

6 Months Training TR-104 Full Stack Development

January, 2026

Day 11 Report

The eleventh day of training focused on strengthening application security and authentication flow by enforcing protected route access, managing authenticated user state, and improving post-login user experience. The session emphasized the use of services and route guards to control navigation, ensure correct session handling, and maintain stable application behavior.

Dashboard User Personalization

The dashboard was enhanced to display authenticated user details after successful login. User information such as name and email was retrieved through shared authentication services and rendered on the dashboard interface.

Key outcomes:

- Displayed logged-in user's name and email
- Verified correct data binding after both email/password and Google authentication
- Ensured dashboard content is shown only to authenticated users

This confirmed correct usage of authentication services for user data access.

Route Protection Using Auth Guard

Route protection was implemented to restrict access to protected pages using an authentication guard.

Key aspects:

- Prevented unauthenticated users from accessing the dashboard route
- Allowed navigation only when a valid authentication session exists
- Automatically redirected users to the authentication flow when access conditions were not met
- Re-evaluated authentication state on page refresh and navigation

This ensured that application routes remain secure and accessible only to authorized users.

Authentication Services Integration

Authentication-related logic was centralized using dedicated services to maintain a single source of truth for user state.

Key responsibilities handled by services:

- Tracking authenticated user information
- Exposing user state to components and guards
- Supporting route protection and dashboard personalization
- Ensuring consistent authentication behavior across the application

This approach improved maintainability and reduced duplication of authentication logic.

Sign-Out Functionality

A complete sign-out mechanism was implemented to allow users to securely end their session.

Key aspects:

- Cleared the active authentication state
- Redirected users away from protected routes after logout

- Ensured dashboard access was blocked immediately after signing out

This completed the authentication lifecycle from login to logout.

Authentication State and Session Behavior

The session included a detailed review of how authentication state is preserved while a user remains logged in.

Key observations:

- Authentication state persists across page reloads
- User sessions remain active until explicitly signed out
- Route guards and services rely on this state to control navigation
- Authentication state directly influences UI rendering and access control

This provided a strong conceptual understanding of session-based authentication behavior.

Verification and Testing

The following scenarios were tested to validate authentication flow:

- Successful login using email/password
- Successful login using Google authentication
- Dashboard access only after authentication
- Blocked access to dashboard without login
- Immediate route restriction after sign-out
- Session persistence verified through browser tools

All scenarios behaved as expected.

Key Learnings

- Implementing route protection using authentication guards
- Using services to manage authenticated user state
- Enforcing access control for protected routes
- Displaying authenticated user data on the dashboard
- Managing secure sign-out behavior
- Understanding session persistence and navigation control

Conclusion

Day 11 focused on strengthening authentication security and application stability by enforcing route protection through guards, centralizing authentication logic using services, and enhancing the dashboard with user-specific information. By controlling access before and after authentication and understanding session behavior, the application achieved a secure and reliable authentication flow, setting a strong foundation for account recovery and advanced user management features in the next phase.