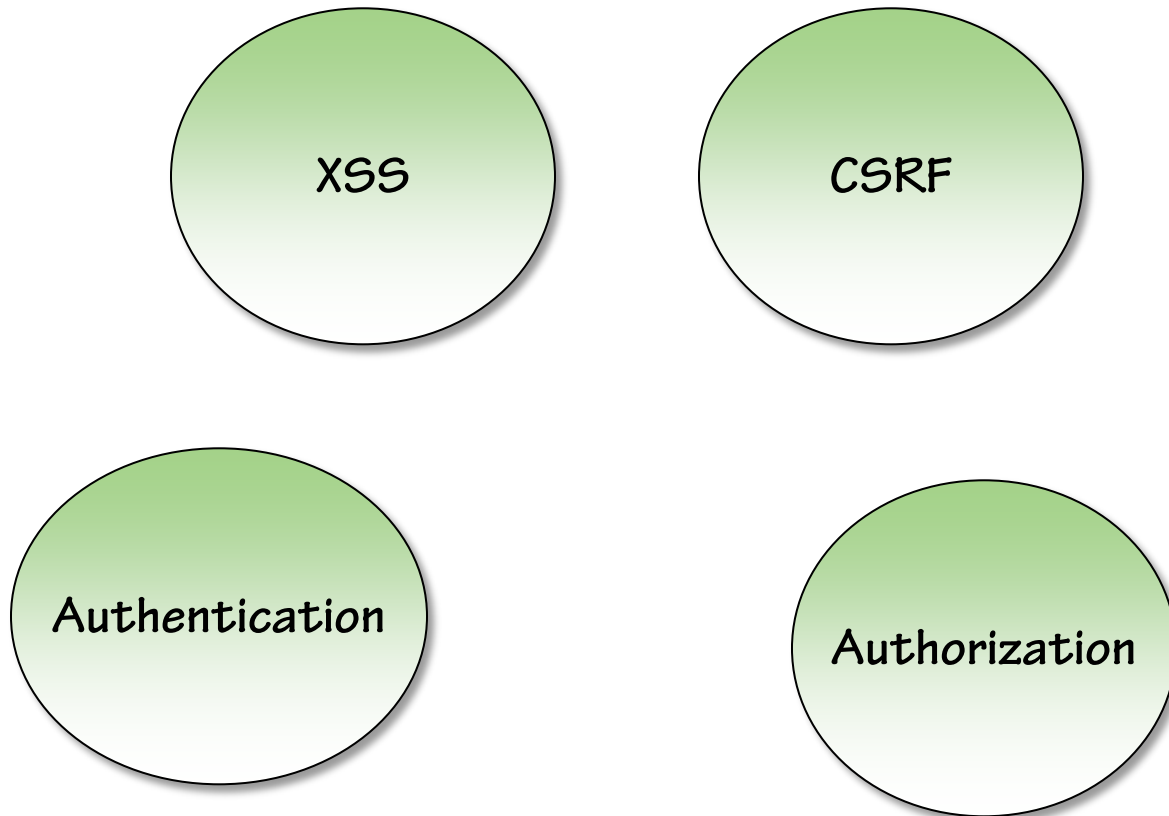


# Security & ASP.NET MVC

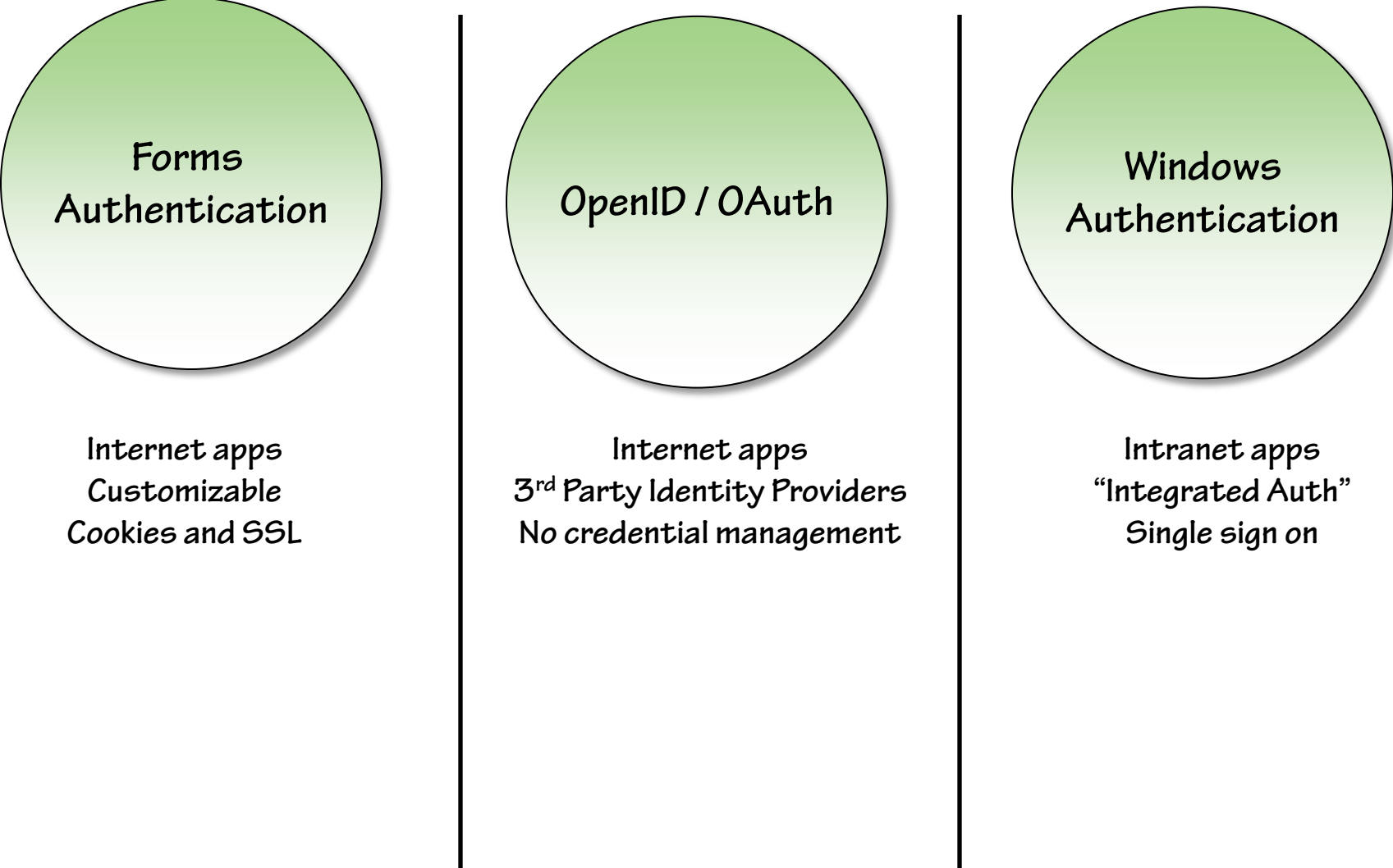
K. Scott Allen



# Overview



# Authentication



## Forms Authentication

Internet apps  
Customizable  
Cookies and SSL

## OpenID / OAuth

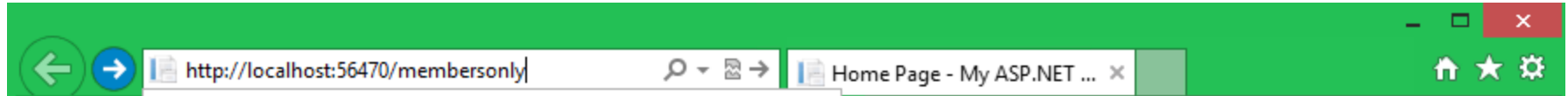
Internet apps  
3<sup>rd</sup> Party Identity Providers  
No credential management

## Windows Authentication

Intranet apps  
“Integrated Auth”  
Single sign on

# Forms Authentication

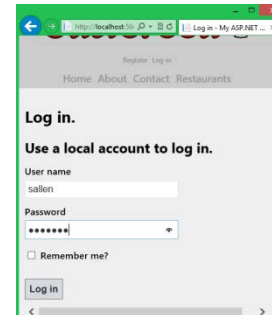
1. User tries to access “members only” page.



