HACKERU

Web Application Penetration Testing

CR110

08
Days

Web Application Penetration Testing

Outline & Objectives

The 8-day Web Application Penetration Testing course teaches participants the fundamentals of penetrating web applications and how to exploit a variety of known vulnerabilities. Participants will be introduced to many techniques used by pentesters and learn how to check for most security vulnerabilities, how to identify security bugs and many more practical skills. The course is geared towards hands-on practitioners and includes a variety of live demonstrations and immersive exercise labs.

Upon course completion, participants will be able to:

- Test web applications and exploit a broad range of vulnerabilities
- Perform lesser-known functions and tricks in order to overcome seemingly impenetrable apps or web functions
- Perform JavaScript basics in order to run penetration tests on a broad level while understanding its impact on security at large

Target Audience

This course is designed for learners who already know the fundamentals of information security and ethical hacking, looking to enter the world of web-app pen-testing.

Primarily

- Ethical Hackers
- Penetration Testers
- Technical Cybersecurity Personnel
- Experienced Web Developers

Prerequisites

- Knowledge in Information Security, Computer Networking and Common Protocols is a must
- Familiarization with ethical hacking and/or infrastructure hacking
- Basic knowledge of web development (HTML, CSS, JavaScript, etc.) is an advantage but not required

Content

Day 1

Module 01
Web Fundamentals

- Web Technologies Overview
- Browser tools & Debugging
- OWASP Top10

Day 1

Module 02
Web Server Installation

- Apache Secure Installation
- Apache Secure Configuration
- Hardening Apache

Day 2

Module 03
Traffic Manipulation

- Burp Suite
- OWASP Zap
- Web Site Enumeration
- Web Application Brute-Force Challenge

Day 2

Module 04
Web Cryptography

- HTTP vs HTTPS
- SSL vs TLS
- Cipher Suites
- OpenSSL – CA vs self-signed certificates

Day 3

Module 05
Introduction to Client-Side Attacks

- Reflected XSS
- Stored XSS
- DOM XSS

Day 3

Module 06
Authorization & Authentication

- CSRF
- Broken Authentication
- Broken Authorization
- Session Attacks

Day 4

Module 07
XML Attacks

- Configuring & Maintaining Databases
- MariaDB
- SQL Syntax

Day 4

Module 08
Marinating Databases

- Error-Based SQL Injection
- Union-Based SQL Injection
- Data Exfiltration
- Injection Automation

Day 5

Module 09
Advanced SQLi

- Blind SQL Injection
- Time-based injection
- NoSQL Injection

Day 5

Module 10
XML Injection

- XML Usage in Web Applications
- XXE
- SSRF
- SSRF through XXE

Day 6

Module 11
PHP Vulnerabilities

- PHP Programming
- PHP Vulnerabilities
- Insecure Input Filtration

Day 6

Module 12
LFI/RFI & Directory Traversal

- LFI
- RFI
- Directory Traversal

Day 7

Module 13
WordPress Hacking

- Content management Systems
- WPScan
- WordPress Enumeration

Day 7

Module 14
File Upload

- File Upload
- PHP Shells

Day 8

Module 15
File Upload

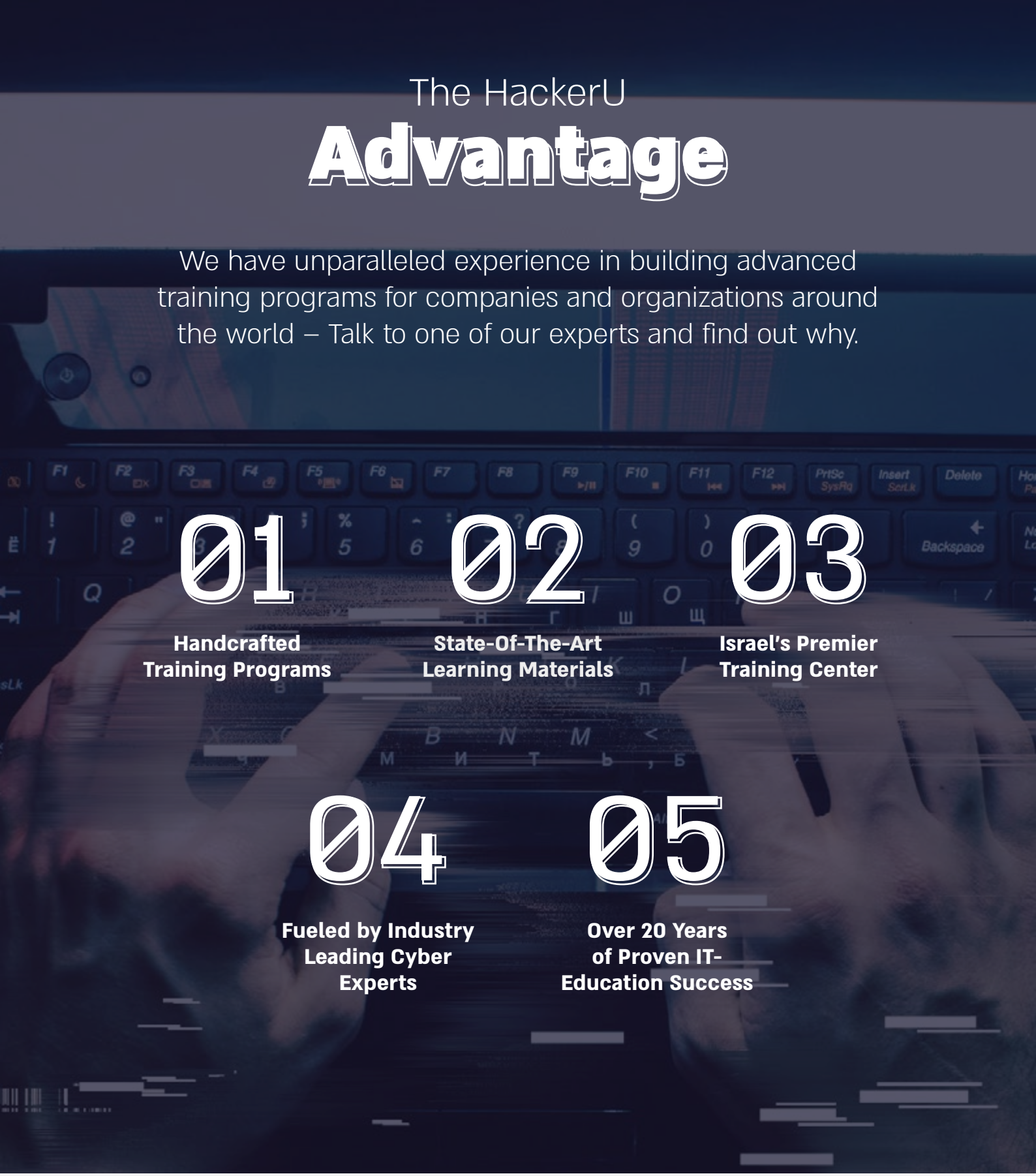
- Nessus
- Qualys
- Writing Reports

Day 8

Module 16
Web Hacking Challenges

- Web Hacking Challenges (CyWar.HackerU.com)

Participants will be introduced to many techniques used by pentesters and learn how to check for most security vulnerabilities



The HackerU Advantage

We have unparalleled experience in building advanced training programs for companies and organizations around the world – Talk to one of our experts and find out why.

01

Handcrafted Training Programs

02

State-Of-The-Art Learning Materials

03

Israel's Premier Training Center

04

Fueled by Industry Leading Cyber Experts

05

Over 20 Years of Proven IT-Education Success

Info@hackerupro.com

hackerupro.com