

WEB APPLICATIONS



Ethical Hacking Course

HANDS-ON HACKING WEB APPLICATIONS

Web applications are the new frontier of hacking. With this in mind, *Hands-on Hacking – Web Applications* has been created for IT professionals who wish to understand what really happens whenever an attack is perpetrated to any web architecture component and which vulnerabilities are exploited.

The course offers an effective and complete perspective on logical security issues with a focus on web applications.

Training Overview

This course is targeted at IT professionals who wish to delve deeply into the latest security threats and most advanced techniques used by malicious hackers today to compromise web-based architectures – firewall, webserver, middleware, applications, databases. The goals? ID theft, just to mention one...

The course offers a set of live simulations and live labs featuring a variety of missions on proprietary targets.

Who Should Attend?

- IT managers
- IT security specialists
- Security officers
- Software engineers
- Network administrators
- Individuals and enthusiasts interested in this topic



zone-h
unrestricted information

HANDS-ON HACKING WEB APPLICATIONS

Course Contents

An intensive 2-day course covering the following topics.

Attacks Profiling: Statistics on Web Server Attacks

HTTP Protocol Basics

Web Server Structure

Classification of Web Application Attacks

Authentication

Authorization

Command Execution

Client-side Attacks

Information Disclosure

Logical Attacks

Collecting Information on Our Target: Search Engine Power

Live session

Cross Site Scripting in Depth

Learn how a technique, considered by some as banal, allows in fact attackers to obtain surprising results. But also learn how to avoid XSS attacks...

Live Session

Cookie Manipulation (cURL and Mozilla Firefox)

Live session

Backdoors with Javascript

How to install backdoors using Javascript

Remote Files Reading/Inclusion

Common Errors in PHP Applications

Execution of arbitrary code

Execution of commands

File disclosure

Live session

SQL Injection (simple, blind, advanced)

Attacking a system using SQL vulnerabilities: Form bypassing, Database dump, others

Live Session

Cross Site Request Forgery (CSRF/XSRF)

Encoding Attacks

Bypassing IDS and filtering

Other Vulnerabilities

AJAX

XPath Injection

LDAP Injection

HTTP Response Splitting

How to modify HTTP packets content

The DON'Ts of Web Developing

What You Will Learn

- Typical techniques used to attack web architecture components
- How to think like a hacker to protect your web-based architecture
- How misconfigured web applications impact heavily on security

Course Style: Live Hacking!

Duration

2 days

Prerequisites

Basic programming skills are desirable.

About Zone-H

Zone-H is an independent and open-source digital observatory, considered today as the most authoritative voice on cybercrime in the Internet. The www.zone-h.org homepage registers about 35,000 single accesses and a total of nearly 800,000 clicks, on an average day.

In addition to information and analysis on cyber terrorism and cybercrime, Zone-H offers the IT community, IT Security services and educational programs, providing a constant stream of web monitoring activities, including daily advisories, statistics, updates and news. The data merge into one of the biggest digital archives in the world, including, to date, over 2 million recorded attacks and information on attacker profiles, motivations and methodologies of intrusion.

Zone-H presents a realistic and “no-hat” perspective on web trends, supported by a worldwide community of more than 50 experts, among which are IT professionals, journalists, students and scholars. Zone-H websites are available in 13 different editions: English, Italian, French, Russian, Brazilian, Slovak, Spanish, Japanese, Slovenian, Turkish, German, Latvian and Croatian.

The Zone-H worldwide education and training programs focus on the fundamental aspects of IT Security. The program addresses a wide ranging international audience, promoting “ethical hacking” techniques and utilizing our own unique proprietary cybercrime observatory, to provide a research-based source of training information.

