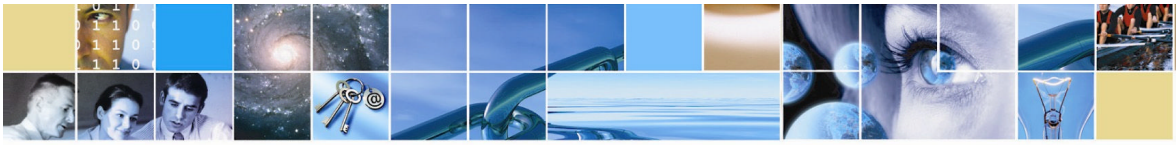

OPTIMA..bit
business information technology

Seminar: Angriff und Verteidigung: Sicherheit für J2EE Applikationen

Beschreibung: Dieses Seminar spricht Manager und Entwickler an, die Ihre Enterprise Anwendungen gegen interne und externe Hacker schützen wollen. Es zeigt wie Java Sicherheitsmechanismen angewendet werden, um Datenschutz und Datenintegrität zu gewährleisten.

Das Seminar basiert auf konkreten Erfahrungen und Beispielen aus der Praxis: es wird keine graue Theorie vermittelt. Fast alle kritischen Phasen eines Projektes werden besprochen, inklusiv sicherer Logins mit JAAS, Secure Sockets (SSL), sicheren Datenbankverbindungen, Container Managed Security und rollenbasierter Sicherheit für Web Applikationen und EJBs.

Eine Besonderheit dieses Seminars ist die konkrete Verwendung von Hackertechniken wie Cross Site Scripting und SQL Injection. Hier werden Angriffe mittels Hackertools durchgeführt. Somit lernen die Teilnehmer wie sie ihre Anwendungen auch gegen fortgeschrittene Angriffstechniken schützen können.

Viele Probleme und Lösungen werden anhand von konkreten Beispielen besprochen. Einige Hacker Tools werden vorgestellt (Prinzip: Know Your Enemy!)

Zielgruppe: Java und J2EE Entwickler, Projekt Manager

Dauer: 2 Tage

Voraussetzungen: Java und J2EE (JSP, Servlet, EJB) Kenntnisse

Inhalt:

Überblick auf J2EE Enterprise Sicherheit
Überblick auf Java Sicherheit
Applikationssicherheit
OWASP Top-10 (Cross Site Scripting, SQL Injection, usw)
Hackertools und Techniken

Sichere Logins mit JAAS
Prinzipien und Konfiguration von Modulen
Beziehungen zu J2EE Rollen
Subjects, Principals und Credentials
Überblick auf Sicherheit für EJBs

Rollenbasierte Sicherheit und Web Applikationen
Wichtige Sicherheitseinstellungen am Container
Rollen abfragen und benutzen
Container Managed Logins

Anti-Hacking Maßnahmen
Sichere Verwendung von SSL
Cross Site Scripting (Stored, Reflected)
Injection (SQL, LDAP, XPATH, usw.)
Sicheres Session-Management (Cookies, URL Rewriting)
Parameter Manipulation
http Header Angriffe (Response Splitting)
HTTP Methods (PUT, DELETE, usw)
Absicherung von JDBC
Absicherung von JNDI
Absicherung von Default Servlets
Kryptographie und Verschlüsselung
Cross-Site Request Forgery