

Rui Pereira, B.Sc.(Hons), CIPS ISP, CISSP, CISA, CWNA
Principal Consultant, WaveFront Consulting Group
ruiper@wavefrontcg.com | 1 (604) 961-0701 | www.wavefrontcg.com

The Internet may be a great place to do business, but it has its dangers. According to a recent Symantec Internet Threat Report (Jul-Dec '06), 66% of vulnerabilities disclosed during this period affected Web applications. According to the company's previous threat report (Jan-Jun '06), 77% of all easily exploitable vulnerabilities related to Web applications and servers. 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 - www.webappsec.org/projects/whid/byyear_year_2007.shtml).

Course Description

This 4-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. In addition, we 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 for 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 in the main tends to be platform agnostic. The idea is to teach the fundamental concepts which can be applied no matter the web application development platform being used. 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, CPTS/CPTE. Rui has over 25 years of experience in the IT industry, the last 13 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.

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
- Network/System Security 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)
- Remote Code Injection
- Broken Access Control
- Session Hijacking
- Forceful Browsing
- HTTP Response Splitting
- Cross-Site Tracing (XST)
- Cross-Site Request Forgery (CSRF)
- CRLF Injection
- Parameter Tampering
- Cookie Manipulation
- Verbose Error Messages
- Known Attacks
- Hidden Fields
- Buffer Overflows
- Denial of Service (DoS)

Web Application Attacks and Defenses (continued)
Information and Source Code Disclosure
Insecure Data Storage
Google Hacking
XML and Web Service Issues
Command Injection
Weak Crypto
Client-Side Checks and other client issues
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
Single Sign On
Web Services Authentication
Identification and Impersonation on Multi-tier Systems
Web Authentication Attacks

Authorization / Access Control

Authorization Models
Role Based Access Control
Authorization in Multi-tier Systems
Authorization for Web Services
Web Authorization Attacks

Cryptography

Conceptual Foundation
The Uses of Cryptography
Cryptographic Building Blocks
Symmetric and Asymmetric Cryptography
Message Digests and Integrity
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 and Identity Management
Password Cracking

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 Audit Trails
- Logging Points
- Logging Best Practices

Database Access and Security

- Connection Strings
- Integrated Security
- Stored Procedures
- Database Access Controls

Secure Application Architecture

- Web Application Security Architectures
- Multi-tier Systems
- Proxy Servers
- Securing the Infrastructure
- Software Design for Security
- Software Development Life Cycle Security

Platform Security

- System Administration and Server Configuration

Web Application Security

- 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

- Cryptographic Support in C# and VB
- Using Authentication Protocols in C# and VB
- Implementing Role Based Access Control (RBAC) in C# and VB
- User Management Enhancements in ASP.NET 2.0
- Built-in Validators in C# and VB
- Session Management and Integrity in C# and VB
- Leveraging Logging Facilities in C# and VB
- Security in the .NET Environment
- Security for Internet Information Server (IIS)
- SQL Server Database Security

Java

- Cryptographic Support in JAVA
- Using Authentication Protocols in JAVA
- Implementing Role Based Access Control (RBAC) in JAVA
- Built-in Validators in JAVA
- Using the JAVA Struts Framework for Validation
- Leveraging Logging Facilities in JAVA
- Session Management and Integrity in JAVA
- Security in the JAVA Environment
- Security for the Apache Web Server
- MySQL and Oracle Database Security
- Application Architecture using MVC II

Security for Other Development Platforms

- Secure Web Application Coding in PHP
- Secure Web Application Coding with AJAX (Web 2.0)
- Secure Web Application Coding in Oracle
- Secure Web Application Coding in Selected Platforms
- Secure Coding Principles

Contact Rui Pereira at 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_2009a.pdf.

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