

Developing Secure Java Web Services, Java EE 6

Duration: 3 Days

What you will learn

The Developing Secure Java(TM) Web Services course provides business component and client developers with the information they need to design, implement, deploy, and maintain secure web services and web service clients using Java technology components and the Java Platform, Enterprise Edition 6 (Java EE 6 platform). Students learn about the need to secure web services and the challenges associated with web services security. Students also learn about prominent industry standards and initiatives developed to provide comprehensive security solutions for web services, and how to apply them to secure web services. In particular, students learn how to secure web services by using application-layer security, transport-layer security, and message-layer security technologies, such as those specified by the WS-* security extensions. Students learn how to secure web services by using the web services security infrastructure built into JavaEE 6 and Glassfish v3 (using Metro 1.2), along with the security providers in Sun Java(TM) System Access Manager 7.1. This comprehensive course also introduces identity management concepts, drivers behind identity management solutions, and Sun Java(TM) System Access Manager functions. Students perform the course lab exercises by using the NetBeans(TM) Integrated Development Environment (IDE), Metro 1.2, Sun Java System Access Manager 7.1 (or OpenSSO), and GlassFish v3.

Learn To:

Apply industry standards to secure web services

Secure web services by using application-layer security, transport-layer security, and message-layer security technologies

Design, develop, implement and maintain standard security mechanisms in web service applications

Audience

Java Developer

Security Compliance Professionals

System Integrator

Related Training

Suggested Prerequisites

Create a Java web service

Demonstrate knowledge of declarative programming concepts

Demonstrate proficiency with XML and interpret XML documents

Display experience with the Java programming language

Course Objectives

Identify the need to secure web services

List and explain the primary elements and concepts of application security

Outline the factors that must be considered when designing a web service security solution

Describe the issues and concerns related to securing web service interactions

Analyze the security requirements of web services

Identify the security challenges and threats in a web service application

Evaluate the tools and technologies available for securing a Java(TM) web service

Secure web services by using application-layer security, transport-layer security, and message-layer security

Describe the concept of identity and the drivers behind identity management solutions

Explain the role of Sun Java System Access Manager in securing web services

Secure web services by using UserName token profile

Secure web services by relying on Sun Java System Access Manager

Course Topics

Encapsulating the Basics of Security

Summarize the characteristics of web services and analyze the impact on application security

Examine how the data exposed by a web service can impact its security requirements

Describe the security principles of web architecture

Describe the characteristics of application security

Describe the technologies used to implement application security

Examining Web Services Security Threats and Countermeasures

Identify the security requirements of web services

List the features that are typically provided by a properly implemented security mechanism

List the security principles for web services

Identify the security challenges and threats in a web service application

Identify the technologies to address the security challenges in a web service application

Securing Java Web Services Using JavaEE

Identify methods to implement security in Java TM Platform, Enterprise Edition (JavaEE) applications

Describe how to use Secure Sockets Layer (SSL) to secure a JavaEE web service application

Outline the security mechanisms used by JavaEE web-tier applications

Describe the JavaEE authentication service

Describe how to secure web services by using application-layer and transport-layer security

Introduction to Web Services Security

Explain message-layer security and its advantages over transport-layer security

Describe various web services security extension specifications and how they address web service security requirements

Web Services Security with JAX-WS and Project Metro

Explain the WS-Policy specification

Describe how to attach policy assertions to a Web Services Description Language (WSDL) file

Describe the web services security technology in Metro

Describe how to configure web services security by using Metro

Understand and use the extension mechanism provided by JAX-WS Handlers to incorporate authentication support in a web service

Understand and use the validation framework provided by WSIT to incorporate authentication support in a web service

Authentication in JAX-WS

Manipulate SOAP structures directly using the SAAJ API

Obtain and verify authentication information using the JAAS API

Identity Management and OpenSSO

Define identity and identity management

Describe the need for identity management in enterprise applications

Identify the technologies behind an identity management solution

Describe the capabilities of OpenSSO

Integrate OpenSSO in the deployment of web services