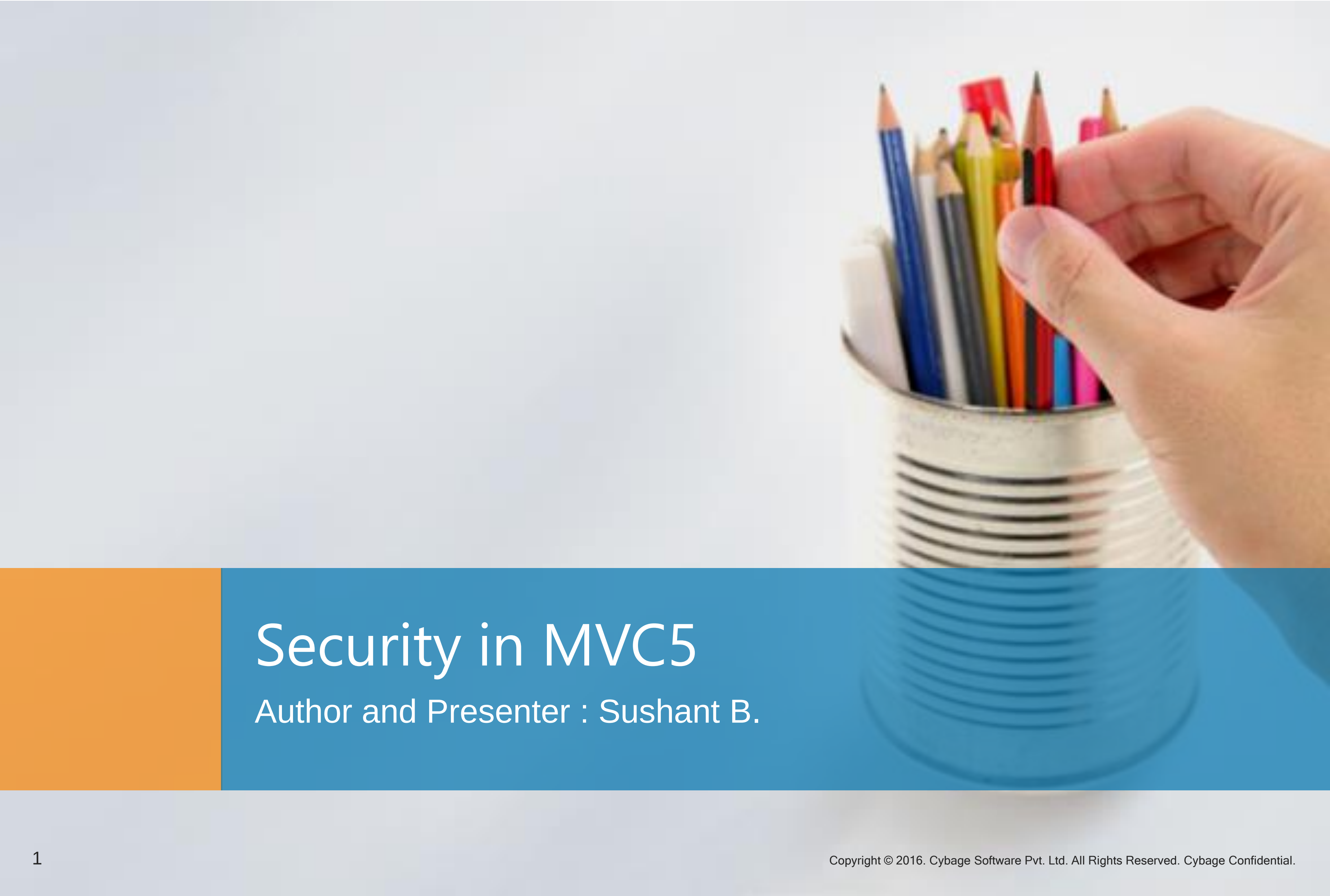