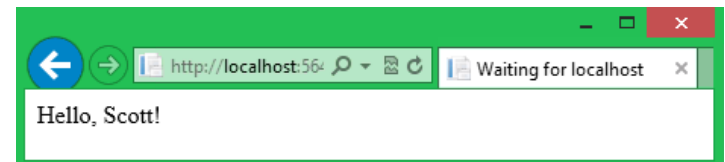
2. ASP.NET redirects user to login page (“~/Account/Login”)



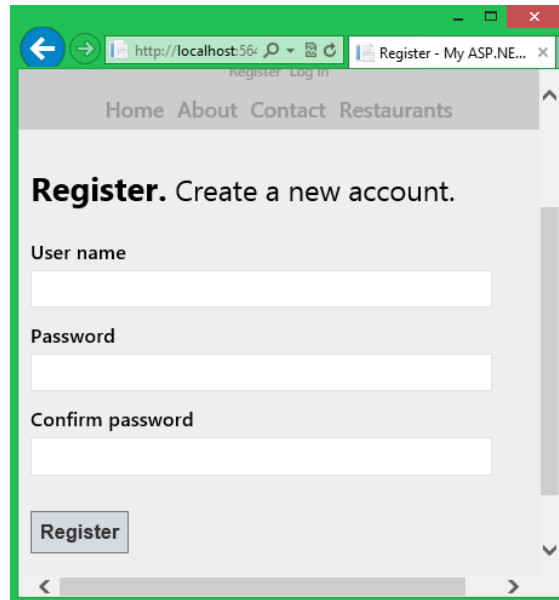
3. User submits username and password



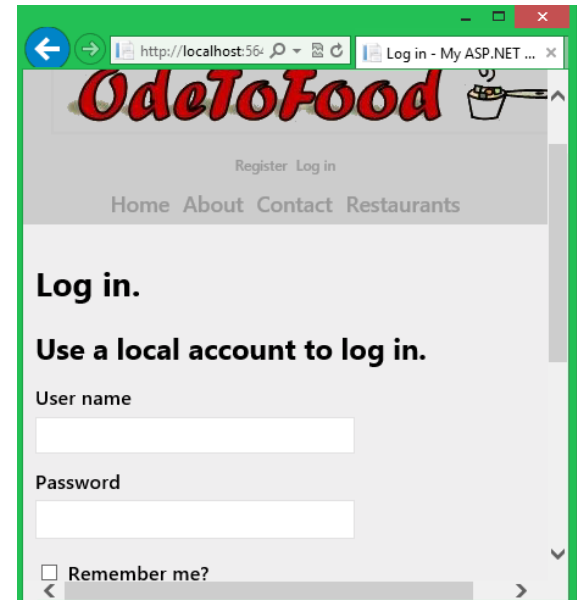
4. ASP.NET sets authentication cookie, redirects back to “members only” page.



# Forms Authentication



A screenshot of a web browser window showing the 'Register' page of a website named 'OdeToFood'. The browser's address bar shows 'http://localhost:56...'. The page has a navigation bar with links: 'Home', 'About', 'Contact', and 'Restaurants'. Below the navigation bar, the heading 'Register. Create a new account.' is displayed. The form contains three input fields: 'User name', 'Password', and 'Confirm password'. A 'Register' button is located at the bottom of the form.



A screenshot of a web browser window showing the 'Log in' page of the 'OdeToFood' website. The browser's address bar shows 'http://localhost:56...'. The page features the 'OdeToFood' logo at the top, followed by 'Register' and 'Log in' links. A navigation bar contains links: 'Home', 'About', 'Contact', and 'Restaurants'. The main heading is 'Log in.' followed by the instruction 'Use a local account to log in.'. The form includes 'User name' and 'Password' input fields, and a 'Remember me?' checkbox at the bottom.

