Securing Java Web Applications v7.0

Course Summary

Description

This course shows experienced developers of Java web applications how to secure those applications and to apply best practices with regard to secure enterprise coding. Authentication, authorization, and input validation are major themes, and students get good exposure to basic Java cryptography for specific development scenarios, as well as thorough discussions of HTTPS configuration and certificate management, error handling, logging, and auditing.

Perhaps the most eye-opening parts of the course concern common web “hacks,” or attack vectors. Students see how easy it is to leave an application unguarded against cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, and other attack types -- and learn that it's also easy to fix such vulnerabilities and the importance of a secure development process.

Objectives

After taking this course, students will be able to:
- Generally, be prepared to develop secure Java web applications, or to secure existing applications by refactoring as necessary.
- Define security constraints and login configurations that instruct the web container to enforce authentication and authorization policies.
- Guard against common web attacks including XSS, CSRF, and SQL injection.
- Validate user input aggressively, for general application health and specifically to foil injection and XSS attacks.
- Configure a server and/or application to use one-way or two-way HTTPS.
- Apply application-level cryptography where necessary.
- Secure log files and establish audit trails for especially sensitive information or actions.

Topics

- Concerns for Web Applications
- Authentication and Authorization
- Common Web Attacks
- Input Validation
- HTTPS and Certificates
- Application-Level Cryptography
- Secure Development Practices

Audience

This course is designed for experienced Java developers.

Prerequisites

Before taking this course, Java programming experience is essential. Servlets programming experience is required. JSP page-authoring experience is recommended but not required.

Duration

Four days
Securing Java Web Applications v7.0

Course Outline

I. Concerns for Web Applications
   A. Threats and Attack Vectors
   B. Server, Network, and Browser Vulnerabilities
   C. Secure Design Principles
   D. GET vs. POST
   E. Container Authentication and Authorization
   F. HTML Forms
   G. Privacy Under /WEB-INF
   H. HTTP and HTTPS
   I. Other Cryptographic Practices
   J. SOA and Web Services
   K. The OWASP Top 10

II. Secure Web Applications
    A. Threats and Attack Vectors
    B. Server, Network, and Browser Vulnerabilities
    C. Secure Design Principles
    D. GET vs. POST
    E. Container Authentication and Authorization
    F. HTML Forms
    G. Privacy Under /WEB-INF
    H. HTTP and HTTPS
    I. Other Cryptographic Practices
    J. SOA and Web Services
    K. The OWASP Top 10

III. Authentication and Authorization
     A. HTTP BASIC and DIGEST Authentication Schemes
     B. Declaring Security Constraints
     C. User Accounts
     D. Safeguarding Credentials in Transit
     E. Replay Attacks
     F. Authorization Over URL Patterns
     G. Roles
     H. FORM Authentication
     I. Login Form Design
     J. EJB Authorization
     K. Programmatic Security
     L. Programmatic Security in JSF

IV. Common Web Attacks
    A. Single Points of Decision
    B. Cross-Site Scripting
    C. Validation vs. Output Escaping
    D. Forceful Browsing
    E. Cross-Site Request Forgery
    F. Request Tokens
    G. Injection Attacks
    H. Protections in JDBC and JPA
    I. Session Management
    J. Taking Care of Cookies

V. Input Validation
   A. Validating User Input
   B. Validation Practices
   C. Regular Expressions
   D. JSF Validation
   E. Bean Validation (a/k/a JSR-303)
   F. Constraint Annotations
   G. Cross-Field Validation
   H. Built-In Support in Java EE
   I. Using a Validator
   J. Producing Error Responses
   K. JSF Validation

VI. HTTPS and Certificates
    A. Digital Cryptography
    B. Encryption
    C. SSL and Secure Key Exchange
    D. Hashing
    E. Signature
    F. Keystores
    G. keytool
    H. Why Keys Aren't Enough
    I. X.509 Certificates
    J. Certificate Authorities
    K. Obtaining a Signed Certificate
    L. Configuring HTTPS
    M. Client-Side Certificates and Two-Way SSL
    N. PKCS #12 and Trust Stores
    O. CLIENT-CERT Authentication
Securing Java Web Applications v7.0

Course Outline (cont’d)

VII. Application-Level Cryptography
A. The Java Cryptography Architecture
B. Secure Random Number Generation
C. The KeyStore API
D. Digital Signature
E. Hashing
F. Password Hashing
G. Why Hashing Isn’t Enough
H. Salts
I. Slow Algorithms
J. Key Lengthening and Key Strengthening
K. The Java Cryptography Extensions
L. The SecretKey and KeyGenerator Types
M. Symmetric Encryption
N. Choosing Algorithms and Key Sizes
O. Dangerous Practices
P. Storing and Managing Keys

VIII. Secure Development Practices
A. Secure Development Cycle
B. Penetration Testing
C. Secure Code Review
D. Error Handling and Information Leakage
E. Failing to a Secure Mode
F. Designing for Failure
G. Back Doors
H. Logging Practices
I. Appropriate Content for Logs
J. Auditing Strategies

IX. Appendix A. Learning Resources