查看是否有此人，通過了「認證」後，發現我在訂單記錄上超過兩次訂房，所以「授權」了我 Genius 1 級會員的優惠。

Genius 1 級會員

在兩年內完成兩次住宿可解鎖 Genius 1 級會員

您目前所在的等級

Genius 旅遊獎勵

- ✓ 會員資格終生免費
一旦成為 Genius 會員，即可終生享有會員資格
- ✓ 精選住宿 10% 折扣
成為 Genius 1 級會員之後，預訂 Genius 住宿可享 10% 折扣

Genius 2 級會員

在兩年內完成五次住房即可升級為 Genius 2 級會員

Genius 旅遊獎勵

- ✓ 會員資格終生免費
一旦成為 Genius 會員，即可終生享有會員資格
- ✓ 精選住宿 10% 和 15% 折扣
除了現有的 10% 折扣，特定住宿還可享 15% 折扣
- ✓ 部分選項有免費早餐
預訂 Genius 住宿可獲免費早餐
- ✓ 部分選項可免費房型升級
免費房型升級為旅程加分

運作原理

當 Client 輸入帳密登入後，Server 會產生一筆 Session 記錄在伺服器，同時把你的身份特徵 SessionID 送回去 Client 端加密保存 (只有 Server 能解密查看)。之後你在網頁上的操作，Server 只要依據你的 SessionID，就能查看剛剛在你身上存的 Session。

想要清除的話，除了等待 Session 過期，還可以使用網站常有的登出，其實就是由 Server 來幫你消除 Session，另外也可以從 Client 端來清除 Cookie (SessionID)。

與 Cookie 差在哪？

雖然說是基於 Cookie，但不同的是 Session 主要還是存在 Server 端，只有單一個 SessionID 會被送去 Client 端並且加密。

JWT 是什麼？

原名 (JSON Web Tokens)，基本上就是帶時效的 Token。

JWT 主要分為三段，個別為 header、payload 與 signature，中間以 . 做區隔，每一段都是透過 Base64Url 去編碼，中間的 payload 有時候會加密。

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJlbWFpbCI6Imhpcm9AZ21haWwuY29tIn0.WAKjPd_0qcEG3dA9pEwAiw-0ADb8VwqFLSWiIYJTymo
```

Base64Url

與 BASE64 差在最後的 「=」 號會去掉，「-`/」 符號會換成底線「_」，「+」會換成 dash「-」。

header

存放 token 型別與加密方式。

```
{  
  "alg": "HS256", // 加密方式
```

```
"typ": "JWT" // token 型別  
}
```

以 Base64Url 編碼後：

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
```

payload

存放需要傳遞的訊息。因為只透過編碼轉換「未經過加密」，不建議在裡面放重要資訊。

另外官方有提供一些可以用的屬性大概分為：

- iss: 發行人
- exp: 到期日
- sub: 主題
- aud: 收件人
- nbf: 不接受早於...日期/時間
- iat: 發行時間
- jti: 唯一識別符，JWT 只能使用一次

接著我們來看看轉換結果：

```
{  
  "email": "hiro@gmail.com"  
}
```

編碼後：

signature

最後的部分，有點像是我們平常買東西條碼上最後的檢查碼，首先會先取得 header 裡的加密方式 SHA256，再透過以下方式產生：

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

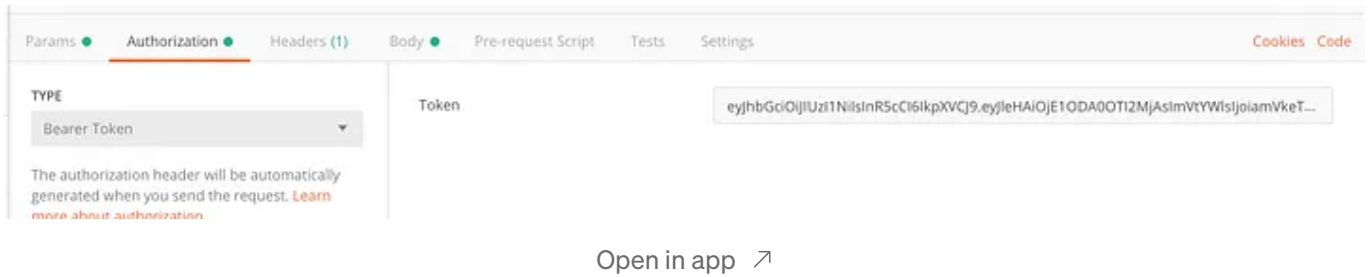
secret 則是可以打上自己要打的，最後一樣會轉換成 Base64Url：
再把三段加在一起就算是 JWT 了！

