JWT (JSON Web Token) es un estándar abierto para crear tokens de acceso que permiten a un usuario verificar su identidad en una aplicación. Esencialmente, es una forma segura de transmitir información entre un cliente y un servidor.

¿Para qué sirve?

JWT se utiliza principalmente para la autenticación y autorización de usuarios en aplicaciones web y APIs. En lugar de almacenar la sesión del usuario en el servidor, el servidor le da al cliente un token que contiene toda la información necesaria para verificar que el usuario está autenticado y tiene los permisos adecuados. Esto hace que las aplicaciones sean más escalables y eficientes, ya que el servidor no tiene que hacer un "viaje a la base de datos" para cada solicitud.

¿Cómo funciona?

Un JWT se compone de tres partes, separadas por puntos:

-Header (Cabecera): Describe el tipo de token (JWT) y el algoritmo de encriptación utilizado, como HMAC SHA256 o RSA.

-Payload (Carga útil): Contiene las "claims" (declaraciones), que son afirmaciones sobre el usuario, como su ID, nombre, roles, etc. También puede incluir información de expiración. No debes guardar información sensible aquí, ya que es fácilmente decodificable.

-Signature (Firma): Se crea al tomar el header y el payload, codificarlos, y luego firmarlos con una clave secreta que solo conoce el servidor. Esta firma es lo que hace que el token sea inviolable.

Cuando un usuario envía una solicitud con un token JWT al servidor, el servidor utiliza la clave secreta para verificar la firma. Si la firma es válida, sabe que la información del token no ha sido alterada y que proviene de una fuente de confianza.

Analogía del auto, imagina que quieres alquilar un auto:

- Sin JWT: Para cada viaje que haces, tienes que ir a la oficina de alquiler para que verifiquen tu licencia y te den la llave del auto. Cada vez que vuelves a buscar el auto, tienes que repetir este proceso. Esto es ineficiente y lento.
- Con JWT: Alquilaste el auto y, en lugar de darte solo la llave, te dan un carnet de identificación temporal sellado por la oficina de alquiler. Este carnet tiene tres partes:

  -El tipo de auto que te dieron (Header).

  -Tus datos personales, tu nombre y la fecha de expiración del alquiler (Payload).

  -El sello de la oficina de alquiler (Signature).

Ahora, cada vez que quieres usar el auto, no tienes que volver a la oficina. Simplemente le muestras el carnet al guardia de seguridad del estacionamiento. El guardia no necesita llamarle a la oficina, simplemente ve el sello (la firma) para asegurarse de que el carnet no es falso. Si el sello es válido, te deja pasar, ya que confía en que la oficina ya verificó tus credenciales.

En resumen: El token JWT es como ese carnet de identificación sellado. Le permite al servidor confiar en la información que el cliente le proporciona sin tener que realizar una verificación de credenciales completa en cada solicitud.