**Token JWT**

**Objetivo**: Explicar de manera detallada y completa el funcionamiento y la estructura del token JWT, incluyendo los procesos de generación, verificación y uso en aplicaciones web y servicios API.

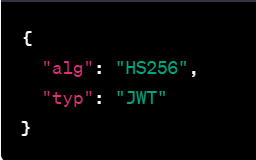
**Descripción del plato a preparar:**

El token JWT (JSON Web Token) es un estándar abierto (RFC 7519) que define un formato compacto y seguro para transmitir información entre partes como objetos JSON. Se utiliza ampliamente en aplicaciones web y servicios API para la autenticación y autorización de usuarios, ofreciendo portabilidad, seguridad y flexibilidad.

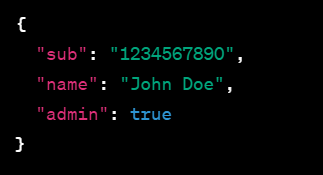
**Recursos necesarios:**

**Conceptos clave:**

* Token JWT: Un token JWT es una cadena de caracteres que consta de tres partes: el encabezado, la carga útil y la firma. Es utilizado para transmitir información de manera segura entre diferentes partes.
* Encabezado (Header): El encabezado especifica el tipo de token y el algoritmo de firma utilizado para protegerlo. Por ejemplo:



* Carga útil (Payload): La carga útil contiene la información que se quiere transmitir, como identificadores de usuario, roles, permisos, entre otros. Puede incluir tres tipos de afirmaciones: "registered claims", "public claims" y "private claims". Por ejemplo:



* Firma (Signature): La firma se utiliza para verificar la integridad del token. Se crea utilizando el encabezado codificado en Base64, la carga útil codificada en Base64 y una clave secreta conocida solo por el servidor. Por ejemplo: HMACSHA256(base64UrlEncode(header) + "." + base64UrlEncode(payload), secret).
* Estructura del token JWT: El token JWT consta de tres partes separadas por puntos ("."): el encabezado, la carga útil y la firma. Por ejemplo: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiAiMTIzNDU2Nzg5MCIsICJuYW1lIjogIkpvaG4gRG9lIiwgImFkbWluIjogdHJ1ZX0.5YQRG2ZnW71X06HkLuzQsVFyY-RzyeuRC9XrTG6V8w0.

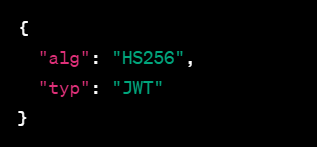
**Pasos:**

**1. Preparar los conceptos clave:**

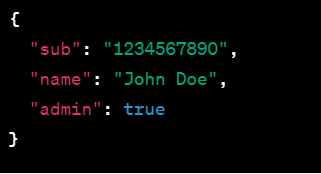
* Explicación del token JWT: Un token JWT es una cadena de caracteres que consta de tres partes: el encabezado, la carga útil y la firma. Cada parte tiene un propósito específico en la estructura del token.
* Encabezado (Header): El encabezado del token JWT especifica el tipo de token y el algoritmo de firma utilizado para protegerlo.
* Carga útil (Payload): La carga útil del token JWT contiene la información que se quiere transmitir. Puede incluir datos como identificadores de usuario, roles, etc.
* Firma (Signature): La firma del token JWT se utiliza para verificar la integridad del token y asegurar que no ha sido alterado.

**2. Comprender la estructura del token JWT:**

* El token JWT consta de tres partes separadas por puntos ("."): el encabezado, la carga útil y la firma.
* El encabezado contiene metadatos sobre el token, como el tipo de token y el algoritmo de firma utilizado. Por ejemplo:



* La carga útil contiene la información que se desea transmitir. Por ejemplo:



* La firma se utiliza para verificar la integridad del token y asegurar su autenticidad.

**3. Generar un token JWT:**

* Codificar el encabezado y la carga útil en objetos JSON separados.
* Codificar los objetos JSON resultantes en Base64 para obtener las partes codificadas en Base64 del token.
* Utilizar el algoritmo de firma especificado en el encabezado (por ejemplo, HMAC-SHA256 o RSA) para generar la firma utilizando una clave secreta o privada.
* Combinar las partes codificadas en Base64 del encabezado, la carga útil y la firma, separadas por puntos, para formar el token JWT completo.

**4. Verificar y utilizar un token JWT:**

* Un cliente o servidor puede recibir un token JWT y verificar su autenticidad.
* Separar las partes del token decodificándolo utilizando Base64.
* Verificar la firma utilizando la clave secreta o pública correspondiente.
* Si la firma es válida, se puede confiar en la información contenida en el token y utilizarla para autenticar y autorizar al usuario.

**5. Transmitir y utilizar el token JWT:**

* El token JWT puede transmitirse fácilmente en las solicitudes HTTP o incluirse en las cabeceras de autenticación, como el encabezado "Authorization: Bearer <token>".
* Al enviar el token, se recomienda utilizar conexiones seguras (HTTPS) para proteger la confidencialidad y la integridad del token durante la transmisión.

**6. Explorar las ventajas del token JWT:**

* Los tokens JWT ofrecen portabilidad, ya que pueden ser utilizados en diferentes sistemas y plataformas que admitan el estándar JWT.
* Proporcionan seguridad al permitir la verificación de la firma y la detección de cualquier manipulación del token.
* Ofrecen flexibilidad al permitir incluir información adicional más allá de la autenticación, como datos de autorización y otros atributos relevantes para la aplicación.