أكاديمية طـويـق
TUWAIQ ACADEMY

JWT

JWT هي اختصار لـJSON Web Token" وهو نموذج لتبادل المعلومات بين طرفين بطريقة امنه وموثوق بها ، يستخدم المصادقة والتأكيد على الهوية في تطبيقات الويب.

هيكل JWT :

١. **Header (الرأس):** يحتوي على نوع الرمز (مثل "JWT") ونوع خوارزمية التوقيع المستخدمة.
٢. **Payload (الحمولة):** تحتوي على المعلومات الفعلية. مثل معرف المستخدم أو الصلاحيات.
٣. **Signature (التوقيع):** توقيع رقمي (مفتاح سري) بين العميل والخادم يتم استخدامه للتحقق من ان الرمز لم يتم تزويره وان المعلومات لم يتم تغييرها

يتم تشفير هذه الأقسام الثلاثة بواسطة خوارزمية معينه .

كيفية عمل JWT :

١. **إصدار الرمز (Token Issuance):** يتم إصدار رمز JWT بعد نجاح عملية المصادقة، مثل تسجيل الدخول بنجاح.
٢. **إرسال الرمز (Token Delivery):** يتم إرسال الرمز JWT إلى العميل، عادة في هيدر الطلبات الخاصة بالويب أو كجزء من استجابة ناجحة لطلب تسجيل الدخول.
٣. **تخزين الرمز (Token Storage):** يتم تخزين الرمز JWT في ذاكرة التخزين المحلية على العميل للاستخدام المستقبلي.
٤. **إرسال الرمز مع الطلبات (Sending Token with Requests):** يتم إرسال الرمز JWT مع كل طلب يتم إرساله إلى الخادم المحمي.
٥. **التحقق من صحة الرمز (Token Verification):** يتم التحقق من صحة الرمز JWT عند استلامه على الخادم، وذلك عن طريق فك توقيعه والتأكد من صحة البيانات المرسلة. إذا كان التوقيع صحيحًا، يتم قبول الرمز واستخدام المعلومات الموجودة في الحمولة لاتخاذ الإجراءات المناسبة، مثل منح الوصول إلى الموردين المحمية أو تحديث حالة تسجيل الدخول للمستخدم.

الاستخدامات الشائعة لـ JWT:

١. **المصادقة المركزية (Single Sign-On - SSO):**
يمكن استخدام JWT لتنفيذ نظام المصادقة المركزية، حيث يتم إصدار رمز JWT بعد تسجيل الدخول بنجاح، ثم يُستخدم هذا الرمز لتوفير الوصول إلى مختلف التطبيقات دون الحاجة إلى إعادة تسجيل الدخول.
٢. **تأمين واجهات برمجة التطبيقات (APIs):**
يمكن استخدام JWT لحماية واجهات برمجة التطبيقات (APIs) من الوصول غير المصرح به. يتم تضمين رمز JWT في كل طلب API، ويتم التحقق من صحته لمعرفة هوية المستخدم وصلاحياته.
٣. **تأمين التبادل بين الخوادم (Server-to-Server Communication):**

يمكن استخدام JWT لتأمين التبادل بين الخوادم في تطبيقات الميكرو سيرفيس أو النظم الموزعة، حيث يتم تضمين الرمز JWT في طلبات الخدمات للتحقق من هوية الخادم المرسل وضمان سلامة البيانات المرسلة.

٤. **تخزين المعلومات (Information Storage):**
يمكن تضمين المعلومات المهمة داخل الحمولة (Payload) لرموز JWT، مثل معلومات المستخدم أو إعدادات التطبيق، وتخزينها بشكل آمن ومشفر داخل الرمز.

٥. **التحقق من الهوية (Identity Verification):**
يمكن استخدام JWT للتحقق من هوية المستخدم وصحة جلساته، حيث يتم تضمين معلومات مثل معرف المستخدم والصلاحيات داخل الرمز، ويتم التحقق من صحته لضمان أن المستخدم معتمد.

الإيجابيات والسلبيات الرئيسية لاستخدام JWT:

الإيجابيات:

١. **بساطة الاستخدام:** JWT سهلة الاستخدام وفعالة في نقل المعلومات بين العميل والخادم.
٢. **مقاومة للاختراق:** يتم توقيع كل رمز JWT بواسطة مفتاح سري، مما يجعلها مقاومة للتزوير عند استخدام خوارزميات التوقيع الآمنة.
٣. **قابلية التوسع:** يمكن استخدام JWT في البيئات الموزعة والمتوسعة مع الاحتفاظ بأداء جيد.

السلبيات:

١. **حجم الرموز:** قد يكون حجم رموز JWT أكبر من غيرها من طرق المصادقة مثل الجلسات، مما يمكن أن يؤدي إلى زيادة حجم حزم البيانات المنقولة.
٢. **عدم القابلية للإلغاء:** بمجرد إصدار رمز JWT، فإنه يظل صالحًا حتى انتهاء صلاحيته، ولا يمكن إلغاؤه أو إبطاله قبل ذلك، مما يزيد من فترة تعرضه للاستخدام غير المصرح به.
٣. **تخزين المعلومات الحساسة:** يمكن تضمين معلومات حساسة داخل الرموز JWT، وعلى الرغم من أنها مشفرة، فإنها قابلة للاستخراج والقراءة بواسطة أي شخص يحصل على الرمز.
٤. **إدارة الحالة (State Management):** لا تتم مشاركة حالة الجلسة بين الخادم والعميل مع JWT، مما يعني أن الخادم لا يمكنه إلغاء الجلسة أو تحديثها بسهولة.

ساره الهزاع