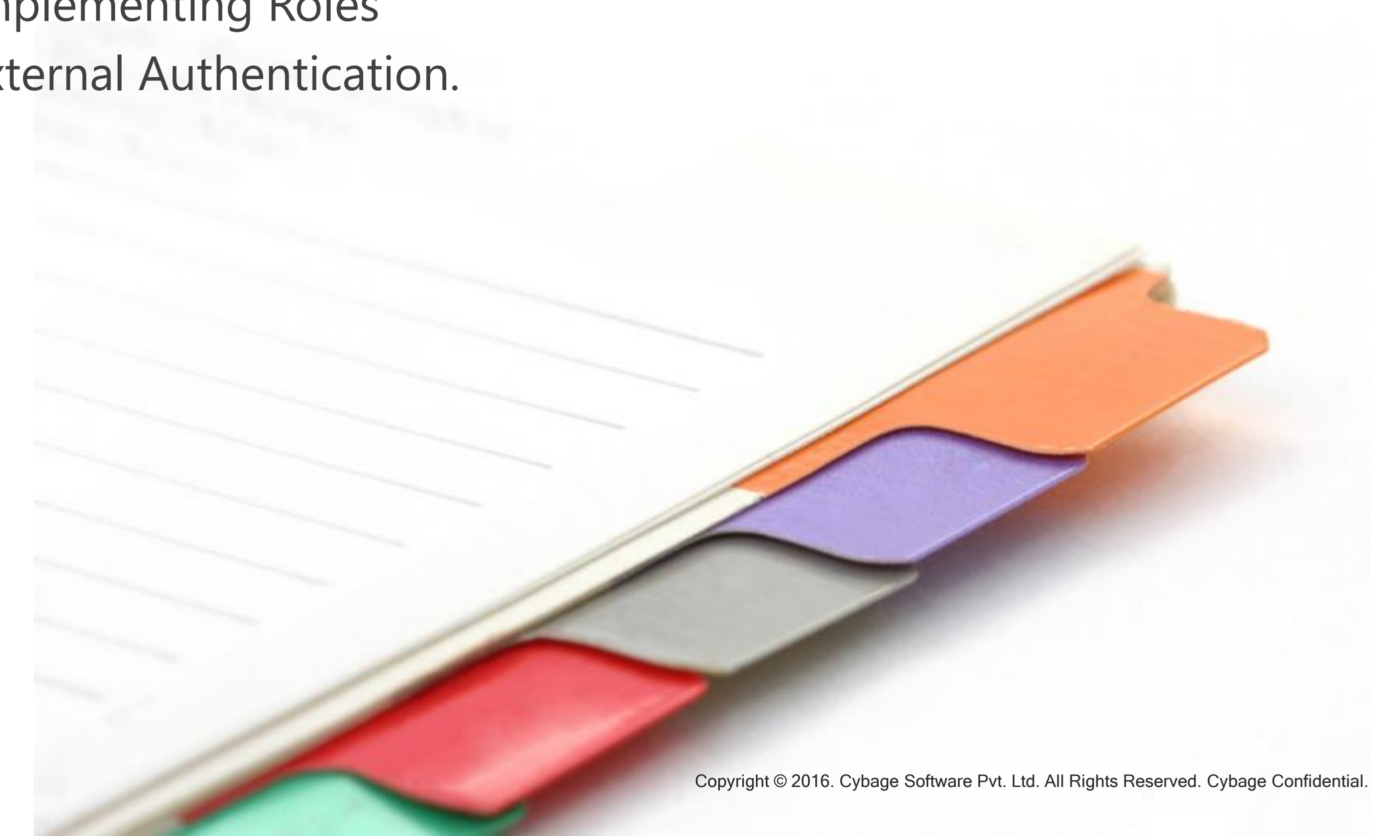


