Varighed: 1 dag
Deltagerpris: 6.800,00 dkr
Kursusnummer: LB1887

Introduction to OpenID Connect and OAuth

Kort om undervisningen

OpenID Connect is the de facto standard we should use for handling authentication and authorization in modern applications. However, it can still be very complex and confusing with all the various concepts, including scopes, claims, flows, resources, and tokens.

This course includes many hands-on exercises that will help you understand how the protocol works under the hood.

Indhold

- Introduction
  - Authentication vs. Authorization
  - Our challenges
  - OAuth versions
  - OAuth vs. OpenID Connect
- Token Service
  - Authorization Server
  - Relying party
  - Token types
  - Bearer tokens
  - Server implementations
  - Identity architecture
  - Service endpoints
  - The discovery document
- Implicit flow
  - How does this flow work
  - Why it is no longer a recommended flow
- JWT tokens
  - ID token
  - Access tokens
  - JSON Web Tokens
  - JWT access tokens
- Claims and scopes
  - What are claims?
  - Claim types
  - Scopes
  - User consent
- Securing the token

    - Unsecure tokens
    - Signed tokens
    - Signature algorithms
    - Private/public keys
    - Encrypted tokens
    - Validating the tokens
    - State and nonce
- Authorization Code Flow
    - Public vs. private clients
    - Front vs. back-channel
    - Authenticating the user
    - The authorization code
    - Getting the tokens
- Refresh tokens
    - One-time refresh tokens
    - Using the refresh token
    - Token introspection
- Client Credentials flow
    - Machine-to-machine communication
    - Getting the access token
    - Using the access token
- Backend For Frontend (BFF)
    - Introduction to the pattern
    - Why we should not handle tokens in the browser
- OAuth 2.1

Forudsætninger

It would be best if you had a good understanding of the following:

- The HTTP(s) protocol (including methods, headers, and cookies …)
- How the web and APIs work in general
- Some experience in developing backend web solutions

Målgruppe

This course is designed for both new and experienced developers and architects seeking to understand the fundamentals of application security using OAuth2 and OpenID Connect. With a focus on the core standards and protocols rather than a specific implementation or programming language, it's the perfect fit regardless of whether you use Duende IdentityServer, Entra ID (AzureAD), KeyCloak, or any other authorization service.

Efter kurset kan deltageren

In this course, you will learn the following:

- Authentication vs. authorization
- How OAuth 2.x and OpenID Connect work
- Fundamental concepts
- How a client authenticates against an authorization server
- How to retrieve and consume JWT tokens
- How OpenID Connect fits into your architecture
- How the tokens are secured and managed

Kommende afholdelsesdatoer

Ingen planlagte datoer, anvend kontaktinformationerne nedenfor.

Oplysning om yderligere afholdelser findes på vores hjemmeside. Andre spørgsmål besvares meget gerne ved brug af vores kontaktformular eller på telefon (+45) 33 861 861