* Course Overview
* Intro
  + Json Web Tokens(JWT)
* Why Use an Auth Provider
  + Authentication: Who are you?
    - Login with email and password
  + Authorization: What are you allowed to do?
    - Check user rights
  + Auth0, Okta
    - OAuth provider
* OAuth 2.0
  + Auth0 is security provider
  + OAuth is security protocol
  + OAuth 2.0 is about authorization
  + Scope is permission
    - String they denotes type of access
    - Like read only, write, etc
  + OAuth
    - Authorization protocol
    - Authorize a user without their password
    - Get info from a third party
  + OAuth setup
    - Register with service(google, facebook, etc)
    - Give app name, website, callback url
    - Auth0 handles this for us
  + OAuth roles
    - Resource owner: user
    - Client: app that want to access user account
    - Auth Server: auth logic, provides access token
    - Resource Server: api application want to access, user data
* Choosing an OAuth Flow
  + Client ap sent auth request to user
  + User accepts request and sends back auth grant to app
  + App sends grant to auth server
  + Auth server sends app access token
  + App use access token to call api in resource server
  + Resource server returns data
  + Grant(aka flow)
    - A way to receive an access token
  + Implicit Flow
    - Your app directs the browser to the Auth0 sigin-in
    - Auth0 redirects your app, at the callback url you chose
    - Your app reads the tokens from the URL
  + OAuth is for authorization not authentication
  + Use OpenID Connect for authentication
* OpenID Connect
  + OAuth is for authorization
    - No standard for scopes and user info requests
  + Nice to avoid managing passwords ourselves
  + OpenID Connect
    - Authenticate users without managing passwords
    - Sits on top of OAuth2.0
    - OAuth2.0 sits on top of http
    - Adds ID Token(JWT), userinfo endpoint, standard scopes(permissions)
  + Using Auth0 we don’t have to implement OpenID connect from scratch
* JSON Web Tokens
  + JWT
  + Access token
  + Used for authorization and info exchange
  + Often contains user info
  + Pronounced “JOT”
  + Digitally signed
  + Can be encrypted
  + JSON is less verbose than XML
  + Smaller when encoded
  + Easier to sign than SAML
  + JSON is easy to parse on the client
  + JWT Parts
    - Header
      * Type, hash algorithm, key id
    - Body
      * User identity claims
    - Signature
      * Verify the sender assure content is legit
  + JWT looks like a bunch of random letters
  + Use <http://jwt.io> to decode JWTs
  + OpenID Connect uses identity token
  + OAuth2.0 uses access token
  + JWTs can’t be revoked
    - So make their lifespan short
    - Auth0 default to 10 hours
* Summary
  + Login and receive JWT identity token(OIDC)
  + Authorize app and receive access token(OAuth 2.0)
    - For api calls
  + Include your access token in API calls for authorization
  + Use identity tokens for authentication
    - Contains user information
  + Use access tokens to access APIs
    - Contains scopes to describe user permissions
* Intro
  + create-react-app
  + react router
* Tools We’re Using in this Cour..
  + Github.com/facebook/create-react-app
  + Install latest version of node.js
  + Install code editing tool like visual studio code
* Create App via create-react-a…
  + running at least Node 6 and npm 5.2
  + in command line type to check
    - node -v
    - npm -v
  + on older versions
    - npm install -g create-react-app
    - create-react-app react-auth0
  + in v6 and above type
    - npx create-react-app react-auth0
  + cd in the folder created
  + type to start react app
    - npm start
  + open the app in vs code
  + install reactjs code snippets package
  + create a ‘Home’ file in src folder
    - type rcc and hit enter to have component snippet generated
    - add <h1>Home</h1> in between the <div> in the return ()
  + create a ‘Profile’ files in src folder
    - remove <div> and add <h1>Profile</h1>
  + in App.js
    - remove everything inside of <div classNampe=”App”> but leave the tags
  + open the visual studio code terminal
  + install dependency(bit.ly/ps-auth0 to get the updated npm install line)
    - npm install auth0-js@9.13.4 auth0-lock@11.25.1 express@4.17.1 express-jwt@5.3.1 express-jwt-authz@1.0.0 jwks-rsa@1.3.0 npm-run-all@4.1.5 react-router-dom@5.2.0
* Add Routing vis React Router
  + user react router to navigate between pages
  + in index.js
    - import {BrowserRouter as Router} from ‘react-router-dom’;
  + then wrap app with router component
  + declare a single route that will render the app component
    - ReactDOM.render(
    - <Router>
    - <Route component={App} />
    - </Router>,
    - document.getElementById(“root”)
    - );
  + in App.js, declare routes
    - import {Route} from “react-router-dom”;
    - import Home from “./Home”;
    - import Profile from “./Profile”;
    - …
    - render() {
    - return(
    - <>
    - <Route path=”/” exact component={Home} />
    - <Route path=”/profile” component={Profile} />;
    - </>
    - );
    - }
    - …
* Add Navigation Bar
  + Add new file to src folder ‘Nav.js’
    - Use rcc
    - Import { Link } from ‘react-router-dom’;
    - …
    - Change <div> to ul
    - <nav>
    - <ul>
    - <li>
    - <Link to=”/”>Home</Link>
    - </li>
    - <li>
    - <Link to=”/profile”>Profile</Link>
    - </li>
    - <ul>
    - </nav>
    - …
  + In App.js
    - Import nav component
    - import Nav from “./Nav”;
    - ..
    - <>
    - <Nav />
    - <Route ….
    - …
* Style App
  + Copy this into index.css
    - nav li a {
    - display: block;
    - color: white;
    - text-align: center;
    - padding: 14px 16px;
    - text-decoration: none;
    - }
    - nav li a:hover {
    - background-color: #d9390d;
    - }
    - nav button {
    - margin-top: 13px;
    - }
* Summary
* Intro
* Auth0 Version Used in the C..
* Sign up for Auth0
  + Tenant: logical isolation unit
    - No tenant can access data in another tenant
    - Think of tenant like a development environment
* Key Auth Decisions
  + Pick a flow
    - Implicit flow for client side web apps
  + Implicit flow
    - App directs browser to auth0 sign in
    - Auth0 redirects to your app at the callback URL you chose
    - Your app reads the tokens from the URL
    - App can use token to call resource server, for example API
  + Pick Login/Sign up
    - Universal
    - Embedded lock
    - Custom UI
  + Universal and embedded use lock widget
    - Easily integrates with Auth0
    - Adapts to your config
    - Looks great on any device
    - Remembers the last used connection
    - Automatic internationalization
    - Detailed password policy check
    - Customizable
  + Universal is hosted by Auth0
    - Avoids cross domain issues
  + Embedded Lock
    - Embedded in app
    - Places login form in app
    - Less secure because it requires cross domain calls
  + Custom UI
    - Build your own interface
    - Use Auth0 APIs
* Create an App in Auth0 D..
  + Click on new application
  + Click Single Page Web Applications
    - Configures auth0 to use the implicit grant
  + Click on app in application to go into settings
    - Specify the callback url
    - <http://localhost:3000/callback>
    - Need specify same callback url in application