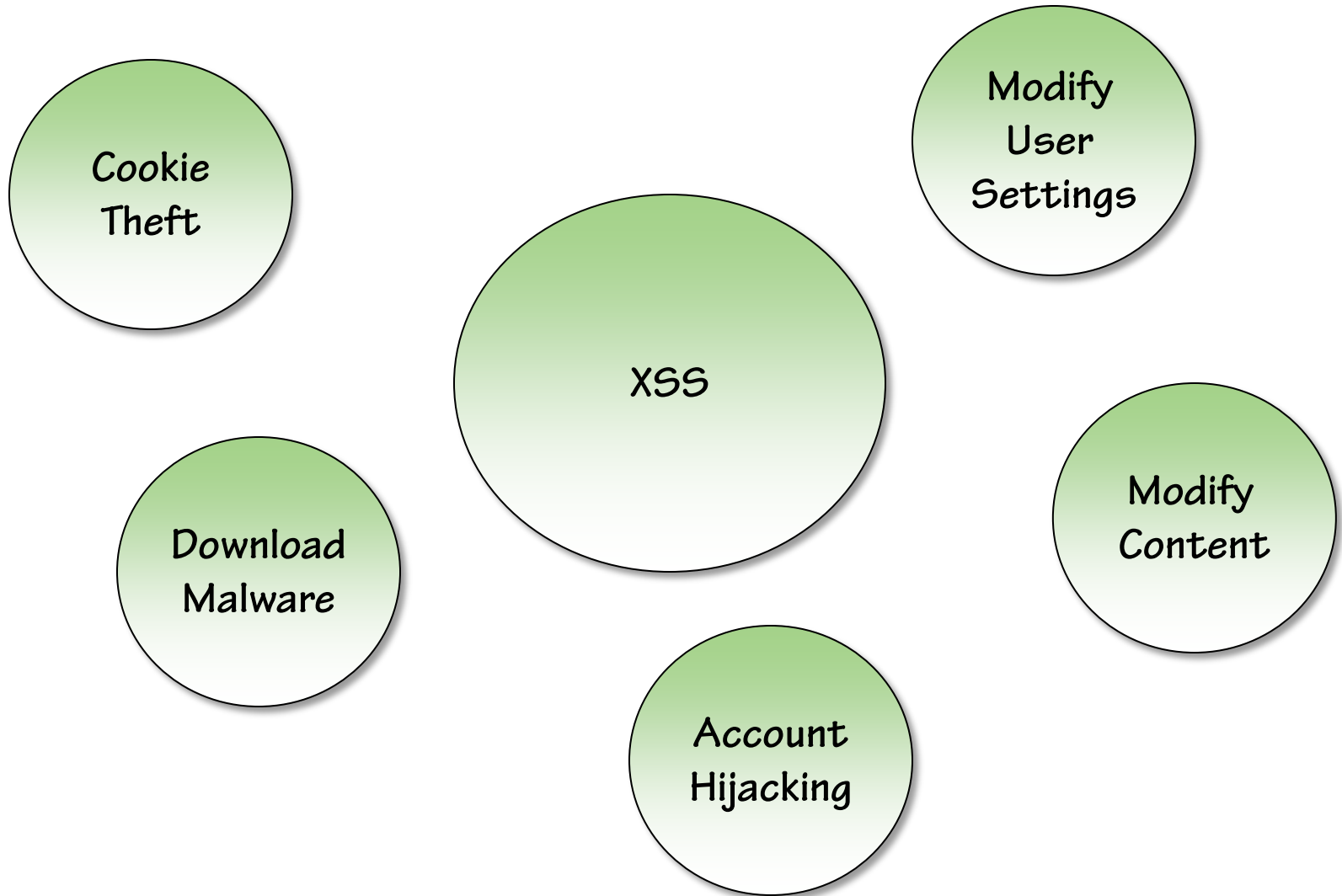
AccountController / Views

WebMatrix WebSecurity

SimpleMembershipProvider

SQL Storage

# Threat: Cross-Site Scripting

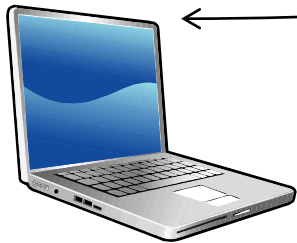


# Cross Site Request Forgery

EVIL.com



YOU.com



<form action="http://you.com/AuthCookie.aspx">

...

Submit data on behalf of evil.com

Login

# Summary

