



LABORATORIO 6:

Seguridad en ASP.NET

Cuestionario obligatorio

GRUPO: HAS_17



TAREA 1: Añadir seguridad basada en formularios a la aplicación web desarrollada en los laboratorios. El objetivo es impedir a los usuarios, no identificados mediante login (anónimos), el acceso a la aplicación de gestión de tareas. Además, se debe impedir el acceso a las páginas para los profesores a aquellos usuarios autenticados como alumnos. El caso de uso exportar tareas sólo lo podrá ejecutar el profesor de email: vadillo@ehu.es

1. Incluir el código del fichero/de los ficheros web.config utilizado/s. (solo la parte modificada)

Se ha utilizado el web.config general y se ha administrado por directorios.

```
<!--Esta es la parte de la web comun a todos-->
<location path="~/General">
  <system.web>
    <authorization>
      <!--permitimos el paso de todo el mundo-->
      <allow users="*" />
    </authorization>
    <compilation debug="true" strict="false" explicit="true"
targetFramework="4.0"/>
    <httpRuntime/>
  </system.web>
</location>

<!--Esta es la parte de alumnos (resgingido a alumnos y profes)-->
<location path="~/Alumnos">
  <system.web>
    <authorization>
      <!--Estos (Alumno y profesor son las Cookies de sesion)-->
      <allow users="Alumno, Profesor, vadillo@ehu.es" />
      <deny users="*" />
    </authorization>
    <compilation debug="true" strict="false" explicit="true"
targetFramework="4.0"/>
    <httpRuntime/>
  </system.web>
</location>

<!--Esta es la parte de la web de Profesores (restringido a profes)-->
<location path="~/Profesores">
  <system.web>
    <authorization>
      <allow users="Profesor, vadillo@ehu.es" />
      <deny users="*" />
    </authorization>
    <compilation debug="true" strict="false" explicit="true"
targetFramework="4.0"/>
    <httpRuntime/>
  </system.web>
</location>
```



```
</system.web>
</location>

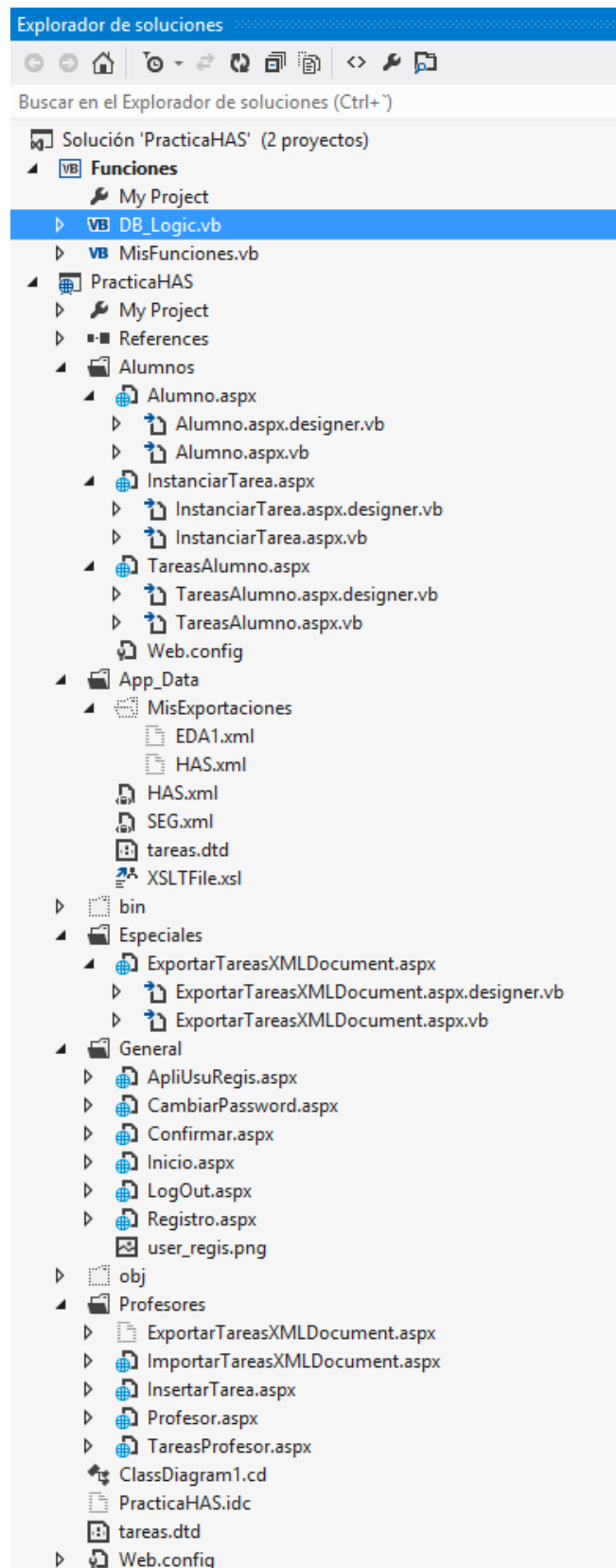
<!--Esta es la parte de características especiales, solo para Vadillo-->
<location path="~/Especiales">
  <system.web>
    <authorization>
      <allow users="vadillo@ehu.es"/>
      <deny users="*/>
    </authorization>
    <compilation debug="true" strict="false" explicit="true"
targetFramework="4.0"/>
    <httpRuntime/>
  </system.web>
</location>
</configuration>
```

