# 6 Months Training TR-104 Full Stack Development

## January, 2026

## Day 12 Report

The twelfth day of training focused on completing the authentication workflow by implementing account recovery functionality and gaining a deeper understanding of how authenticated user state is managed and retained during an active session. The session emphasized both practical implementation and conceptual clarity around authentication persistence and security behavior.

## Forgot Password Functionality

A password recovery feature was implemented to allow users to reset their account password when access credentials are forgotten.

Key aspects included:

- Creating a dedicated “Forgot Password” component
- Designing a reactive form to capture user email
- Triggering a password reset email through the authentication system
- Displaying success and error feedback to the user
- Managing submission state to prevent duplicate requests

This completed the full authentication lifecycle from account creation to recovery.

## Password Reset Verification

The password reset flow was tested end-to-end to verify correct behavior.

Key observations:

- Reset request was successfully processed
- Password reset email was delivered to the registered email address
- User feedback was displayed correctly after submission
- No authentication state was exposed during the reset process

This ensured the account recovery mechanism functioned as expected.

## Retrieving Authenticated User Information

The session included understanding different approaches to accessing authenticated user data within the application.

Key points:

- Authenticated user information was accessed for display purposes
- User data was retrieved reliably for protected pages
- Correct timing of data access was ensured to avoid incomplete rendering

This reinforced correct handling of authenticated user information after login.

## Authentication Session Persistence

A major focus of the day was understanding how authentication state is retained across application reloads and navigation.

Key concepts covered:

- Authentication state persists across page refreshes
- User remains logged in until explicitly signed out
- Session data is stored and restored automatically by the authentication system

- Route guards and resolvers rely on this restored state to control access

This provided a clear understanding of why authenticated users remain logged in and how session continuity is maintained.

## Token Retention and Session Behavior

The final topic of the day involved understanding how authentication tokens are managed during an active session.

Key learnings:

- Authentication tokens are generated upon successful login
- Tokens are securely stored by the browser
- Tokens are refreshed automatically when required
- Tokens are cleared when the user signs out

This explained how secure access is maintained without manual token handling in the application.

## Verification and Testing

The following scenarios were verified:

- Successful password reset request
- Correct email delivery for password reset
- Persistent authentication state across reloads
- Correct retrieval of authenticated user information
- Proper session termination on sign-out

All scenarios worked as expected.

## Key Learnings

- Implemented account recovery using password reset
- Understood how authenticated user information is accessed
- Learned how authentication sessions persist across reloads
- Gained clarity on token storage and refresh behavior
- Strengthened understanding of authentication security concepts
- Completed the full authentication lifecycle

## Conclusion

Day 12 successfully concluded the authentication chapter by implementing password recovery and developing a strong conceptual understanding of authentication session persistence and token retention. By combining hands-on implementation with internal session behavior analysis, the application achieved a complete, secure, and reliable authentication system. This marks a solid transition point toward database integration and real application data management in the next phase.