WAKjPd_0qcEG3dA9pEwAiw-0ADb8VwqFLSWiIYJTymo

運作原理



關於 Auth 則是選擇 Bearer Token，另外也有放在 Body 裡或是 URL 後方的做法，但需要多注意一些細項，詳細可以參考 [Bearer Token 的使用方法](#)。



Search

Write



使用時機

看完上面可以知道，JWT 的主要目的只是「**確立資料來源以及可信度**」。因此在應用上也會限制較多。以下是較常被使用的時機：

- 跨伺服器下的請求

可以參考運作原理的圖，如果我們同時擁有許多伺服器，可以把身份驗證伺服器獨立出來，登入後使用 JWT 就可以在不同伺服器遊走。

- 一次性、時效短的請求

因為 JWT 不能主動撤銷，一般用於會員身份驗證會不太適合，多用於一次性下載檔案，或是時間限制內更改密碼等等...

- APP 身份驗證

一般 APP 是不存在 Session 的，所以在持續身份驗證上可以使用 JWT，但要確保使用者的執行環境是安全的。

結論

常常看到有人會問說：

JWT 可以代替 Session 嗎？

這其實是個假議題，東西存在一定有它的價值。透過 Booking.com 的例子，我們可以得知 Session 能較方便的「授權」不同身份，以及能夠主動撤銷。反之 JWT 不能主動撤銷，出來的 Token 一大坨，除了傳輸上較慢，也需要花較多時間去解碼。

關於更深的資料可以參考：別再使用 JWT 作為 Session 系統！

參考資料

JWT.IO

JSON Web Token (JWT) is a compact URL-safe means of representing claims to be transferred between two parties. The...

jwt.io

淺談JWT的安全性與適用情境

以Python為例，從實作理解JWT並分析其適用性

medium.com

你在用 JWT 代替Session?

现在，JSON Web Tokens (JWT) 是非常流行的。尤其是 Web 开发领域。所有这些因素，令 JWT 名声大振。但是，今天我要来说说使...

segmentfault.com

不要用JWT替代session管理（上）：全面了解Token,JWT,OAuth,SAML,SSO

本文关于 OAuth 授权和 API 调用实例都来自 Google API。token 即使是在计算机领域中也有不同的定义，这里我们说的token，是指...

zhuanlan.zhihu.com

Sessions

Jwt

Jwt Token

Cookies

W3hexschool



Written by 集點送紅利 / Hiro


88 Followers

從日文歪到Frontend

Follow



More from 集點送紅利 / Hiro

 集點送紅利 / Hiro

[Vue] 還是不懂Computed ?

前言

4 min read · Apr 24, 2020



199

1



 集點送紅利 / Hiro

[Node.js] 實作MySQL 圖片上傳

Node.js 搭配MySQL 儲存圖片


10 min read · Feb 5, 2020



39

1



 集點送紅利 / Hiro

初探WebRTC—手把手建立線上視訊(2)

講解WebRTC 實作方式


8 min read · Feb 29, 2020



101

2



 集點送紅利 / Hiro

初探WebRTC - 手把手建立線上視訊(1)

從零建置1對1網頁視訊

4 min read · Feb 22, 2020



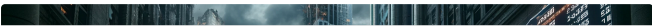
69

1



See all from 集點送紅利 / Hiro

Recommended from Medium




 Ignacio de Gregorio

OpenAI Just Killed an Entire Market in 45 Minutes

The Story Everyone Should Have Seen Coming

★ · 6 min read · Nov 10


 10.6K  151  

 Unbecoming

10 Seconds That Ended My 20 Year Marriage

It's August in Northern Virginia, hot and humid. I still haven't showered from my...

★ · 4 min read · Feb 17, 2022

 69K  999  

Lists



Staff Picks
505 stories · 453 saves



Stories to Help You Level-Up at Work
19 stories · 307 saves

Self-Improvement 101
20 stories · 898 saves

Productivity 101
20 stories · 821 saves

AL Anany 

The ChatGPT Hype Is Over—Now Watch How Google Will Kill...

It never happens instantly. The business game is longer than you know.

★ · 6 min read · Sep 2



18.8K



577



The PyCoach in Artificial Corner

OpenAI Just Released GPTs: Create Your Own ChatGPT And Make...

We're about to see the App Store for AI.

★ · 4 min read · Nov 8



4.2K



70



Nick Wignall

4 Habits of Emotionally Strong People

#1: Control your attention, not your emotions

7 min read · May 13



7.8K



204



FadinGeek

Top 20 mobile apps which nobody knows about...

In the vast ocean of mobile applications, some remarkable gems often go unnoticed. While...

6 min read · May 28



6.4K



159



See more recommendations