Training content

DAY 1: Foundation & Authentication

- 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

Labs:

- Authentication and Authorization
- External Authentication
- Federated Gateway

DAY 2: Web APIs & Access Control

- 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

Labs:

- Web APIs
- Mobile and Native Client Applications
- JavaScript Client Applications

DAY 3: IdentityServer Architecture & scenarios

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

DAY 4 and 5

OAuth 2.0 and SAML

Best practices

Security Patterns

Common Attacks and

implementationVulnerability 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 mutualTLS

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

protocolOauth, 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

Lab: SaaS application AM integrations (Salesforce with SAML)

Lab: Custom application Security development, configuration and integration with AM (Oauth/OIDC JWTparsing)

Access Management platform -- To be planned (Okta is my suggestion)

Programming language if no restriction than Java Preferred

Add here Oauth Scope, Consent and access policies

Application Vulnerabilities (High level)

Fully OWASP Top 10 Web Application Security Risk

IIS and Nginx Hardening (High level)

Fixing Application Vulnerabilities listed above (Application Vulnerabilities)