

Rui Pereira, B.Sc.(Hons), CIPS ISP, CISSP, CISA, CWNA/CWSP, CPTC/CPTC  
Principal Consultant, WaveFront Consulting Group  
[ruiper@wavefrontcg.com](mailto:ruiper@wavefrontcg.com) | 1 (604) 961-0701 | [www.wavefrontcg.com](http://www.wavefrontcg.com)

The Internet may be a great place to do business, but it has its dangers. According to the most recent Symantec Internet Threat Report (<http://www.symantec.com/business/theme.jsp?themeid=threatreport>), "In 2009, 60 percent of identities exposed were compromised by hacking attacks, ... The majority of these were the result of a successful hacking attack on a single credit card payment processor. The hackers gained access to the company's payment processing network using a **SQL-injection attack**." The 2008 report identifies 12,885 site-specific vulnerabilities, with **63% of all vulnerabilities affecting Web applications**. Cyber criminals are always searching for ways to make easy money, and insecurely coded Web Applications provide easy pickings. Given that most organizations are not even aware of the problem, this is a disaster waiting to happen (and has already happened to some high profile organizations - see <http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database>).

## Course Description

This four-day course aims to provide web application developers with an understanding of application security issues and attack vectors, and the skills, tools and techniques necessary to code defensively against web attacks. We will show how hackers can abuse web applications, and what developers can do to prevent this. We also show how developers and testers can test their own applications in order to determine if they are susceptible to web application attacks. The material would also be of interest to software testers (QA); system, network and database administrators; software, network and system architects; Information Security personnel; and Compliance Officers (Privacy, SOX, PCI, etc.)

Although we use Java and .NET examples throughout, the material is platform agnostic. The idea is to teach fundamental concepts which can be applied no matter the web application development platform in use. We will concentrate on platform-specific security issues on Day 4, and will spend some time on Microsoft ASP/.Net, Java, PHP, Oracle and Ajax. We can address specific platforms used by students if requested. In each area, the course covers theoretical foundations, common implementation pitfalls, details on historical exploits, suggested security policies, implementation best practices, and pseudo-code examples.

The course involves both lectures and hands-on computer labs and exercises. We use mainly open source security tools and sample web applications, although some commercial tools are also discussed and demonstrated. We provide all the necessary equipment and software.

## Learning Outcomes

At the end of this course the student should be able to:

- Recognize and implement techniques to deal with web client and server vulnerabilities;
- Explain potential problems with state-based attacks;
- Discuss and design ways to prevent attacks on user-supplied inputs;
- Explain cryptography and privacy issues;
- Understand and be able to implement techniques to address requirements for the confidentiality, integrity and availability of Web Applications;
- Understand and be able to implement techniques to address requirements for the authentication, access control and auditing of Web Applications;
- Understand and implement techniques for testing Web Applications for security issues;

- Understand the types of Web Application attacks available, and how to design applications to defend against each of them;
- Understand threat modeling and the various web application attack and defense tools available;
- Understand the web application security techniques available in the major development languages (ASP/.NET, Java and PHP);
- Understand security issues with Web 2.0 technologies;

### **Our Trainer**

This course was developed and is presented by our Chief Trainer, Mr. Rui Pereira, B.Sc.(Hons), CIPS ISP, CISSP, CISA, CWNA/CWSP, CPTE/CPTC. Rui has over 25 years of experience in the IT industry, the last 15 in Information Security and Audit (with many web application penetration tests and vulnerability assessments under his belt). In addition to WaveFront's suite of IT Security courses, Rui has also developed and teaches several courses at the University of British Columbia (UBC) and the British Columbia Institute of Technology (BCIT). Rui's biography and resume are online at [www.wavefrontcg.com/PrincipalConsultants.html](http://www.wavefrontcg.com/PrincipalConsultants.html).

### **Course Outline**

#### **Day 1 - Introduction, Attacks and Defenses**

##### **Introduction**

- What is web application security?
- The problem with web application security
- The cost of insecure software
- Cyber-crime
- Privacy and legislative compliance
- PCI DSS and PABP
- Network/system vs. web application security
- Confidentiality, Integrity, Availability (CIA)
- Threats, Vulnerabilities, Risk, Attacks, Exploits
- Hacking 101
- Web application security standards and guidelines
- The OWASP Top Ten

##### **Web Application Attacks and Defenses**

- SQL Injection
- Cross-Site Scripting (XSS) (incl. XST, CSRF, CRLF Injection and HTTP Response Splitting)
- Broken Access Control
- Logic and control errors
- Remote Code and File Injection
- Parameter Tampering
- Session Hijacking and Fixation
- Cookie manipulation and insecure cookies
- Directory Traversal
- Open Re-Direction
- Forceful Browsing
- Client-Side Issues (Client-side Checks, Password Auto-complete, Cached SSL Pages, Hidden Fields, etc.)
- Insecure data storage and weak cryptography

