Application Security Training

Course Overview

Table of Contents

Abstract

With the rapid proliferation of web-based technologies, "hackers", too, have shifted their attention from conventional network-based attacks to those targeting web applications. By attending this course you will learn how to identify web application vulnerabilities most commonly exploited by attackers, using the same tools and techniques as used by them. You will also learn about the countermeasures to protect against each of the discussed attacks. The course is hands-on and entails discussions of real world attacks, live demonstrations, and hands-on web hacking labs.

Note: The course is suitable for IT auditors, QA testers, application architects, software developers, and information security professionals. The only pre-requisite is a basic understanding of the HTTP protocol.

Course Agenda

This two day long course covers the following:

Day 1

- Application Security Overview
- Introduction to Security Testing Tools
- OWASP Top Ten
- SQL Injection
- LAB 1
- Cross Site Scripting
- Session Management
- Cookie Manipulation
- LAB 2

Day 2

- Parameter Tampering
- Cross Site Request Forgeries
- CAPTCHA Pitfalls
- HTTP Response Splitting
- Error Handling
- Paros: the Swiss Army Knife
- Security in the SDLC
- Risk Estimation
- Threat Modeling
- LAB 3

Instructors

Our instructors include security experts that have conducted security assessments of hundreds of applications for financial instituions, telecommunications providers, and retail organizations. We have assisted development teams of varying sizes in enhancing the security mechanisms incorporated in their SDLCs. Additionally we have taught application security to hundreds of Fortune 500 information security officers, application developers, and students at the nation's top ranked universities (viz. Carnegie Mellon University).

Appendix: Relevant Staff Biographies

Rohyt Belani, CISSP, CISM

Rohyt Belani is a Managing Partner and co-founder of the Intrepidus Group and Adjunct Professor at Carnegie Mellon University. Prior to starting Intrepidus, Mr. Belani was the Managing Director at Mandiant where he established and ran the practice in New York City. Before joining Mandiant, he worked as a Principal Consultant at Foundstone and Researcher at the US-CERT. During his tenure in the field, Mr. Belani has conducted large enterprise security assessments, offered strategic advice to the Office of the President of the World Bank, reviewed critical financial, retail and telecommunications applications for security flaws, and assisted organizations in responding to high exposure security incidents involving securities fraud and credit card theft.

He is a contributing author for Osborne's Hack Notes – Network Security, as well as Addison Wesley's Extrusion Detection: Security Monitoring for Internal Intrusions.

Mr. Belani is a regular speaker at various industry conferences including Black Hat, OWASP, ASIS, Hack In The Box, Infosec World, CPM and several forums catering to the FBI and US Secret Service agents.

As an industry expert he has written columns and technical articles for online publications like SecurityFocus and SC magazine, and has been interviewed by BBC UK Radio, Forbes magazine, InformationWeek, E-Commerce Times and Hacker Japan.

Mr. Belani holds a Bachelor of Engineering in Computer Engineering from Bombay University and a Master of Science in Information Networking from Carnegie Mellon University. He currently leads the OWASP Java Project a world-wide consortium of Java security experts.

Corey Benninger, CISSP

Corey is a Principal Consultant with the Intrepidus Group, specializing in web and mobile application security. He has performed code reviews and conducted application penetration tests for numerous Fortune 500 clients.

Prior to joining Intrepidus Group’s professional services team, Corey served as a Senior Consultant at Foundstone.

Corey is a polished public speaker and has been invited to speak at leading conferences like Black Hat, OWASP, NYCBSDCon, Secure Development World and Infragard. In addition, his expert opinion has been published in industry publications like eWeek. He has also published several whitepapers on cutting edge security issues, like vulnerabilities in AJAX, and the security implications of web browser data caching. He is the co-founder and leader of the OWASP Mobile Security Project, a consortium of mobile security developers and experts.

Corey has an undergraduate degree from Boston University. He is a Certified Information Systems Security Professional (CISSP).

Mike Zusman, CISSP

Michael Zusman is a Senior Consultant with the Intrepidus Group. Prior to joining Intrepidus Group, Mr. Zusman has held the positions of Escalation Engineer at Microsoft, Security Program Manager at Automatic Data Processing, and lead architect & developer at a number of smaller firms.

In addition to his corporate experience, Mr. Zusman is an independent security researcher, and has responsibly disclosed a number of critical vulnerabilities to commercial software vendors and other clients.

Mr. Zusman has also founded a number of successful entrepreneurial ventures including Global Uplink Solutions Incorporated (acquired by Flare Technologies in 2005) and Dish Uplink LLC, a leader in satellite TV subscription activations in the US.

Mr. Zusman brings 10 years of security, technology, and business experience to Intrepidus Group. He is a CISSP and an active member of the OWASP foundation.