Web Application Security

Simply, the securing of web applications

eXtreme hacking
Defending Your Site

Date & Venue

14th – 15th January 2008
(Monday & Tuesday)
9.00am – 5.30pm

Knowledge Connection Pte Ltd

1 Maritime Square #10-33A/B
HarbourFront Centre (Lobby C)
Singapore 099253

Course Fees

S$1,600 (excludes GST)

Course Pre-requisites

- ☑ Basic knowledge in web application technology or web application development
- ☑ Basic knowledge of general network infrastructure

Registration & Contacts

For registration and more information, please contact Cindy Lee at:

Tel: +65-6309 6180
Email: risk.eys@sg.ey.com

Q What is the buzz around web application security?

To keep up with increasing global demands for better information mobility, the recent proliferation of web-enabled applications and web services has outpaced most organizations' ability to keep up with new threats and security challenges. Web applications—either internally developed or packaged—are often the weak link that hackers exploit to compromise your sensitive data.

Q How is the security of web applications compromised?

The security of web application can be easily compromised when insecure design, processes, programming practices, or supporting technologies are deployed during the development process. In addition, existing network defenses such as Intrusion Detection Systems or firewalls provide little protection against web application attacks.

Q How is the course delivered?

The course, structured over two days, is presented through a series of thought-provoking lectures, demos, and lab sessions. Taught by full-time security practitioners with years of large-scale enterprise application assessment experience, you can ensure that your learning experience is truly an exciting and well-rounded one.

Q How will I benefit from the course?

Ernst & Young's Web Application Security course has been specially designed to educate participants with a proper balance of the technical guts of application development and the understanding of secure design, architecture, and processes. At the end of the course, participants will gain an understanding of how to make better decisions to reduce ad-hoc remediation costs and enhance web applications, without exposing critical resources to unacceptable levels of risk.

Q Who should attend?

Day 1 – Vital session for security professionals, application architects/designers, system analysts and developers to examine threats that pose critical risks to typical web applications and services and the technical skills required to defend and protect their organization's web applications.

Day 2 – Crucial for security professionals, project management staff, architects/designers and system analysts to gain a thorough understanding of the importance of entrenching security into various stages of the web application's life cycle.

ERNST & YOUNG
Quality In Everything We Do

Course Overview

Day 1

Evolution of Hacking
- Approaches and techniques in systems and network hacking
- Motivation for hacking web applications
- Emerging web technologies (Web 2.0, AJAX, Web Services, SOA)

Threat Profiling and Risk-Based Security testing
- Techniques to identify and profile threats
- Principles to identify control objectives to mitigate risks posed by threats
- Develop risk-based test scenarios

Web Application Security Framework
- Using Web Application Security Framework and Methodology to perform web penetration test
- Infrastructure and Application Security profiling

Input Validation
- Secure input validation techniques
- Risks and best practices for Client-side controls, SQL injection, Cross Site Scripting, Cross Site Request Forgery and Command Injection

Authentication and Access Control
- Risks and best practices for authentication and access control

Session Management
- Risks and best practices for session handling, predictable session ID, ineffective timeout and logout

Cryptography and Random Number
- Risks and best practices for the use of random numbers and cryptography

Error Management
- Use of failsafe principles in web applications
- Risks and best practices for error management

Hacking AJAX
- Risks and best practices for implementing AJAX

Web Services Security
- Introduction to Web Services Architecture and components
- Understanding Web Services Security Standards
- Using Web Services Assessment Methodology and tools to assess web services security
- Web Services threats and countermeasures

Ultimate Web Hacking Lab Challenge

Day 2

Common Pitfalls and Controls in Web Applications
- Identify the common design and implementation flaws of web applications

Platform and Web Server Security Configuration
- Implementation of platform security
- Risks and best practices for web server configuration

Web Application Security in System Development Life Cycle
- Introduction to System Development Life Cycle
- Applying security in the Systems Development Life Cycle processes of web applications

Web Application Security Management Processes
- Applying security management processes to web applications

Comparison of Automated Tools and Manual Approach
- Understand the pros and cons of assessment and defense tools and manual approach of web application security testing

Service Oriented Architecture Security
- Introduction to Services Oriented Architecture
- Risks and best practices implementing Service Oriented Architecture