JWT Tokens

What is a JWT Token?

JWT stands for JSON Web Token. It is a compact, URL-safe means of representing claims to be transferred between two parties. These tokens are used to authenticate and authorize users in applications.

How does a JWT Token work?

A JWT token consists of three parts: Header, Payload, and Signature, separated by dots (`.`). The process involves the following steps:

1. **Header**: Contains metadata about the type of token and the hashing algorithm used.
2. **Payload**: Contains claims, which are statements about an entity.
3. **Signature**: Created by encoding the header, payload, and a secret key using the specified algorithm. It ensures the token's integrity.

Why are JWT Tokens used?

- **Stateless**: Since JWT tokens carry all the required information, server-side storage of session data is not necessary, making it stateless.
- **Security**: The signature ensures that the token has not been tampered with.
- **Efficiency**: Being compact, JWT tokens are efficient to transmit and process.