**تعريف JWT ومما يتكون :**

تعني اختصار "JSON Web Token"

وهو معيار لتبادل المعلومات بين الخادم والعميل بطريقة آمنة , حيث يمكن التحقق من صحة المعلومات ومصداقيتها بسهولة , عبارة عن نص String مشفر يتكون من ثلاثة أجزاء: الرأس (Header)، الحمولة (Payload)، والتوقيع (Signature).

1- Header : يحتوي على نوع التشفير algorithmو نوع الأمان JWT

2- Payload: يحتوي على البيانات التي يتم نقلها مثل معلومات المستخدم .

3- Signature : تستخدم لتحقق من أن الجزء الأول والثاني بياناته موثوقة ولم يتم التغير والتعديل عليها عبر التوقيع عليها باستخدام مفتاح سري secret key.

**طريقة عمل JWT:**

- يقوم المستخدم بتسجيل الدخول ويقدم بيانات اعتماده.

- يولد الخادم JWT إذا كانت بيانات الاعتماد صحيحة، يقوم الخادم بإنشاء JWT ويرسله إلى المستخدم.

- المستخدم يستخدم JWT في طلبات لاحقة بحيث يتم إرفاق JWT في رأس الطلب (Header)، مما يسمح للخادم بالتحقق من هوية المستخدم.

مثال : عندما يقوم المستخدم بعملية login أول مره البيانات المدخلة ترسل ل Server ثم يقوم الخادم بإرسالها ل database لتحقق من أن هذا المستخدم موجود أم لا اذا كان المستخدم موجود فعلا يتم ارسال token معين للمستخدم بحيث لو قام المستخدم بأي requests يتم معرفته من قبل token الخاص به .

**مزايا استخدام JWT وسلبياتها :**

-**الأمان:** يوفر وسيلة آمنة وفعالة لتبادل المعلومات بواسطة مفتاح سري، مما يجعلها صعبة الاختراق والتلاعب بها.

**المرونة و سهولة الاستخدام:** JWT سهلة الاستخدام ومفهومة متاحة للاستخدام في العديد من لغات البرمجة الشائعة.

**لا حاجة للتخزين:** لا حاجة للحفاظ على حالة الجلسة على الخادم، مما يقلل من التحميل

**من سلبياتها :**

**حجم البيانات:** في بعض الحالات، يمكن أن تكون حجم بيانات JWT كبيرًا، خاصة عند تضمين معلومات إضافية في الجسم (Payload).

الخلاصة: JWT هو أداة قوية للمصادقة والأمان في تطبيقات الويب. باستخدامه، يمكن تأمين الاتصالات بين الخادم والعميل وضمان تبادل البيانات بشكل آمن.