

:JWT (JSON Web Token)

JWT هو طريقة stateless لتوثيق المستخدمين. عند تسجيل المستخدم أو تسجيل دخوله، يقوم السيرفر بإصدار Token تحتوي على معلومات المستخدم ويتم توقيعها بمفتاح سري (secret key). يتكون الـ JWT من:

1. Header: يحدد نوع الـ token وخوارزمية التشفير.
2. Payload: يحتوي على بيانات المستخدم مثل الـ ID وتاريخ انتهاء الصلاحية،
.username
3. Signature: يتم توقيعها لضمان عدم التلاعب بالـ token باستخدام secret key.

بما أن الـ token يحتوي على جميع البيانات، لا يتم تخزين الجلسات في قاعدة البيانات.

المزايا: تحسين الأداء وتقليل الحمل على السيرفر.

العيوب: إذا تم تسريب الـ token، يمكن استغلاله حتى انتهاء صلاحيته. للحماية، يمكن استخدام تاريخ انتهاء صلاحية قصير أو Refresh Token.