Angular 2 Security: Authentication

Sang Shin
JPassion.com
"Code with Passion!"

Topics

- JWT (JSON Web Token) based authentication
- Guarding Routes
- Conditional display of UI components

JWT (JSON Web Token) Based Authentication

What is JWT authentication service?

- Is used to login and logout of the application
- Login process
  - In order to perform login, the client posts user credentials (such as username/password) to the authentication server
  - If the authentication was successful, JWT token is returned to the client
  - The client then saves the token in the local storage
- After login
  - Subsequent requests to the resource server sends the token in the “authorization” HTTP request header in order to access secured resource

Where to store JWT token?

- The JWT-token can be stored in local storage
  - So the user will stay logged in if he refreshes the browser and also between browser sessions until they logout
- If you don't want the user to stay logged in between refreshes or sessions the behaviour could easily be changed by storing user details somewhere less persistent such as session storage or in a property of the authentication service

Guard Routes

Routes Can be Guarded

- Routes can be guarded against unauthenticated and unauthorized access

```
const routes: Routes = [
    { path: 'login', component: LoginComponent },
    { path: '', component: HomeComponent, canActivate: [AuthGuard] },

    // otherwise redirect to home
    { path: '**', redirectTo: '' }
];
```

Conditional Display of UI Components

Conditional Display UI Components

- Login UI component needs to be displayed only a user is in “not logged” state
- Logout UI component needs to be displayed only a user is in logged state

Code with Passion!
JPassion.com