What is JSON Web Tokens (JWT) ?

MALEK BENTAHER

JWT

- A JWT (or JSON Web Token) is an open standard used to share security information between two parties: a client and a server.

- Each JWT contains encoded JSON objects, including a set of claims.

- These claims can represent various pieces of information, such as user identity, permissions, or other relevant data.

MALEK BENTAHER

Structure of JWT

A JWT consists of three parts:

- Header: Contains information about the algorithm used for signing the token.
- Payload: Contains the actual claims (data) you want to transmit.
- Signature: Ensures the integrity and authenticity of the token.

MALEK BENTAHER

Use Cases

- **Authentication: JWTs are commonly used for user authentication. After a user logs in, the server generates a JWT, which the client includes in subsequent requests.**

- **Authorization: JWTs can carry authorization information, allowing clients to access specific resources based on their roles or permissions.**

- **Single Sign-On (SSO): JWTs facilitate seamless authentication across multiple services without the need to re-enter credentials.**

Best Practices

- Set an expiration time to limit the token's validity.

- Always use HTTPS to transmit JWTs to prevent man-in-the-middle attacks.

- Avoid storing sensitive information in JWT payloads, as they are visible to anyone who has access to them.

MALEK BENTAHER

THANK YOU FOR READ

MALEK BENTAHER