

**Authorization Code flow in OAuth 2.0**

1. **Authorization Request Initiation:** The client application requests access to the user's data by hitting the OAuth authorization server's /authorization endpoint, passing parameters such as **client\_id**, **redirect\_uri**, **response\_type=code**, **scope**, and **state**. This kicks off the OAuth process.
2. **User Login and Consent:** The user logs into their account on the authorization server and consents to the access of their data as defined by the requested scopes (**scope**). If the user has previously granted consent, this step may be skipped.
3. **Authorization Code Reception:** Following user consent, the browser is redirected to the client application's **redirect\_uri** with an authorization code included in the query parameters.
4. **Access Token Request:** The client application exchanges the received authorization code for an access token by making a request to the authorization server, including **client\_id**, **client\_secret**, **redirect\_uri**, **grant\_type=authorization\_code**, and the received code.
5. **Access Token Issuance:** Upon successful authentication and validation of the request, the authorization server issues an access token, the token type, its lifetime, and the permitted scopes (**scope**).
6. **Accessing Protected Resources:** With the access token, the client application can request protected resources by including the token in the Authorization header.
7. **Resource Access Granted:** The resource server verifies the token's validity and, upon successful verification, provides the requested user data corresponding to the allowed **scope**.