**Spring Security**

By default the Spring Security gives us the password(display on log when project started with username and ‘user’) using which we can login into the system.

Now by default all the endpoints are disabled i.e (/register,/signup,/login)

To whitelist/enable these endpoints we need to do configuration so that these endpoints can bypass the security.

**OAuth:-** Open Authorization

OAuth is used to authenticate the user which will access the resources once authorized.

**Resource Owner**:- Resource owner is the server/machine which holds/stores the resources.

**Client:-** User who is trying to access the resources

**Authorization Server:-** Is the server which will send the access tokento the requested client using which the client will access the resources from the resources server once the access token is verified.

**Resources Server:-** Server that protects the user resources and receives the access request from the client. It accepts and validates the access token from the client and returns the appropriate resources.

**Combining OAuth with OpenID gives complete Authorization and Authentication.**