Szkolenie: Capstone Courseware
121 Securing Java Web Applications

<table>
<thead>
<tr>
<th>FORMA SZKOLENIA</th>
<th>MATERIAŁY SZKOLENIOWE</th>
<th>CENA</th>
<th>CZAS TRWANIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stacjonarne</td>
<td>Tradycyjne</td>
<td>3750 PLN NETTO*</td>
<td>4 dni</td>
</tr>
<tr>
<td>Stacjonarne</td>
<td>Tablet CTAB</td>
<td>4150 PLN NETTO*</td>
<td>4 dni</td>
</tr>
<tr>
<td>Metoda dlearning</td>
<td>Tradycyjne</td>
<td>3750 PLN NETTO*</td>
<td>4 dni</td>
</tr>
<tr>
<td>Metoda dlearning</td>
<td>Tablet CTAB</td>
<td>3750 PLN NETTO*</td>
<td>4 dni</td>
</tr>
</tbody>
</table>

* (+VAT zgodnie z obowiązującą stawką w dniu wystawienia faktury)

LOKALIZACJE

Kraków - ul. Tatarska 5, II piętro, godz. 9:00 - 16:00
Warszawa - ul. Bielska 17, godz. 9:00 - 16:00

Cel szkolenia:

Version 7.0

This course shows Java web developers how to secure their 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.

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.
- 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.

Plan szkolenia:

- Chapter 1. Concerns for 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
- 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
  - Session Fixation
  - Protections
  - Programmatic Security
  - Programmatic Security in JSF
- Common Web Attacks
  - Forceful Browsing
  - Predictable Resource Locations
  - Using Random Numbers
Cross-Site Scripting
Output Escaping
Cross-Site Request Forgery
Synchronizer Tokens
Injection Attacks
Protections in JDBC and JPA
Session Management
Taking Care of Cookies

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

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

Application-Level Cryptography
- The Java Cryptography Architecture
- Secure Random Number Generation
- The KeyStore API
- Digital Signature
- Hashing
- Password Hashing
- Why Hashing Isn't Enough
- 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

- Secure Development Practices
  - Secure Development Cycle
  - Penetration Testing
  - Secure Code Review
  - Error Handling and Information Leakage
  - Failing to a Secure Mode
  - Designing for Failure
  - Back Doors
  - Logging Practices
  - Appropriate Content for Logs
  - Auditing Strategies

Wymagania:

- [Java programming](#) experience is essential -- Course 103 is excellent preparation.
- Servlets programming experience is required -- Course 111.
- JSP page-authoring experience is recommended but not required -- again, Course 111.

Poziom trudności
Certyfikaty:

The participants will obtain certificates signed by Capstone Courseware.

Prowadzący:

Authorized Capstone Courseware Trainer.