Security in MVC5

Author and Presenter : Sushant B.

Agenda

- Common Threats
- Identity and security
- Creating Users
- Implementing Roles
- External Authentication.



XSS/CSS Attack

- Stands for Cross-site Scripting
- It’s a script injection attack to your app
- It can steal session cookies or any sensitive information
- Using HTML Encoding disables scripts.

Overposting Attack

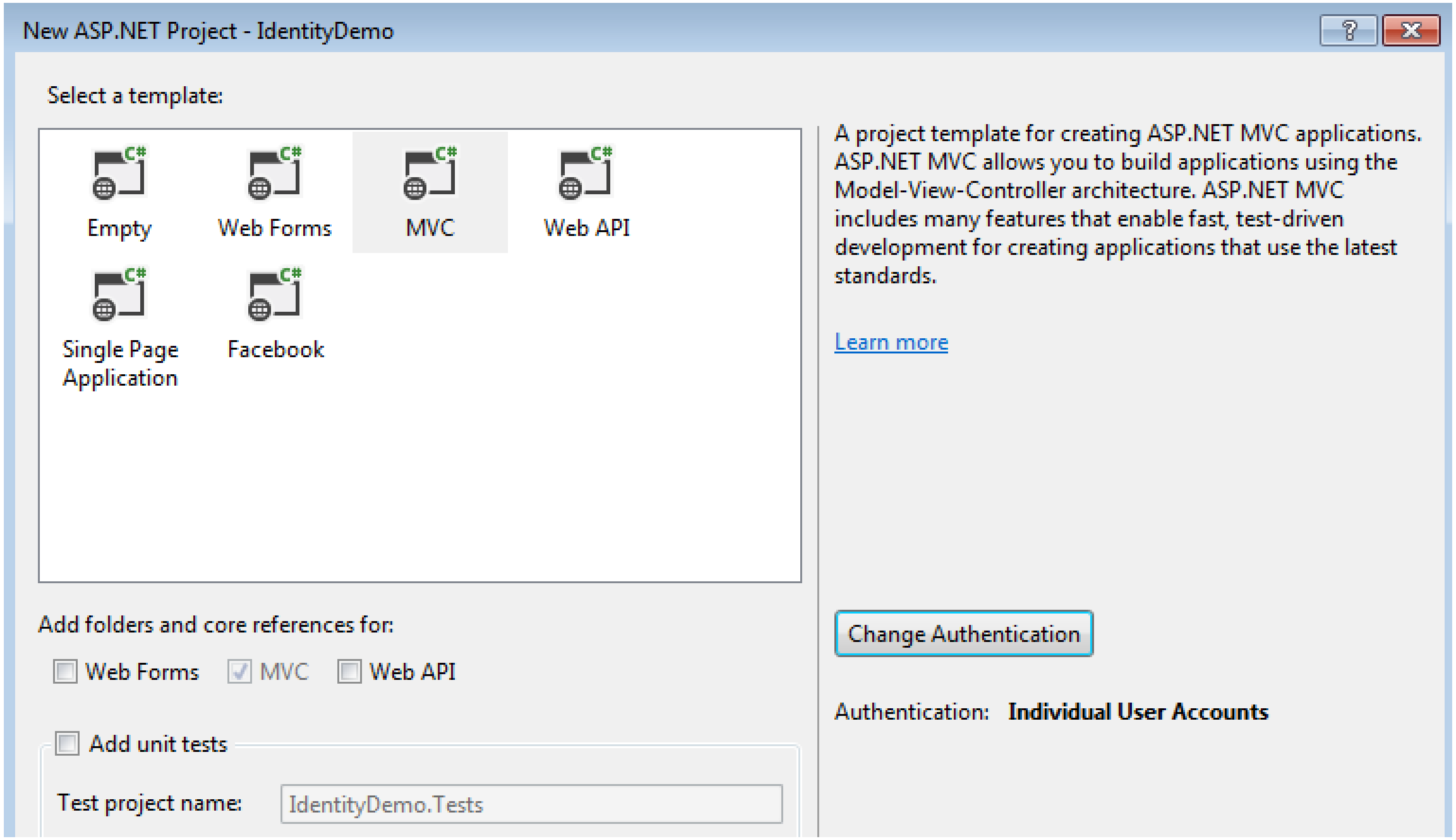
- Unwanted changes in Model property
- Tools such as Fiddler can be used
- Blacklist or Exclude
- Whitelist or Include
- Using ViewModel is better option.

CSRF Attack

- CSRF / XSRF – Cross-site Request Forgery
- ValidateAntiForgeryToken attribute in action
- @Html.AntiForgeryToken() method in Views.

Demo

Select Authentication



New ASP.NET Project - IdentityDemo

Select a template:

A project template for creating ASP.NET MVC applications. ASP.NET MVC allows you to build applications using the Model-View-Controller architecture. ASP.NET MVC includes many features that enable fast, test-driven development for creating applications that use the latest standards.