En el caso de que quisiéramos tener un web.config por carpetas, sería así. Este es un ejemplo de web.config para administrar los permisos de la carpeta Alumnos:

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <system.web>
    <authorization>
      <allow users="Alumno, Profesor"/>
      <deny users="*/>
    </authorization>
  </system.web>
</configuration>
```

2. Incluir una pantalla con la ventana del Solution Explorer de vuestra aplicación Web. Ver ejemplo:

La solución de nuestra aplicación se puede ver en la siguiente página.





3. Escribir el fragmento de código que incluye la llamada al método `SetAuthCookie(...)`

```
If (databaseLogic.AutenticarLogIn(user, passCifrada) = True) Then
    Respuesta.Text = "Login Correcto."
    Session("Email") = BoxUsuario.Text
    If (databaseLogic.esAlumno(user)) Then
        Session("Rol") = "A"
        FormsAuthentication.SetAuthCookie("Alumno", False)

'System.Web.Security.FormsAuthentication.RedirectFromLoginPage("Alumno", False)
    Response.Redirect("~/Alumnos/Alumno.aspx")
    Else
        If (BoxUsuario.Text.Equals("vadillo@ehu.es")) Then
            Session("Rol") = "P"
            FormsAuthentication.SetAuthCookie("vadillo@ehu.es", False)

Response.Redirect("~/Especiales/ExportarTareasXMLDocument.aspx")
        Else
            Session("Rol") = "P"
            FormsAuthentication.SetAuthCookie("Profesor", False)
            Response.Redirect("~/Profesores/Profesor.aspx")
        End If
    End If
    Respuesta.Text = "Login Incorrecto."
End If
End If
```

Este método primero comprueba si el usuario es un alumno, en tal caso se le asigna la cookie de `user="Alumno"`. Si no es alumno, por descarte, es un profesor, así que comprobamos si es Vadillo para asignarle una cookie personalizada que le garantice algunos privilegios. En caso de ser otro profesor, se le añade la cookie de `"Profesor"`.

4. Describir de forma precisa cual ha sido el diseño de la solución para los requerimientos de seguridad dados y las pruebas realizadas.

Se ha organizado el código por carpetas y se han actualizado los vínculos. Se ha cambiado el `web.config` de la raíz y se han añadido las restricciones y permisos mediante `allow` y `deny`. Posteriormente se ha actualizado el código para diferenciar entre profesor y alumno mediante el uso de la cookie. Con anterioridad lo hacíamos mediante el uso de una `Session` a la que denominábamos `Rol`. Hemos añadido también cifrado mediante el resumen MD5.



TAREA 2: Modificar la aplicación de registro para trabajar con el password almacenado en la BD utilizando la transformación que realiza una de las funciones hash de la librería System.Security.Cryptography.

1. Describir las modificaciones realizadas ilustrando esta descripción con los fragmentos de código adecuados.

Hemos creado una función para Hashear que guardamos en la biblioteca "MisFunciones". El código es el siguiente:

