

Securing Web Applications, Services and Servers: Hands-On - 4 Days

Course 940 Overview

You Will Learn How To

- Implement and test secure Web applications in your organisation
- Identify, diagnose and correct the most serious Web application vulnerabilities
- Configure a Web server to encrypt Web traffic with HTTPS
- Protect Ajax-powered Web 2.0 applications
- Secure XML Web services with WS-Security
- Audit Web application security with manual and automated scanning

Course Benefits

Cybersecurity is a serious challenge today as attackers specifically target Web application vulnerabilities. These vulnerabilities can be exploited to obtain confidential information and compromise organisational integrity. As a result, organisations must integrate robust security measures into the Web application development process. This course provides in-depth, hands-on experience securing Web-based applications and host servers.

Who Should Attend

Those who want to implement, test and deploy secure Web applications. Basic knowledge of Web application operation and Web server administration is assumed. Web application development and security knowledge are helpful but not required.

Hands-On Training

Throughout this course, extensive hands-on exercises based on an evolving case study provide you with practical experience in securing applications. Exercises include:

- Creating a trust boundary with proper input validation
- Avoiding cross-site scripting (XSS) and cross-site request forgery (CSRF/XSRF)
- Preventing SQL injection vulnerabilities
- Implementing URL access restrictions
- Detecting unauthorised file system modification
- Enabling HTTPS on a Web server
- Protecting Web services with WS-Security
- Identifying vulnerabilities with an application scanner

Securing Web Applications, Services and Servers: Hands-On - 4 Days

Course 940 Outline

Setting the Stage

- Defining threats to your Web assets
- Surveying the legal landscape and privacy issues
- Exploring common vulnerabilities

Establishing Security Fundamentals

Modelling Web security

- Achieving confidentiality, integrity and availability (CIA)
- Performing authentication and authorisation

Encrypting and hashing

- Distinguishing public- and private-key cryptography
- Verifying message integrity with message digests, digital signatures and digital certificates

Augmenting Web Server Security

Configuring security for HTTP services

- Managing software updates
- Restricting HTTP methods

Securing communication with SSL/TLS

- Obtaining and installing server certificates
- Enabling HTTPS on the Web server
- Protecting the exchange of credentials

Detecting unauthorised modification of content

- Configuring permissions correctly
- Scanning for file-system changes

Implementing Web Application Security

Employing OWASP resources

- The Open Web Application Security Project (OWASP) Top Ten
- Recognising cybersecurity risks
- Remediating identified vulnerabilities

Securing database and application interaction

- Uncovering and preventing SQL injection
- Defending against an insecure direct object reference
- Limitations of encrypting database content

Managing session authentication

- Protecting against session ID hijacking
- Enforcing URL access control
- Blocking cross-site request forgery

Controlling information leakage

- Displaying sanitised error messages to the user
- Handling request and page faults

Performing input validation

- Establishing trust boundaries
- Revealing and removing the threat of cross-site scripting (XSS)
- Exposing the dangers of client-side validation
- Preventing E-shoptlifting

Enhancing Ajax Security

Ajax features

- Identifying core Ajax components
- Exchanging information asynchronously

Assessing risks and evaluating threats

- Managing unpredictable interactions
- Exposing JSON vulnerabilities

Securing XML Web Services

Diagnosing XML vulnerabilities

- Identifying non-terminated tags and field overflows
- Uncovering Web service weaknesses

Protecting the SOAP message exchange

- Validating input with an XML schema
- Encrypting exchanges with HTTPS
- Implementing WS-Security with a framework
- Authenticating access to Web services

Scanning Applications for Weaknesses

Operating and configuring scanners

- Matching patterns to identify faults
- "Fuzzing" to discover new or unknown vulnerabilities

Detecting application flaws

- Scanning applications remotely
- Strategies for testing and scanning
- Testing Web applications with Netcat, Cryptcat and Wget
- Intercepting traffic with OWASP WebScarab

Best Practices for Web Security

Adopting standards

- Reducing risk by implementing proven architectures
- Handling personal and financial data
- Developing guidelines for logging

Managing network security

- Modelling threats to reduce risk

- Integrating applications with your network architecture