WEB APPLICATION PENETRATION TESTING TRAINING

focal point

www.focalpoint-sprl.be

Course Description

Introduction to methodologies

We will introduce the most relevant web application security methodologies in use today.

Particular emphasis will be given to the following web application testing methodologies:

- OWASP Testing Guide v.4
- "Web Application Hacker's handbook" book series of Dafydd Stuttard and Marcus Pinto.

CYBER RANGE

Dedicated cyber range with a virtual infrastructure.

TARGET AUDIENCE

Ethical hackers, penetration testers, IT security professionals.

HANDS ON

Hands-on required for each exercise. Laptop is required.

DURATION

5 days (9:00 – 5:00)

Course Description

OWASP Top Ten Overview

We will then cover the OWASP Top Ten, with a short description of each type of critical vulnerability.

A technical example of each OWASP Top Ten vulnerability will be explained and demonstrated during the training course.

TOPICS

- A1 – Injection
- A2 - Broken Authentication and Session Management
- A3 - Cross-Site Scripting (XSS)
- A4 - Insecure Direct Object References
- A5 - Security Misconfiguration
- A6 - Sensitive Data Exposure
- A7 - Missing Function Level Access Control
- A8 - Cross-Site Request Forgery (CSRF)
- A9 - Using Components with Known Vulnerabilities
- A10 - Unvalidated Redirects and Forwards

Course Description

Methodology phases

We will dive into the methodology itself, by starting with information gathering, application analysis, identification of attack vectors and exploitation.

This part will take most of the course time and will be accompanied by hands-on exercises.

TOPICS

- Information gathering
- Test configuration and deployment management
- Analyze application
- Test client-side controls
- Test identity management
- Test authentication system
- Test session management
- Test access controls
- Test for input-based vulnerabilities
- Test function-specific input vulnerabilities
- Test for business / logic flaws
- Test for application server vulnerabilities
- Miscellaneous checks
- Test client-side technologies
- Web-services testing

Course Description

Tools
We will introduce different security tools which aid a penetration tester when performing a web application security assessment.
We will explore all possible options and use of such tools, with particular emphasis on web proxies, such as Burp.

Exploitation
During this part of the training, we will teach how to turn a web application vulnerability in a full system compromise. We will also teach students how a web application vulnerability can be used to perform advanced attacks against their users.

TOPICS

- Web Proxies + Proxy plugins
Burp, OWASP ZAP, Fiddler

- Web application scanners
arachni, skipfish, w3af

- Vulnerability scanners
Nessus, Nmap and Metasploit

- Exploitation frameworks
Metasploit and BeEF

- Network & client-side attacks
Persistence & lateral movement
Payload generation
Advanced attacks with BeEF framework
Social engineering attacks