Spring Security JWT

(Spring Security Exercise – Durrah Dahash)

What is JWT, and How is it Used on Websites?

* Definition:

JWT, or **JSON Web Token**, is a secure and compact token format used to transmit user information between a website and its backend server. It is commonly utilized for authentication and authorization.

*Components of JWT:

1- **Header**: Specifies the token type (JWT) and the signing algorithm (e.g., HS256).

2- **Payload**: Contains claims, such as user information and metadata.

3- **Signature**: Verifies the token's integrity and ensures it hasn't been tampered with.

*How JWT Works:

1- The server generates a JWT after successful login and signs it is using a secret key.

2- The client stores the token (e.g., in cookies or localStorage).

3- For every request to protected resources, the client sends the token in the Authorization header.

4- The server validates the token to ensure the user is authenticated.

JWT is widely used in modern websites to enable secure, stateless, and efficient communication between the frontend and backend.