Learn more

Add folders and core references for:

□ Web Forms ☑ MVC □ Web API

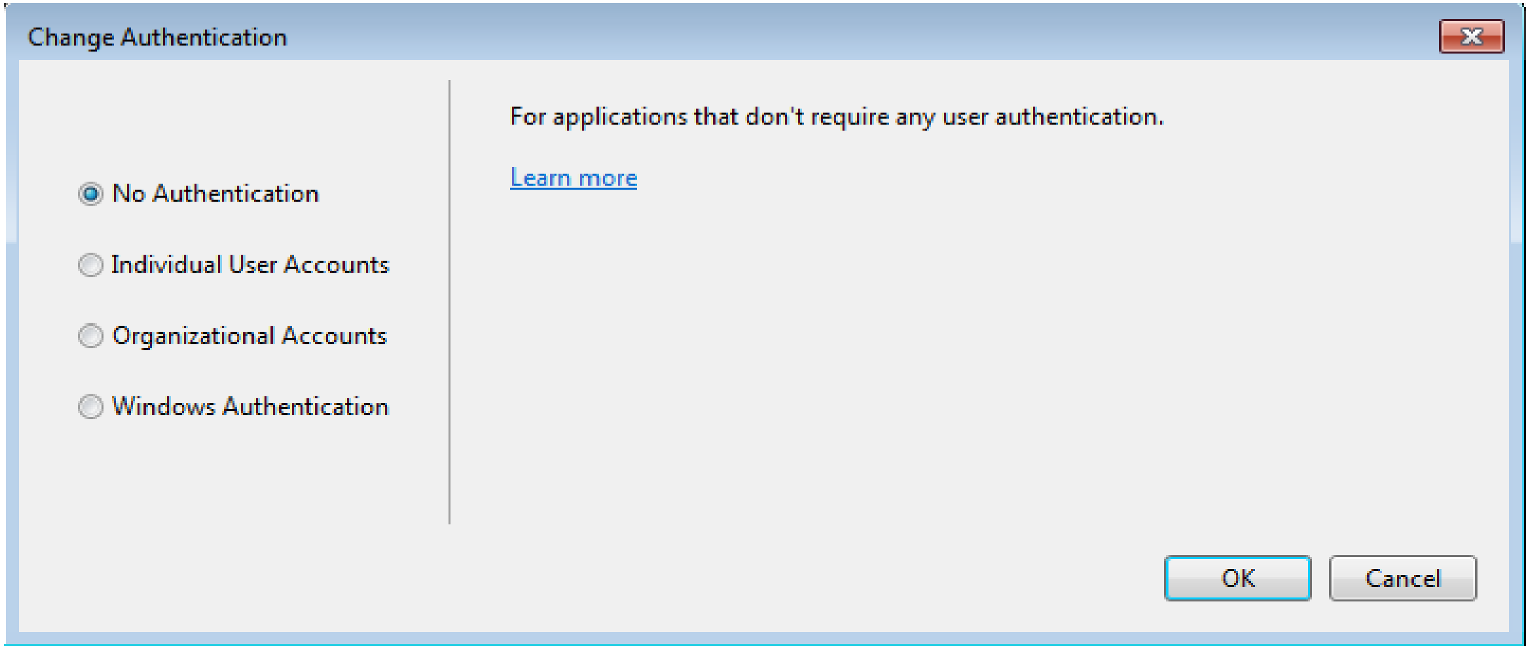
□ Add unit tests

Test project name: IdentityDemo.Tests

Authentication: **Individual User Accounts**

No Authentication

- Allows anonymous users
- Doesn't identify or authenticate users.



