# Full Stack Development - I

**COMP 3123**

# Goals For This Authentication System

- **Private and public routes**: This application will have basic "landing" pages, which any user can visit. Along with these, signing up and logging in should be declarative public routes. On the other hand there will be many pages that require authentication to view.

- **Redirect to Login**: If the user does not have tokens, or the token refresh does not work, the user will automatically be redirected to the Login page if they attempt to see a private route.

- **Redirect to referrer**: If a user wants to view a specific page, but does not have a valid token, they will be redirected to the login page. We want to make sure that after logging in they're sent to the page they originally wanted. The default will be the dashboard.

- **Authentication Tokens**: We'll use tokens to read and write authentication with. These should be stored in local storage so the user can stay logged in if they leave the site.

- **UI is intuitive and straightforward**: This really isn't going to be much of an "examination" on the UI aspect, but I do think it's essential for our Login and Sign up page to be simple, and follow the do's and don'ts outlined by Brad Frost here.

**What is OAuth**

- OAuth is an open-standard authorization protocol.
  - For example, you can login to any site(BBC) without keep separate username and password for that & login with Facebook or Google.
  - Since Facebook knows your identity it allows access to BBC site.
  - Facebook act as a authorization server & use authorization token for granting access.

**What is AuthO**

- AuthO is 3rd party tool providing Authentication & Authorization as a service.

- With AuthO developers and companies can secure their applications without having to become security experts.

- AuthO provides simple & secured login for any type of platform & any type of devices. AuthO is free up to 1000 external users.

- For Enterprise level configuration developers or companies have to get a subscription.

**Why Auth0**

- Authentication and Authorization implementation is not an easy Task.

- When it comes to different type of devices, technologies and platforms, it will take lot of time to research and Development using different Technologies.

- AuthO will simplify the work and Provide Many Built-in services.

# Some Features provided by AuthO

- **Standard Protocols**

    Auth0 supports industry standards such as SAML, OpenID Connect, JSON Web Token, OAuth 2.0, OAuth 1.0a, WS-Federation and OpenID.

- **Multi-factor Authentication**

    Enhanced security to your application. With Auth0 you can enable Multi factor Authentication in minutes.

- **Single Sign On**

    Let your users log into multiple applications just once by following some simple steps.

- **Social Login**

    Simplify registrations and logins for end users allowing them to use existing login information from their favorite social network provider.

- **Simple Apis**

    Auth0 allows you to authenticate and authorize apps and APIs with any identity provider running on any stack on any device or cloud.

Example & Demo

Read more here

Thank You