Java Bootcamp – Day 45 – Exercise (JWT)

Submitted by: Nawaf AlMutairi

Date 22/12/2024

Question 1: What is JWT?

- JWT (JSON Web Token) is a compact, URL-safe method of representing claims between two parties (a client and a server). It is widely used for authentication and information exchange in web applications.

Question 2: What is the JSON Web Token structure?

A JWT is made up of three parts, separated by dots (.):

1- Header
2- Payload
3- Signature

A JWT typically looks like the following:

- xxxxx.yyyyy.zzzzz

- **Header:** Contains metadata, including the token type (e.g., JWT) and the signing algorithm (e.g., HS256 or RS256).
- **Payload:** Contains the claims or data being transmitted, such as user ID, role, or session information. This part is typically base64-encoded.
- **Signature:** A cryptographic signature is created by combining the header and payload with a secret key or private key. It ensures the integrity and authenticity of the token.

Question 3: What are the use cases of JWT?

- **Authentication:** To validate and identify users securely.
- **Authorization:** To grant or deny access to resources based on roles or permissions.
- **Information Exchange:** To transmit secure data between two parties.

Question 4: What are the advantages of JWT?

- **Compact:** It is lightweight and easy to transmit in URLs, HTTP headers, or cookies.
- **Self-contained:** The token includes all the necessary information, reducing the need for additional database lookups.
- **Cross-domain:** JWTs are suitable for Single Sign-On (SSO) scenarios as they can be used across different domains.
- **Security:** Supports signing and optional encryption to ensure data integrity and confidentiality.