Advanced WEB APPLICATION PENETRATION TESTING TRAINING

focal point
Cyber Defence Exercises as a Service

www.focalpoint-sprl.be

Course Description

Introduction to advanced techniques

We will introduce the most advanced web application security techniques in use today, and focus on vulnerabilities that are actively being used in the latest breaches.

Particular emphasis will be given to the Tools, Techniques and Procedures we encounter in our Penetration Tests.

VIRTUAL LAB

Dedicated virtual machines with practical exercises.

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

Advanced Class Overview

We will cover the following topics with many hands-on interactive labs per topic.

We will also be exploiting exotic vulnerabilities and focusing on methods used by current attackers.

SYLLABUS

- Advanced Cross-Site Scripting (XSS)
- Bypassing XSS Filters
- Advanced SQL Injection
- Bypassing anti-SQL Injection Filters
- Bypassing Web Application Firewalls
- Exploiting Web Services
- Red Team Assessments
  - Setup
  - OSINT
  - Exploitation
- Mobile App testing & Exploitation
  - Intro to Mobisec
  - Attacking an Android application

Course Description

Tools
We will introduce different security tools which aid a penetration tester when performing a web and mobile application security assessment.
All tools used will be given to students.

Exploitation
During this part of the training, we will teach how APT works introducing a Red Team workshop. Furthermore, we will also teach students how to bypass common filters and controls in many different contexts, and how to take exploitation to the next step.

TOPICS

- Web Proxies + Proxy extensions Burp, OWASP ZAP, Fiddler
- OS distribution for Mobile Hacking – Mobisec
- Exploitation frameworks Metasploit and BeEF
- Red Team Frameworks & Tools Powershell Empire, Cobalt Strike, Encoders, SET