REVIEW LESSON

MTA Course: Web Development Fundamentals
Lesson name: Web Development Fundamentals 5.1
Topic: Configuring authentication and authorization
File name: WebDevFund_RL_5.1

Lesson Objective:

5.1: Configure authentication and authorization. *This objective may include but is not limited to:* Forms Authentication, Windows Authentication; authorization; file authorization; impersonation.

This objective does not include: Windows® Cardspace™ authentication, Passport (Windows Live™ ID) authentication, Custom authentication.

Preparation Details

Prerequisite student experiences and knowledge

This MTA Certification Exam Review lesson is written for students who have learned about Web design and Web application programming. Students who do not have the prerequisite knowledge and experiences cited in the objective will find additional learning opportunities using resources such as those listed in the Microsoft® resources and Web links at the end of this review lesson.

Students should have a basic understanding of how to integrate various authentication schemes into a Web application.

Instructor preparation activities

For this lesson, you will need a computer with Microsoft Office 2007®, and Microsoft Visual Studio 2008® attached to a liquid crystal display (LCD) projector to display and review the Microsoft PowerPoint® document.

Resources, software, and additional files needed for this lesson:

- WebDevFund_PPT_5.1 (PowerPoint Slides)
- WebDevFund_SA_5.1 (Student Activity)

- A Windows-based PC with installed Web development software. Examples include Visual Studio 2008, or
  - Microsoft Visual Basic 2008®, Express Edition (*http://www.microsoft.com/express/downloads/#2008-Visual-Basic*)
  - Microsoft Visual C# 2008®, Express Edition (*http://www.microsoft.com/express/downloads/#2008-Visual-CS*)
  - Microsoft Visual Web Developer 2008, Express Edition (*http://www.microsoft.com/express/downloads/#2008-Visual-Web-Developer*)

Teaching Guide

Essential vocabulary:

authentication—the process of validating client identity, usually by means of a designated third-party authority. The client might be a user, a computer, an application, or a service. The client's identity is called a security principal. To authenticate with a server application, the client provides some form of credentials to allow the server to verify the client's identity. After the client's identity is confirmed, the application can authorize the principal to perform operations and access resources.

Forms authentication—Forms authentication uses an authentication ticket that is created when a user logs on to a site, and then it tracks the user throughout the site. The Forms authentication ticket is usually contained inside a cookie. However, ASP.NET version 2.0, as well as later versions of ASP.NET, supports cookieless Forms authentication, which results in the ticket being passed in a query string.

Windows authentication—the ASP.NET Web application relies on the Windows operating system to authenticate the user.

authorization—the process of determining whether an identity (a user, a computer, an application, or a service) should be granted access to a specific resource.

file authorization—checks the access control list (ACL) of the .aspx or .asmx handler file to determine whether a user should have access to the file. ACL permissions are verified for the user's Windows identity (if Windows authentication is enabled) or for the Windows identity of the ASP.NET process.

impersonation—ASP.NET applications can execute with the Windows identity (user account) of the user making the request when using impersonation. Impersonation is commonly used in applications that rely on Microsoft Internet Information Services (IIS) to authenticate the user.

URL authorization—a process which maps users and roles to URLs in ASP.NET applications. and can be used to selectively allow or deny access to arbitrary parts of an application (typically directories) for specific users or roles.

Lesson Sequence

Activating prior knowledge/lesson staging (10 minutes)

Warm up Activity—"Authentication vs. Authorization"

1. Distribute a notecard to each student**.** Ask the students to write their definition of *authentication* and any example that will help describe the term (it does not have to be related to Web development).
2. On the back of the notecards, students will do the same for the term *authorization.*
3. As a class, discuss the student definitions to compare and contrast authentication and authorization.

Lesson activity (30 minutes)

1. Using the PowerPoint presentation WebDevFund_PPT_5.1, review the concepts for this lesson.
2. Distribute Student Activity WebDevFund_SA_5.1.
   a. Students will demonstrate how to configure Web applications for authorization and authentication and understand the differences between the two.
3. Discuss the key objectives of the review assignment.

Assessment/lesson reflection (10 minutes)

1. Ask some students to display their solutions to portions of the activity.
2. Wrap up and provide homework/enrichment opportunities.

Microsoft resources and Web links

Students who wish to explore this lesson topic further may visit the following links:

Web references:

http://www.asp.net/learn/security-videos/video-376.aspx
http://www.asp.net/learn/videos/video-7420.aspx
http://www.asp.net/learn/videos/video-06.aspx
http://msdn.microsoft.com/en-us/library/aa480476.aspx

Microsoft ASP.NET:

http://www.asp.net

Suggested best practices:

- It may be beneficial to display code examples using the LCD projector for each of the major concepts, particularly when the vocabulary is being reviewed. Randomly select students to demonstrate the concepts to the class. It may also be advantageous to have students complete this activity in small groups.