Change Authentication

● No Authentication

○ Individual User Accounts

○ Organizational Accounts

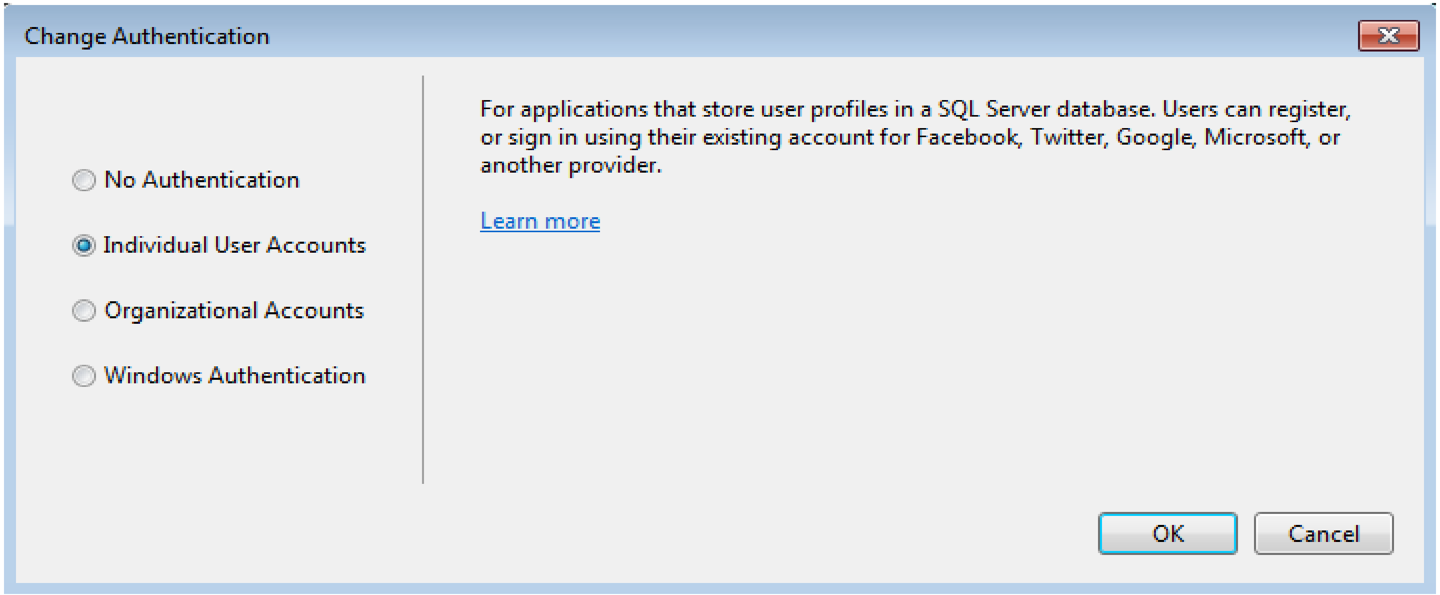
○ Windows Authentication

For applications that don't require any user authentication.

Learn more

Individual User Accounts

- Traditional form based authentication
- Uses SQL Server database
- Can implement third party authentication.



