SPRING SECURITY JWT

SPRING BOOT

WALEED MOHAMMED MUTIQ ALTHUBYANI

Spring Security JWT

Json web token (JWT) is a widely used mechanism for securing RESTful APIs. It provides stateless authentication, which means that the server doesn't store any user session information on the backend but stores it in local storage or as a cookie.

JWT structure

1- Header: contains the token data such as the algorithm used in creating it.
2- Payload: contains the user information such as username and role.
3- Signature: make sure that the first two are valid against a secret key.

Authentication flow

When a user successfully logs in, the server will generate a JWT, sings it with a secret key then sends it to the client. For the remainder of the session any action a user takes the server will validate the token and if it passes, will grant access.

Benefits of JWT

1- Stateless authentication.
2- Decentralized authentication: JWT can be used across multiple services since the token contain all necessary user date.
3- Performance: Reduce the need for sending queries to the database for each request.

Challenge of JWT

1- Token revocation: Since JWT is stateless it is difficult to revoke a token before its expiration date.
2- Secure storage: If a JWT is exposed the attacker could impersonate the user until the token expiration date.