

Capítulo 13

Configurando la seguridad de aplicaciones Web ASP.NET

Objetivo

Al finalizar el capítulo, el alumno:

- Implementar tópicos de seguridad en las aplicaciones Web.

Temas

1. Autenticación y autorización
2. ASP.NET Identity 2.1

1. Autenticación y autorización

Autenticación y autorización

- **Autenticación**

Es el proceso por el que se comprueba la identidad de alguien o algo, para comprobar si es lo que dice ser. Ese "alguien" o "algo" se le denomina principal. La autenticación requiere pruebas de identidad, denominadas credenciales. Por ejemplo, una aplicación cliente puede requerir un login y contraseña como credenciales. Si la aplicación cliente presenta las credenciales correctas, se asume que es quien dice ser.

- **Autorización**

Es el proceso de determinar los accesos/permisos de ese alguien o algo ya autenticado. Por ejemplo, cuando ya autenticamos a un usuario del sistema, se procede a autorizarle el acceso a ciertas opciones o menús de aplicación.

13 - 4

Copyright © Todos los Derechos Reservados - Cibertec Perú S.A.C.



Es importante determinar y conocer las diferencias entre los conceptos de autenticación y autorización:

Autenticación

Es el proceso por el que se comprueba la identidad de alguien o algo, para comprobar si es lo que dice ser. Ese "alguien" o "algo" se le denomina principal. La autenticación requiere pruebas de identidad, denominadas credenciales. Por ejemplo, una aplicación cliente puede requerir un login y contraseña como credenciales. Si la aplicación cliente presenta las credenciales correctas, se asume que es quien dice ser.

ASP.NET considera 2 tipos de autenticaciones, Windows y Forms:

- Autenticación de Windows (Windows Authentication) se refiere a autenticar contra las cuentas de usuario de Windows.
- La autenticación de formularios (Forms Authentication) es un método independiente de autenticación .NET, en el cual se pueden validar las credenciales que el usuario ingresa contra una base de datos u otro lugar en el que se tenga el listado de usuarios con acceso al sistema.

Configuración de autenticación de tipo Forms (en el archivo .config)

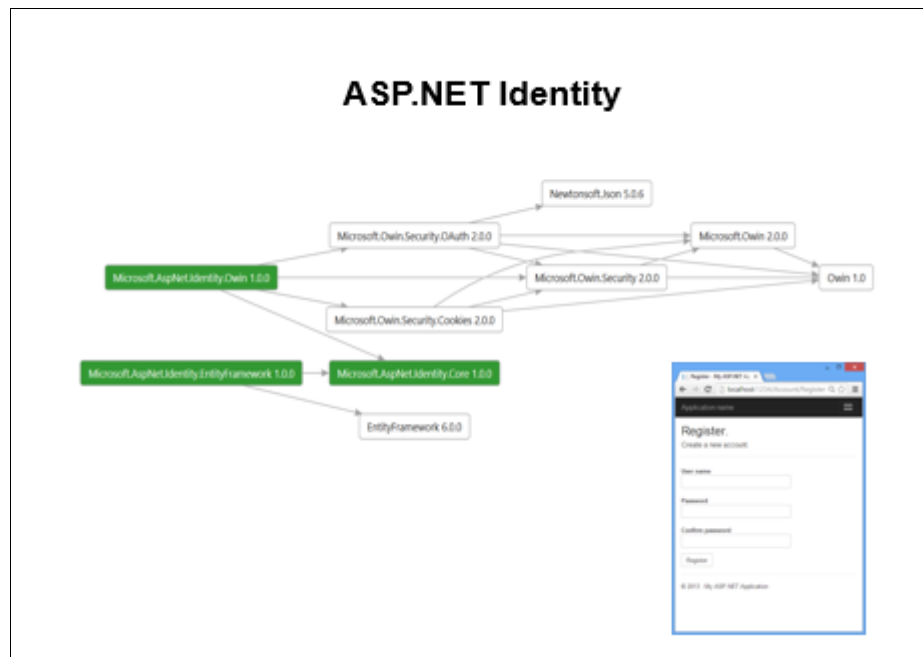
```
<authentication mode="Forms">  
  <forms loginUrl="login.aspx" name=".ASPXFORMSAUTH"></forms>  
</authentication>
```

Autorización

Es el proceso de determinar los accesos/permisos de ese alguien o algo ya autenticado. Por ejemplo, cuando ya autenticamos a un usuario del sistema, se procede a autorizarle el acceso a ciertas opciones o menús de aplicación.

```
<authorization>  
  <deny users="?">  
</authorization>
```

2. ASP.NET Identity



Para manejar de manera más rápida y fácil el aspecto de Autenticación y Autorización en aplicaciones Web, ASP.NET incluía **ASP.NET Membership** (hasta ASP.NET 3.5), esto incluía un panel de administración de permisos en el cual registrábamos usuarios, roles, esto se registraba en un esquema de datos ya definido. Posteriormente, se desarrolló **ASP.NET Simple Membership** (ASP.NET 4) y ahora se tiene **ASP.NET Identity** (ASP.NET 4.5 y 5).

ASP.NET Identity también incluye un esquema de base de datos predefinido que podemos utilizar inmediatamente con la configuración predeterminada de nuestros proyectos. Podemos cambiar la ubicación por defecto en la que nuestra base de datos será generada (Entity Framework Code First) cambiando la cadena de conexión que viene por defecto en el archivo Web.config.

ASP.NET Identity permite realizar la autenticación no solo utilizando el mecanismo de usuario/password sino por medio de proveedores globales de identidad como es Facebook, Twitter, entre otros.

ASP.NET Identity fue desarrollado para brindar soporte a WebForms, ASP.NET MVC, Web API y SignalR.