Securing Web Applications (4 Days)

Audience

This course is designed for Java developers, system designs and project managers that seek to design, create and implement secure applications.

Course Abstract

Our Web Security class will illustrate how to ensure your web applications are deployed with the most advanced security measures for coding, communication and configuration. The class begins by discussing threats and mitigation techniques, application of security design principles, conventional and public key cryptography, and the most popular authentication protocols, including SSL and TLS, encryption and hashing, OWASP utilization, SQL injection, cross-site scripting, web service security vulnerabilities, session hijacking, AJAX issues, SOAP message protection, security flaw detection and review of security design patterns.

Objectives

Upon conclusion, each participant will have acquired these skills:

- Illustrate current security challenges and highlight application flaws
- Depict security architecture and design patterns (web, business, services and identity tiers) to ensure CIA principles
- Illustrate Public Key Cryptography, Hashing, Signatures and Symmetric Encryption
- Learn the role of Java Authentication Authorization Services (JAAS)
- Depict the usage of JAAS Authentication and Authorization
- Discuss secure communications with SSL and TLS
- Discuss the functions of the JEE Security Manager
- Understand the role of OWASP in web application security
- Discuss threats and mitigation techniques with SQL injection
- Illustrate digital certificates and their role in message security
- Demonstrate the techniques for managing security for Web Services
- Depict input validation, use of trust boundaries and protection against cross-site scripting
- Managing AJAX security issues
- HTTP Authentication and Authorization
- Demonstrate Servlets and role-based security

Class Format

Lecture/Lab

Prerequisites

You should be familiar with the basics of the web system architecture including processes, class loading, and threads. Some programming experience on the Java platform is preferable.

COURSE TOPICS

I. IT Security Status

- Security basics
  - Confidentiality
  - Integrity
  - Authentication/Authorization
  - Non-repudiation
- Cryptographic roles
  - Key management
  - Trust models
  - Revocation
  - Random generation
- Application flaws and threat modeling
- Security realities
- Security threat layers
  - Hub and Spoke
  - Perimeter
  - Identity
  - Hardware
  - OS
- Security patterns
- Services security

II. Security Patterns

- Best practices
- Review patterns catalog
- Pattern design methodology
- Tier patterns
  - Services
  - Identity
  - Provisioning
  - Personal

III. Communication Security

- SSL architecture
- SSL alert protocols
- SSL threats
- Use of TLS
- Security certificates
  - Digital certificates
  - CA utilization
  - Distribution
  - Revocation

IV. Application Server Security

- HTTP restrictions
- HTTPS utilization
- Security API
    - Hashing algorithms
    - Cryptographic API
    - JCE API
    - JSSE
    - JAAS
- Certificate management
- Encryption techniques
    - Symmetric vs Asymmetric
    - Block cipher
    - Cipher Block
- Session authentication
    - Hijacking prevention
    - Request forgery
    - Vulnerabilities
    - Session fixation issue
    - Timeout issues
    - Encryption threat mitigation

V. Web Application Security

- Role-based granularity
- Use of OWASP
- OWASP vulnerabilities
    - Injection flaws
    - Authentication and Sessions
    - Cross-site scripting
    - Direct object references
    - Sensitive data
    - Access granularity
    - Invalidated redirects
- Application role security
    - Client tier
    - EJB tier
    - Component tier
- Error handling
    - Standardized error management
    - Request faults
    - Page faults

VI. AJAX Management

- AJAX components
- Asynchronous issues
- Vulnerabilities
    - Javascript
    - SQL injection
    - Bridging
    - XSS
- Vulnerability testing

VI. Web Services Security

- Architecture
- Core issues
    - Threats
    - Vulnerabilities
    - Risks
- Security requirements
    - Authentication
    - Integrity
    - Traceability
    - Confidentiality
    - Non-repudiation
    - Interoperability
- XML encryption
- XML Key management
- WS-Security

VII. Identity Management

- Core issues
- SAML overview
- SAML Architecture
    - Assertions
    - Domain model
    - Policy enforcement
    - Request-Reply model
    - Attribute assertion
    - XML signatures

VIII. Application Scanning

- Application threat analysis
    - SQL injection
    - XSS
    - Command execution
    - Server configuration
    - Directory traversal
- Use of tools
    - Commercial
    - Software-as-a-Service
    - Open Source

IX. Security Design Patterns

- Web-tier
  - Authentication
  - Enforcers
  - Validators
  - Proxy
  - Interceptors
- Business-tier
  - Container managed
  - Obfuscation
  - Delegator
  - Facade
  - Service management
- Web Service tier
  - Network layer stack
    - Perimeter defense
    - XML firewall
  - Transport layer stack
    - Infrastructure
    - Identity provider
    - Directory services
  - Message layer stack
    - Interceptor
    - Secure router
    - Gateway