

Ultimate Hacking: Web

Foundstone® Services Training Course

With every application that an organization brings online or ecommerce business that goes live, malicious hackers are waiting to attack. This course provides security professionals with the knowledge and tools to recognize software vulnerabilities, develop countermeasures, and perform ongoing assessments of Internet-facing applications. In a hands-on setting, our instructors offer demonstrations on how attackers can access corporate information with little more than a web browser.

Course Goals

- Identify and respond to web attacks.
- Identify and respond to data validation attacks.
- Work with authorization and vulnerability scanning.

Agenda At A Glance

- Web Technology and Testing Tools
- Data Validation Attacks
- Other Web Attacks
- Authorization, Non-Browser Clients, and Automated Scanners

Audience

- System and network administrators, corporate security personnel, auditors, law enforcement officers, and consultants responsible for investigating malware outbreaks or network investigations.

Course Description

Recommended Pre-Work

Basic understanding of UNIX, Windows OS, computer forensics, and TCP/IP networking is required for the course to be fully beneficial.

Course Outline

Module 1—Web Technology and Testing Tools

- Preparation and Planning
- HTTP Overview
- Profiling the Environment

Module 2—Data Validation Attacks

- Parameter Manipulation
- Cross-Site Scripting
- Data Validation
- SQL Injection
- Other Browser Attacks

Module 3—Other Web Attacks

- Information Disclosure
- Authentication
- User Management
- Session Management
- Other Injection Attacks

Module 4—Authorization, Non-Browser Clients, and Automated Scanners

- Authorization
- Other Clients
- Automated Web Application Vulnerability Scanning
- Wrap-Up/Methodology

To order, or for further information, please call 1 888 847 8766 or email SecurityEducation@intel.com.

