



Capstone Courseware, LLC

33 Boylston Street
Jamaica Plain, MA 02130

877-227-2477
capstonecourseware.com

121. Securing Java Web Applications

Version 5.0

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.

Prerequisites

- Java programming experience is essential -- Course 103 is excellent preparation.
- Servlets programming experience is required -- Course 110.
- JSP page-authoring experience is recommended but not required -- Course 112.



Learning Objectives

- 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.
- 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.

Timeline: 3 days.

IDE Support: Eclipse WTP 2.0

In addition to the primary lab files, an optional overlay is available that adds support for Eclipse WTP 2.0. Students can code, build, deploy, and test all exercises from within Eclipse, and take advantage of WTP's built-in editors, integrated debugging, and wizards for web applications, XML files, JSPs, and more. See also our orientation to Using Capstone's Eclipse Overlays, and please be advised that this is an optional feature; it is not a separate version of the course, and the course itself does not contain explicit Eclipse-specific lab instructions.





Chapter 1. Secure Web Applications

- Threats and Attack Vectors
- Server, Network, and 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

Chapter 2. Authentication and Authorization

- 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
- EJB Authorization
- Programmatic Security
- Programmatic Security in JSF

Chapter 3. Secure Application Design

- Single Points of Decision
- Cross-Site Scripting
- Validation vs. Output Escaping
- Forceful Browsing
- Cross-Site Request Forgery
- Request Tokens
- Injection Attacks
- Protections in JDBC and JPA
- Session Management
- Taking Care of Cookies
- Validating User Input
- Validation Practices





Regular Expressions
JSF Validation

Chapter 4. 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

Chapter 5. Application-Level Cryptography

The Java Cryptography Architecture
Secure Random Number Generation
The KeyStore API
The Signature Class
The SignedObject Class
The MessageDigest Class
The Java Cryptography Extensions
The SecretKey and KeyGenerator Types
The Cipher Class
Choosing Algorithms and Key Sizes
Dangerous Practices

Chapter 6. Secure Development Practices

Secure Development Cycle
Error Handling and Information Leakage
Failing to a Secure Mode
Logging Practices
Appropriate Content for Logs
Auditing





Strategies: Filters, Interceptors, and Command Chains
Penetration Testing
Back Doors

Appendix A. Learning Resources

System Requirements

Hardware Requirements (Minimum)	1 GHz, 256 meg RAM, 500 meg disk space.
Hardware Requirements (Recommended)	1.5 GHz, 512 meg RAM, 1 gig disk space.
Operating System	Tested on Windows XP Professional. Course software should be viable on all systems which support a J2SE 5.0 JDK.
Network and Security	Limited privileges required -- please see our standard security requirements at http://capcourse.com/Guides/Security.html .
Software Requirements	All free downloadable tools.

