**OAuth2.0**

* Open Authorization(free)
* Allows users to share private resources (photos, videos ext.) to third party while keeping credentials secret
* Actors in OAuth:

1. Resource Server:

* validates access token and serves protected resources
* Hosts user owned resources protected by OAuth.

1. Resource Owner:

* User of the application
* can grant or deny access to the user owned services hosted on Resource Server

1. Authorization Server:

* gets consent from resource owner and issues access tokens to client for accessing protected services hosted on resource server.

1. Client:

* Application making API requests to perform protected services on behalf of Resource Owner.
* Before doing it must be authorized by resource owner and authorization must be validated by resource server/authorization server.
* Types based on confidentiality:
  + 1. *Confidential*: maintains confidentiality of credentials (ex: Appl running on web server)
    2. *Public*: incapable of maintaining confidentiality of credentials. (web browser-based application) and incapable of secure authentication
* Grant types: To get access code, client obtains authorization from Resource owner. This can be expressed in the form of grant types. Types:

1. Authorization code: for confidential clients
2. Implicit grant: for public clients.
3. Resource owner password credentials: when Resource owner trusts client and provides his credentials to client
4. Client Credentials: when client itself owns the data and does not need to get authorization from Resource owner

**CSRF:** Cross site request Forgery