```
Imports System.Security.Cryptography

Shared Function GetMd5Hash(ByVal md5Hash As MD5, ByVal input As String) As String
    ' Convierte la entrada en tipo Byte y realiza los cálculos para cifrar.
    Dim data As Byte() = md5Hash.ComputeHash(Encoding.UTF8.GetBytes(input))

    ' Crea una estructura
    Dim sBuilder As New StringBuilder()

    ' Cicla por cada byte del hash y le asigna un valor hexadecimal
    Dim i As Integer
    For i = 0 To data.Length - 1
        sBuilder.Append(data(i).ToString("x2"))
    Next i

    ' Devuelve el resumen MD5
    Return sBuilder.ToString()
End Function
End Class
```

Después, lo tenemos que usar en la página Inicio, para iniciar sesión:

```
Dim pass As String = BoxPass.Text
Dim md5Hash As MD5 = MD5.Create()
Dim passCifrada As String = Funciones.MisFunciones.GetMd5Hash(md5Hash, pass)
```

De la misma forma lo utilizamos en registro para registrar al usuario, de forma que la contraseña que se guarde sea la cifrada.

2. Añadir una pantalla con la tabla de la BD que incluya los passwords cifrados.

pedro@ikasle.e...	AA	aa	aa	23232323	True	6	A	pedro
pepe@ikasle.eh...	Pepe	Mi nombre	Pepe	12345678	True	1	A	926e27eedbc7...
vadillo@ehu.es	JA Vadillo	Mi apellido	Vadillo	87654321	True	NULL	P	c6458de5d97a5...
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

**TAREA 3 (*Opcional*) : Añadir a la BD el usuario: admin@ehu.es con password: admin**

Implementar un caso de uso, el que querías, relacionado con el dominio del proyecto que sólo pueda ser ejecutado por el usuario creado (administrador).

- 1. Describir al caso de uso. Añadir el código de su implementación. Añadir una pantalla con su ejecución (sólo si no se ha desplegado a Azure)**

Se ha añadido una carpeta llamada Admin a la que sólo puede entrar admin@ehu.es.

Tiene la opción de cambiar la contraseña de cualquier usuario, introduciendo mediante un desplegable.

E-mail: blanco@ehu.es
Contraseña: ●●●●
Confirmar Contraseña:
Cambiar Contraseña

Se ha modificado el cambiar contraseña para usuarios genéricos. Ahora si se olvida la contraseña se genera una aleatoria y se le envía al correo.

Todo ello se hace con el cifrado.

- 2. ¿Que habéis modificado en la aplicación para asegurarnos que sólo lo puede ejecutar el usuario *admin*?**

```
<location path="~/Admin">
  <system.web>
    <authorization>
      <allow users="admin@ehu.es"/>
      <deny users="*/>
    </authorization>
    <compilation debug="true" strict="false" explicit="true"
targetFramework="4.0"/>
    <httpRuntime/>
  </system.web>
</location>
```

Hemos modificado el web.config y el inicio de sesión.



...
Else

```
If (BoxUsuario.Text.Equals("vadillo@ehu.es")) Then
    Session("Rol") = "P"
    FormsAuthentication.SetAuthCookie("vadillo@ehu.es", False)
```

```
Response.Redirect("~/Especiales/ExportarTareasXMLDocument.aspx")
ElseIf (BoxUsuario.Text.Equals("vadillo@ehu.es")) Then
    Session("Rol") = "P"
    FormsAuthentication.SetAuthCookie("admin@ehu.es", False)
    Response.Redirect("~/Admin/CambiarPassAdmin.aspx")
Else
    Session("Rol") = "P"
    FormsAuthentication.SetAuthCookie("Profesor", False)
    Response.Redirect("~/Profesores/Profesor.aspx")
End If
```