

This advanced 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 learn that it is easy to fix vulnerabilities and the importance of a secure development process.

Course Objectives:

- Learn to develop secure new and existing Java web applications.
- 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.
- Store sensitive information securely, hash user passwords and understand the importance of salting and of using slow hashing algorithms and processes to maximize the safety of stored credentials.
- Secure log files and establish audit trails for especially sensitive information or actions.

Audience: Experienced Java web developers.

Prerequisites: Java programming experience developing web applications is required. Servlet knowledge is required, JSP knowledge is helpful.

Number of Days: 4 days

<p>1 Concerns for Web Applications</p> <ul style="list-style-type: none"> Threats and Attack Vectors Server, Network, Browser Vulnerabilities Secure Design Principles GET vs. Post Container Authentication and Authorization HTML Forms Privacy Under/Web-INF HTTP and HTTPS Other Cryptographic Practices SOA and Web Services The OWASP Top 10 	<p>2 Authentication and Authorization</p> <ul style="list-style-type: none"> HTTP BASIC and DIGEST Authentication Schemes Declaring Security Constraints User Accounts Safeguarding Credentials in Transit Replay Attacks Authorization Over URL Patterns Roles FORM Authentication Login Form Design Session Fixation Protections Programmatic Security Programmatic Security in JSF
--	---

3	Common Web Attacks Forceful Browsing Predictable Resource Locations Using Random Numbers Cross-Site Request Forgery Synchronizer Tokens Injection Attacks Protections in JDBC and JPA Session Management Taking Care of Cookies	Salts Key Lengthening and Key Strengthening Slow Algorithms The Java Cryptography Extensions The SecretKey and KeyGenerator Types Symmetric Encryption Choosing Algorithms and Key Sizes Dangerous Practices Storing and Managing Keys
4	Input Validation Validating User Input Validation Practices Regular Expressions Bean Validation (a/k/a JSR-303) Constraint Annotations Cross-Field Validation Built-In Support in Java EE Using a Validator Producing Error Responses JSF Validation	7 Secure Development Practices Secure Development Cycle Penetration Testing Secure Code Review Error Handling and Information Leakage Failing to a Secure Mode Back Doors Logging Practices Appropriate Content for Logs Auditing Strategies
5	HTTPS and Certificates Digital Cryptography Encryption SSL and Secure Key Exchange Hashing Signature Keystores keytool Why Keys Aren't Enough X.509 Certificates Certificate Authorities Obtaining a Signed Certificate Configuring HTTPS Client-Side Certificates and Two-Way SSL PKCS #12 and Trust Stores CLIENT-CERT Authentication	
6	Application-Level Cryptography The Java Cryptography Architecture Secure Random Number Generation The KeyStore API Digital Signature Hashing Password Hashing Why Hashing isn't Enough	