Securing Java Applications (Custom for Boeing)

Course Summary

Description

This advanced course shows experienced developers of Java enterprise applications how to secure those applications and to apply best practices with regard to secure coding. Authentication, authorization, and input validation are major themes, and participants use cryptographic algorithms (via the JCA and JCE) for specific development scenarios. The course alson includes thorough discussions and hands-on exercises in common web-application concerns and hacks (XSS, injection, etc.), HTTPS configuration and certificate management, error handling, logging, and auditing.

Objectives

At the end of this course, students will be able to:

- Be prepared to develop secure Java web applications, or to secure existing applications by refactoring as necessary.
- Instruct the web container to enforce your desired authentication and authorization policies.
- Validate user input aggressively, for general application health and to foil specific attacks including injection and XSS.
- Be on guard against common web-application attack vectors such as cross-site scripting, injection, and request forgery, and take appropriate counter-measures.
- Configure a server and/or application to use one-way or two-way HTTPS.
- Use cryptography appropriately in application design and implementation, including signature and signature verification, encryptiong, hashing, and tactical use of secure random numbers.
- Secure log files and establish audit trails for especially sensitive information or actions.

Topics

- Java SE Security
- Secure Coding Practice
- Java EE Security
- Authentication and Authorization
- Special Concerns for Web Applications
- HTTPS and Certificates
- Cryptography in Java SE
- Cryptography in Web Applications
- Secure Development Practices

Audience

This course is appropriate for experienced Java developers who want to be able to follow secure development practice and to secure new and existing standalone, web, and enterprise applications.

Prerequisites

This course is designed for students with java programming experience, including understanding of OO practices, exception handling and multi-threading. Servlets programming experience is recommended but not required. JSP page-authoring experience is recommended but not required.

Duration

Four days

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

ProTech
protechtraining.com

"Charting the Course ...

... to Your Success!"

Securing Java Applications (Custom for Boeing)

Course Outline

I. Java SE Security
- A. The AccessController Class Utility
- B. Permissions, Code Sources, and Protection Domains
- C. The Policy Class
- D. Policy Files

II. Secure Coding Practice
- A. Code Injection
- B. Final Classes and Methods
- C. Inner Classes
- D. Singletons, Factories, and Flyweights
- E. Methods, Collections, and Data Hiding
- F. Object Serialization
- G. Software Bugs as Security Holes
- H. Overflows, Overruns, and Wraparounds
- I. Race Conditions

III. Java EE Security
- 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

IV. 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

V. Special Concerns for Web Applications
- 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
- K. Validating User Input
- L. Validation Practices
- M. Whitelist Validation
- N. Blacklist Validation
- O. Regular Expressions
- P. Constructing REs
- Q. Using REs in Java
- R. 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

VII. Cryptography in Java SE
- A. The Java Cryptography Architecture
- B. The KeyStore API
- C. The Signature Class
- D. The SignedObject Class
- E. Signing and Sealing JAR Files
- F. Verifying JAR Signatures
- G. Authorizing Code by Signature

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Securing Java Applications (Custom for Boeing)

Course Outline (cont'd)

VIII. Cryptography in Web Applications

A. Secure Random Number Generation
B. The MessageDigest Class
C. The Java Cryptography Extensions
D. The SecretKey and KeyGenerator Types
E. The Cipher Class
F. Choosing Algorithms and Key Sizes
G. Dangerous Practices
H. Using JSSE

IX. Secure Development Practices

A. Secure Development Cycle
B. Error Handling and Information Leakage
C. Failing to a Secure Mode
D. Logging Practices
E. Appropriate Content for Logs
F. Auditing
G. Strategies: Filters, Interceptors, and Command Chains
H. Penetration Testing
I. Back Doors

X. Appendix A. Learning Resources

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically

Course Title

Course Outline (con't)

Due to the nature of this material, this document refers to numerous hardware and software products by their trade names. References to other companies and their products are for informational purposes only, and all trademarks are the properties of their respective companies. It is not the intent of ProTech Professional Technical Services, Inc. to use any of these names generically