مفهوم JSON Web Token (JWT) :

- المقدمة
- تعريف JWT وأهميته في تبادل البيانات.
- دور JWT في أنظمة المصادقة الحديثة.

- 1. ما هو JWT؟
- تعريف JWT كمعيار مفتوح (RFC 7519).
- مكوناته الرئيسية:
.نوع التوكن وخوارزمية التشفير :**(الرأس) Header** -
"claims". البيانات أو :**(الحمولة) Payload** -
.لضمان سلامة البيانات :**(التوقيع) Signature** -

- 2. كيفية عمل JWT
- خطوات إنشاء JWT:
  - تسجيل دخول المستخدم.
  - إنشاء التوكن بواسطة الخادم.
  - إرسال التوكن إلى العميل.
- كيفية استخدام JWT في الطلبات اللاحقة (ترويسة HTTP).

- 3. مزايا استخدام JWT
- **أمان**: تشفير التوكن والتحقق من صحته.
- **محمول**: يمكن استخدامه مع تقنيات متعددة.
- **كفاءة**: لا حاجة للرجوع إلى قاعدة البيانات في كل طلب.

- 4. عيوب JWT
- حجم البيانات: قد يكون أكبر من بعض أساليب المصادقة الأخرى.
- فقدان السيطرة: إذا تم تسليم التوكن بشكل غير صحيح، قد يؤدي ذلك إلى مشاكل في الأمان.

- 5. تطبيقات JWT
- أنظمة المصادقة (Authentication) في الويب.
- خدمات الواجهة البرمجية (APIs).
- تطبيقات الهاتف المحمول.

- 6. مقارنات مع أساليب أخرى
- مقارنة JWT مع تقنيات المصادقة الأخرى مثل OAuth وSession-based authentication.
- المزايا والعيوب لكل تقنية.

- 7. أمثلة عملية
- مثال على كيفية إنشاء JWT في لغة برمجة معينة (مثل JavaScript أو Python).
- كيفية التحقق من صحة التوكن في خادم.

- 8. الأمن والتحديات
- التحديات المرتبطة باستخدام JWT.
- أفضل الممارسات لضمان أمان JWT.

- الخاتمة
- تلخيص النقاط الرئيسية حول JWT.
- أهمية JWT في تطوير تطبيقات الويب الحديثة.

-المراجع
- قائمة بالمصادر المستخدمة في البحث، مثل الوثائق الرسمية وكتب البرمجة.