JWT

JWT وهو اختصار لـJSON Web Token ، وهي طريقة آمنة لنقل البيانات المشفرة بين الطرف المُرسِل والمُستقبِل.

يتكون الـ JWT من ثلاثة أجزاء رئيسية:

1. الـ Header: وهو جزء يحتوي على معلومات حول نوع الترميز المستخدم ونوع الشفرة.
2. الـ Payload: وهي البيانات الفعلية التي يتم نقلها، مثل معرف المستخدم، وتاريخ انتهاء الصلاحية.
3. الـ Signature: وهو جزء يستخدم لتأكيد صحة الـJWT ، ويتم إنشاؤه من خلال تشفير الـ Header والـ Payload باستخدام Secret Key .

طريقة عمل الـ JWT :

1. عند تسجيل الدخول، يقوم الـ Server بإنشاء JWT وإرسالها إلى المتصفح.
2. يقوم المتصفح بتخزين الـToken في ملف الكوكيز أو في التخزين المحلي.
3. عند إجراء طلب إلى الـServer ، يقوم المتصفح بإرسال الـ Token مع الطلب في رأس الطلب.
4. يقوم الـ Server بفك تشفير الـ JWT وفحص صحتها باستخدام الـSecret Key.
5. إذا كانت الـ Token صحيحة، يسمح الـ Server بالطلب. وإذا كانت غير صحيحة، يرفض الـ Server الطلب.

اهم الخصائص:

1. يمكن إعطاء صلاحيات مؤقتة للمستخدم عن طريق تحديد مدة صلاحية ال Token.
2. يسمح بنقل البيانات المهمة دون الحاجة للاتصال الى قاعدة البيانات.
3. يعتمد على العميل في حفظ الحالة بدلا من ال Server.