**4. Spring Security**

**OAuth2 Authentication:**

• **Theory:**

1. **Introduction to OAuth2 and how it is used for third-party authentication (Google, Facebook):-** OAuth2 (Open Authorization 2.0) is a protocol that allows secure authentication and authorization for web and mobile applications without exposing user credentials. It enables users to log in using third-party providers like Google, Facebook, GitHub, etc.
2. **Explanation of OAuth2 flows: Authorization Code Grant, Implicit Grant, etc:-**

OAuth2 Flows (Short & Simple)

1️.uthorization Code Grant (Most Secure)  
 Used for web apps (server-side).  
 User logs in → gets authorization code → exchanged for access token securely.

2️.Implicit Grant (Deprecated, Less Secure)  
 Used for SPAs (JavaScript apps).  
 User logs in → access token sent directly in URL (security risk).

3️.Password Grant (For Internal Apps)  
 User enters username & password → app gets access token directly.  
 Not recommended for third-party apps.

4️.Client Credentials Grant (For APIs & Servers)  
 No user login, only app authentication.  
 App sends Client ID & Secret → gets access token to call APIs.