Change Authentication

○ No Authentication

● Individual User Accounts

○ Organizational Accounts

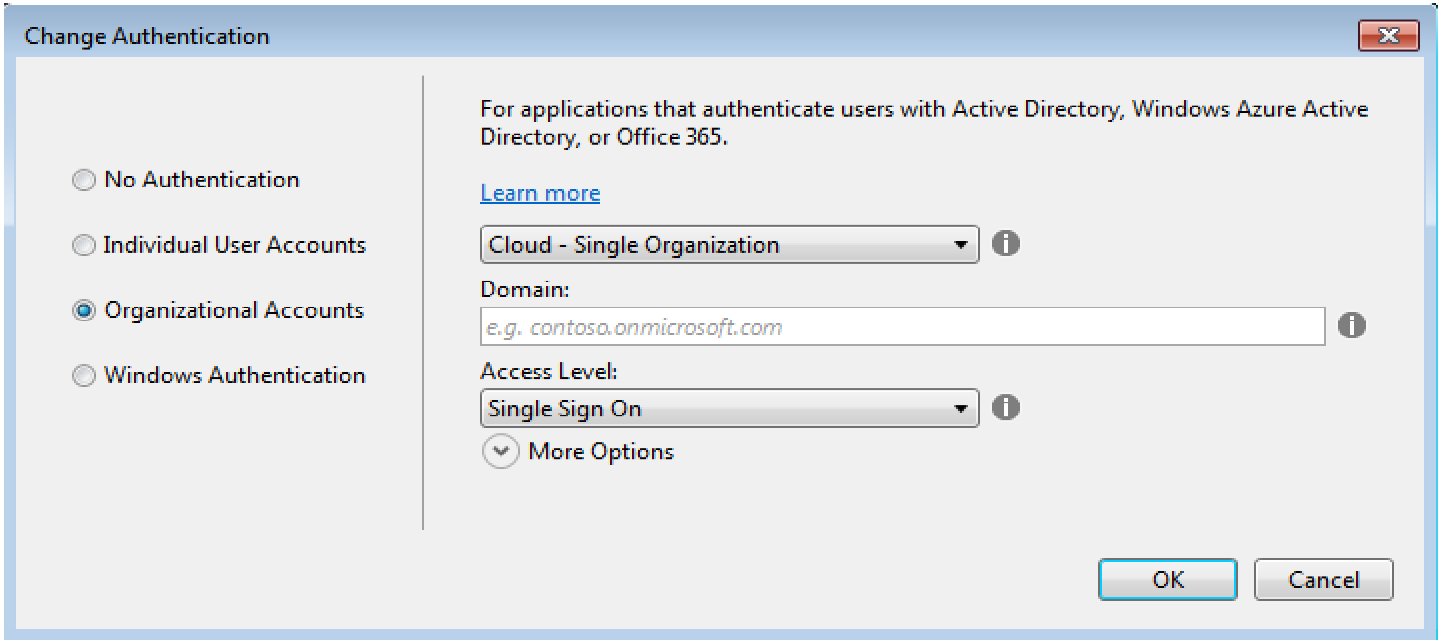
○ Windows Authentication

For applications that store user profiles in a SQL Server database. Users can register, or sign in using their existing account for Facebook, Twitter, Google, Microsoft, or another provider.

Learn more

Organizational Accounts

- Uses Active Directory Authentication with more options
- Single Sign On for Internal and Cloud App.



Change Authentication

○ No Authentication

○ Individual User Accounts

● Organizational Accounts

○ Windows Authentication

For applications that authenticate users with Active Directory, Windows Azure Active Directory, or Office 365.

Learn more

Cloud - Single Organization

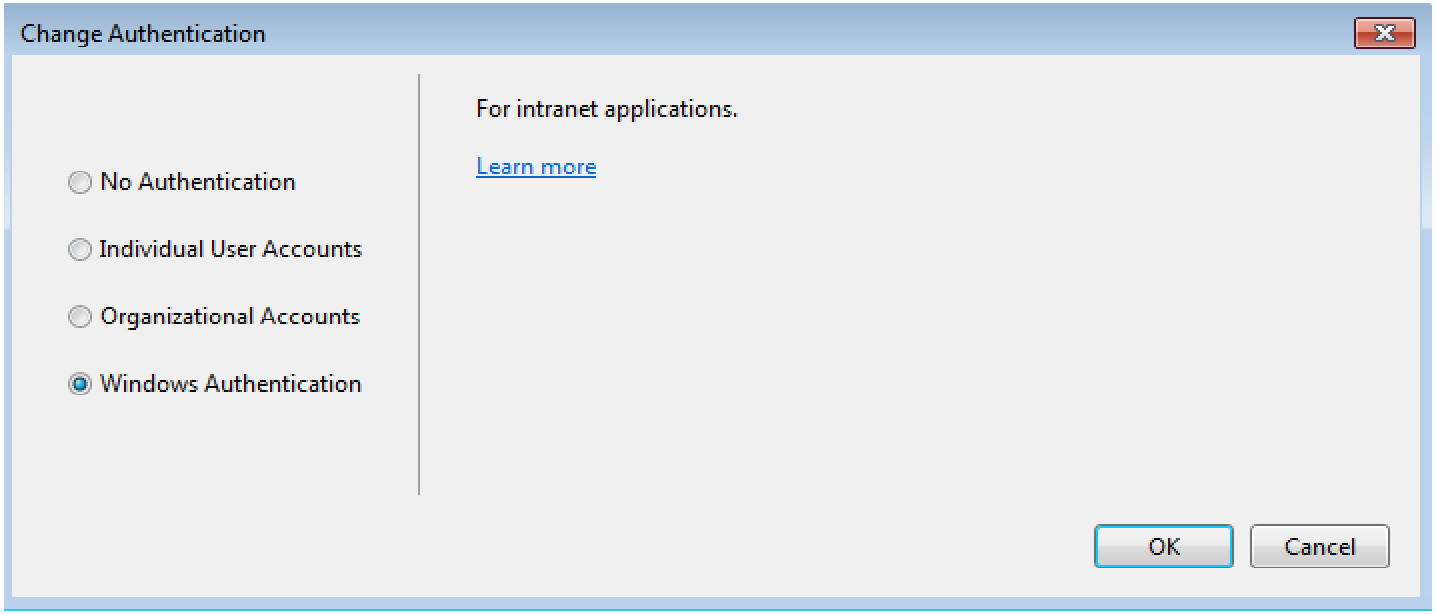
Domain: e.g. contoso.onmicrosoft.com

Access Level: Single Sign On

More Options

Windows Authentication

- Suitable for Intranet based applications
- Doesn't allow anonymous users
- Uses Active Directory.