#### Web Application Attacks and Defenses (continued)

- Known attacks incl. buffer overflows and format string attacks
- Administrative interfaces and uploading files
- Information disclosure and leakage (incl. Forceful Browsing, Verbose error messages, Source code disclosure and Google hacking)
- XML and Web Services issues
- Dangerous HTTP commands
- Authentication issues (passwords)
- Various other issues incl. Clickjacking, HTTP Parameter Pollution, Denial of Service (DoS), Web Crawling / Mirroring, Shopping Cart Software, Sample applications, etc.

### **Day 2 – Authentication, Authorization, Cryptography, User Management, Data Validation, Client Side Security**

#### Authentication

- Fundamental web application security services
- Authentication, Authorization, Accounting (AAA Services)
- Methods of authentication
- Session logout mechanisms
- Centralized authentication and Single Sign-On
- Web Services authentication
- Identification and impersonation on multi-tier systems
- Web authentication attacks

#### Authorization / Access Control

- Authorization models
- Authorization in multi-tier systems
- Role Based Access Control (RBAC)
- Authorization for Web Services
- Web authorization attacks

#### Cryptography for Web Applications

- Conceptual foundation
- Uses of cryptography
- Cryptographic building blocks
- Symmetric and Asymmetric cryptography
- Message Digests and integrity
- Hybrid cryptography
- Digital Certificates and Certificate Authorities
- Cryptography for network traffic
- Cryptography for data at rest
- Key management
- Cryptographic attacks

#### User Management

- Secure user management systems
- Password and account management
- Single Sign-On (SSO) and Identity Management
- Password cracking
- User management Q&A

Data Validation

- Data validation and sanitization
- Data validation models
- Trust boundaries
- Data validation attacks

Client Side Security

- Clients in untrusted environments
- Malicious code
- Client attacks
- Securing the client platform
- Code obfuscation

**Day 3 - Error Handling, Database Security, Logging, Secure Application Architecture, Platform and Web Application Security**

Error Handling and Exception Management

- Designing for failure
- Failing securely
- Designing error messages

Event Logging and Auditing

- Logs and monitoring
- Uses of logs
- Logging processes and problems
- Logging best practices

Database Access and Security

- Database access for web applications
- Connection strings
- Integrated security
- Stored procedures
- Database access controls

Secure Application Architecture

- Exposure and risk
- Web application security architectures
- Multi-tier systems
- Forward and Reverse Proxies
- Sample web architecture

Software Design for Security

- Security and the SDLC
- Secure SDLC deliverables
- Application migration

Platform Security

- Securing the infrastructure
- System administration and server configuration

Sundry Web Application Security Issues  
Session management  
Software security testing  
Penetration Testing  
Threat Modeling  
Attack and defense tools

#### **Day 4 - Secure Web Application Coding in Microsoft ASP/.NET and Java**

##### Microsoft ASP/.Net

Declarative vs. Programmatic security  
Cryptographic support  
Using authentication protocols  
Implementing Role Based Access Control (RBAC)  
User management enhancements in ASP.NET 2.x and 3.x  
Built-in validators  
Session management and integrity  
Leveraging logging facilities  
Security in the .NET environment  
Security for Internet Information Server (IIS) and SQL Database Server

##### Java

The Java security model  
Security in the Java Language  
Application architecture using MVC II  
Java frameworks  
Cryptographic support in JAVA  
Authentication and access control in JAVA (incl. RBAC)  
Built-in validators in JAVA, incl. the JAVA/Apache Struts framework  
Leveraging logging facilities in JAVA  
Session management and integrity in JAVA  
Database access in Java  
Security in the JAVA environment  
Security for the Apache web server, and the MySQL and Oracle database servers  
Java do's and don'ts

##### Security for Other Development Platforms

Secure web application coding in PHP, AJAX (Web 2.0), Flash, Oracle, and other platforms  
Secure coding principles and best practices

##### Code walkthrough's

Contact Rui Pereira at [ruiper@wavefrontcg.com](mailto:ruiper@wavefrontcg.com) or 1 (604) 961-0701 to book a place on the next run-through, or for further information. This document is also available online at [http://www.wavefrontcg.com/IntroWebAppSec\\_2011.pdf](http://www.wavefrontcg.com/IntroWebAppSec_2011.pdf).

Please enquire about our other training offerings, including [“Ethical Hacking, Penetration Testing and Vulnerability Assessments”](#) and [“Wireless Network Security Complete”](#).