

KOENIG SOLUTIONS · COURSE OUTLINE

Identity and Access Control for Modern Applications

Learn to secure ASP.NET applications and APIs using claims-based identity, OAuth 2.0, OpenID Connect, IdentityServer and SAML.

5 Days

DURATION

66

TOPICS

8

HANDS-ON ACTIVITIES

COURSE OVERVIEW

This course covers identity and access control in ASP.NET Core, including claims-based identity, cookie authentication, social logins, OpenID Connect, authorization and single sign-on patterns. It then moves to securing web APIs with token-based authentication, OAuth 2.0 flows, scopes, refresh tokens and support for mobile, native and single-page applications. It examines IdentityServer setup, configuration, customization, storage and deployment on Linux and Windows. Finally, it addresses OAuth and SAML security practices, hardening techniques such as PKCE and mutual TLS, SAML protocol bindings and assertions, and application integration for single sign-on.

WHO THIS COURSE IS FOR

ASP.NET Developers

API Developers

Identity Architects

Security Engineers

Application Integration Engineers

LEARNING OBJECTIVES

- Explain claims-based identity and cookie authentication in ASP.NET Core
- Configure social logins and OpenID Connect for web applications
- Implement single sign-on, claims transformation and federation gateways
- Apply OAuth 2.0 flows, scopes and token lifetime management for APIs
- Configure IdentityServer including services, storage and UI workflows
- Deploy IdentityServer on Linux and Windows environments
- Apply hardening techniques such as PKCE and mutual TLS to OAuth
- Design SAML single sign-on integrations using assertions and bindings

66 Topics

DAY 1 Foundation & Authentication

TOPICS

3 Labs

- Identity & Access Control in ASP.NET
- ASP.NET Core Security Framework
- Claims-based Identity
- Cookie-based Authentication
- Social Logins (e.g. Google, Facebook, Twitter, etc.)
- OpenID Connect
- Data Protection
- Authorization
- Web Application Patterns
- Single Sign-on/Single Sign-off
- Claims Transformation
- Federation Gateway
- Account & Identity Linking
- Home Realm Discovery

DAY 2 Web APIs & Access Control

TOPICS

3 Labs

- Securing APIs
- Architecture & Scenarios
- Token-based Authentication
- OAuth 2.0
- Clients
- Scopes
- Flows
- Token Lifetime Management
- Refresh Tokens
- OpenID Connect & OAuth 2.0 Combined
- Server-to-server Communication
- Native & Mobile Applications
- SPAs
- Custom Credentials & Token Requests

DAY 3 IdentityServer Architecture & Scenarios

TOPICS

- Setup (Linux and Windows)
- Configuration
- Dependency Injection
- Services
- Customizations
- Claims & Tokens
- User Interface
- Storage System
- UI Workflows
- Logging & Eventing
- Hosting & Deployment (Linux and Windows)

TOPICS

2 Labs

- Best practices
- Security Patterns
- Common Attacks and implementation Vulnerability fixing
- New release and security of today's OAuth architecture
- Hardening the front-channel with PKCE and signed authorization requests
- Hardening the back-channel with asymmetric key based client authentication and mutual TLS
- Hardening API calls with proof-of-possession access tokens
- Scope parameter replacement with authorization request
- Advanced high security profile for OAuth 2.0 and 2.1 with FAPI 2.0
- Access Management
- Single Sign on
- Federation
- SAML Protocol
- SAML Assertions
- SAML Protocol IDP init SSO, SP init SSO
- SAML Bindings Redirect/Post binding and Sign on flow
- Design, Implement application integrations for SSO with SAML protocol
- Oauth, OIDC protocol
- Oauth token formats
- Oauth flows
- Implicit, Auth Code, Client credentials (itna deep me discussion ni hua tha but for reference)
- Design, develop and implement application integrations for SSO with Oauth and OIDC protocol
- Authentication mechanisms - form, Multi Factor Authentication
- Policy driven Authorizations
- Add here Oauth Scope, Consent and access policies

Application Vulnerabilities (High Level)

TOPICS

- Fully OWASP Top 10 Web Application Security Risk

IIS and Nginx Hardening (High Level)

TOPICS

- Fixing Application Vulnerabilities listed above (Application Vulnerabilities)

NOTES

- Access Management platform to be planned, trainer suggests Okta.
- Programming language if no restriction then Java preferred.

HANDS-ON ACTIVITIES

Practise What You Learn

MODULE	ACTIVITY
Foundation & Authentication	LABS
	■ Authentication and Authorization
	■ External Authentication
	■ Federated Gateway
Web APIs & Access Control	LABS
	■ Web APIs
	■ Mobile and Native Client Applications
	■ JavaScript Client Applications
OAuth 2.0 and SAML	LAB
	■ SaaS application AM integrations (Salesforce with SAML)
	■ Custom application Security development, configuration and integration with AM (OAuth/OIDC JWT parsing)

WHAT IS INCLUDED

Everything You Need to Succeed

- Koenig course material for every module
- Delivery by certified instructors and subject matter experts
- Hands-on exercises throughout the course
- Course completion certificate from Koenig

ABOUT KOENIG

Who We Are

Established in 1993, Koenig Solutions is a globally recognised training provider with 35+ technology partnerships, 5,000+ training programmes and a network of certified instructors and subject matter experts, supporting individuals and enterprise teams worldwide.

FLEXIBLE DELIVERY

Learn the Way That Suits You

Classroom Training

Live Online Classes (ILO)

Fly-Me-A-Trainer (FMAT)

Flexi (Self-Paced)

1-on-1 Training

Ready to Get Started?

Talk to a learning advisor about schedules, group training and customised delivery.

Visit koenig-solutions.com

✉ info@koenig-solutions.com