Change Authentication

○ No Authentication

○ Individual User Accounts

○ Organizational Accounts

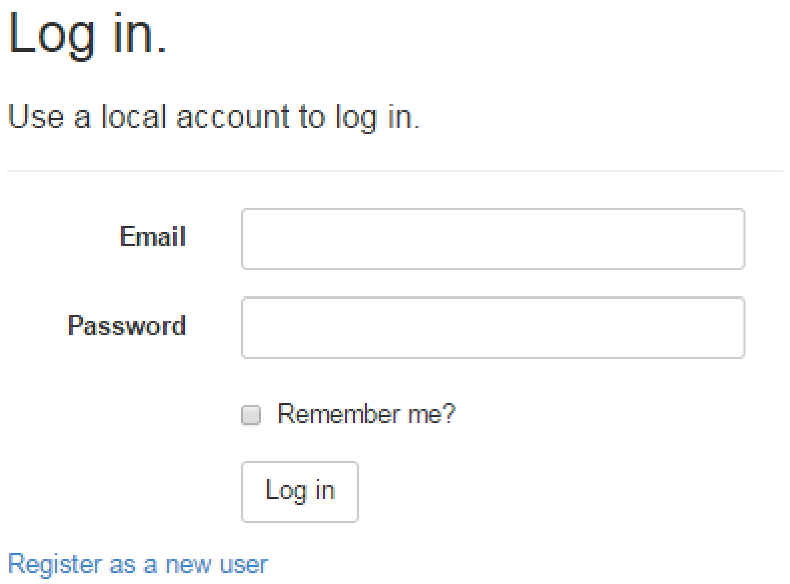
● Windows Authentication

For intranet applications.

Learn more

Form Based Authentication

- Register or Login using a project implements MVC template
- Create database using EF to store authentication information.



Log in.

Use a local account to log in.

Email	
Password	

□ Remember me?

Assemblies

- `using Microsoft.AspNet.Identity`
- `using Microsoft.AspNet.Identity.EntityFramework.`

Authorize Attribute

- Where to Apply
  - Apply on Controller level
  - Apply on Action level
- What it does
  - Authenticates Users
  - Implements Roles Based Authentication
- Allow Anonymous Users.

Authenticating Users

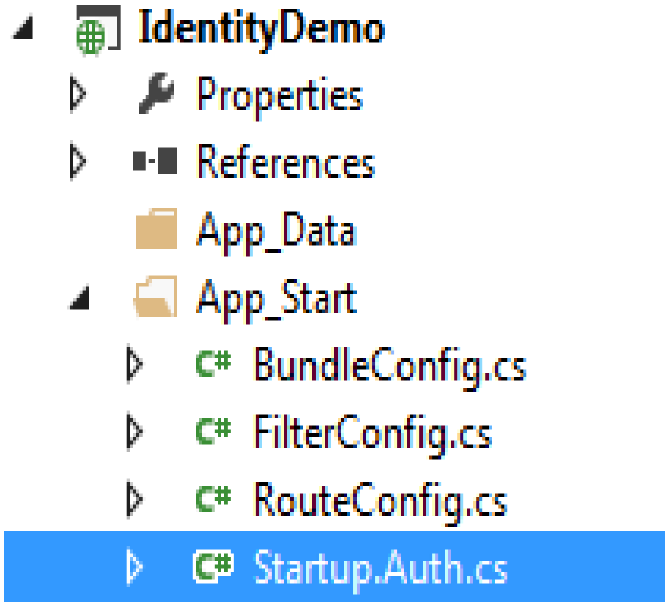
- UserStore class
- UserManager Class
- ApplicationUser Class.

Managing Roles

- RoleStore Class
- RoleManager Class
- IdentityRole Class.

External Authentication

- Microsoft
- Twitter
- Facebook
- Google.



Summary

- Common threats
- Authenticating users
- Identifying users and roles
- External Authentication.

Bibliography, Important Links

- http://www.asp.net/identity
- http://www.asp.net/identity/overview/getting-started/introduction-to-aspnet-identity
- http://www.asp.net/mvc/overview/security/xsrfcsrf-prevention-in-aspnet-mvc-and-web-pages
- http://www.asp.net/mvc/tutorials/older-versions/security/preventing-javascript-injection-attacks-cs

Any Questions?

Email : SushantBa@cybage.com
Extn. : 7221

Thank you!