1. While creating user redirect to login
2. While login encrypt the id of user with jwt and send the token to frontend
3. In front end set the token in localstorage
4. Using http Interceptors in providers at app module will add headers with jwt token for every request
5. Passport can validate token based on jwt and social platforms

**Steps for creating passport with JWT:**

1. While login encrypt the user returned user id with jwt and send the token
2. In frontend while receiving response store the token in local storage
3. Create http-interceptor class in angular and add http-interceptor in providers of root module of required components we need to ingest.
4. Http- interceptor class has functions to set token in header from local storage if its present.
5. Add app.use(passport.initialize()) and app.use(passport.session()) and configureJWTStrategy function which has function to process the token we send from angular and return whether its valid or not.
6. Wherever we need to include authentication include passport.authenticate("jwt", { session: "false" }), so when route is triggered it uses function inside configureJWTStrategy.
7. Include function for serialize and deserialize user in app.js