CONDITION™ ZEBRA

Beyond IT Security Training. We Train Differently

THE COMBAT OF WEB APPLICATION: HACKER VS DEVELOPER

Cyber Security Online Training 2022
The Combat of Web Application: Hacker vs. Developer

In this training, we shall learn about web application penetration testing, web application vulnerability assessments and ways to protect against incoming threats in the manner of virtual hands-on training.

It's recommended that participants should have basic programming language and prior experience in managing, developing or testing web applications.

Training Details

Day 1: Wednesday, 9am to 1pm
Day 2: Thursday, 9am to 1pm
Day 2: Thursday, 2pm to 4pm (optional)
Platform: Microsoft Teams Meeting
Duration: 8 hours (4 hours a day) plus 2 hours mentoring session (optional)
Course Fee: **RM700 (*subject to 6% SST)**

[NOTE]: This is a paid training with *subject to HRDF claim for qualified HRDF contributing companies.

Benefits

- Trained by award-winning Cybersecurity Training Provider with Top Rated Web Pentester.
- 80% practical hands-on training with focus on skill development to successfully learn how to conduct Web Penetration Testing.
- Get an e-certificate of attendance from leading Cybersecurity training provider.
- 100% HRDF (Human Resource Development Fund) claimable under SBL-KHAS
- Materials and technical support provided - Training guide, supporting materials and training access link.

What you will learn?

- The simplest way to master the fundamental of web application security by learning from a top-rated Web Penetration Tester.
- Learn our 5-step Web Penetration Testing methodology refined by experts with years of experience conducting Pentest projects for thousands of clients.
- What is OWASP Top 10 Web Application Risks...? Learn to protect your company from these dangerous risks.
- How to do passive and active information gathering like a Professional Hacker would do before launching their attacks.
- The secrets to avoiding web application attacks that hackers don't want you to know about!
- What NEVER to do best practices so your web application doesn't expose high-security vulnerabilities that can be easily exploited by hackers.
- Do you know that SQL Injection is one of the leading techniques used by 70% of hackers? Learn more about this technique and how to remediate against this!

Who should attend?

- Information Technology Professionals
- Information Security Professionals
- Mobile/Web Application Developer
- Other Business or IT Professionals, who are responsible for IT Security and Data Protection

The Combat of Web Application Course Outline

Day 1 – Module 1 to 5

Module 1: Introduction to Web Application Penetration Testing
      1.1 Introduction to Information Security
      1.2 Penetration Testing and its Necessity
      1.3 Different Stages of Penetration Testing
      1.4 Learn to do Penetration Testing
      1.5 Cyber Law against Hacking
      1.6 Introduction to OWASP Top 10 Web Application Risks

Module 2: Web Application Architecture & Development
      2.1 Typical Web Application Architecture
      2.2 Designing a Sample Webpage
      2.3 Fundamental Web Application Security

Module 3: HTTP Basics
      3.1 Introduction to HTTP
      3.2 HTTP Methods
            3.2.1 Safe Methods
            3.2.2 Unsafe Methods
      3.3 HTTP Status Codes
      3.4 HTTP Security Issues
      3.5 List of HTTP Security Headers
      3.6 HTTPS

Module 4: Information Gathering
      4.1 Passive Information Gathering
            4.1.1 Search Engine Reconnaissance
            4.1.2 Fingerprint Web Server
      4.2 Active Information Gathering
            4.2.1 Identifying Application Entry Points

Module 5: SQL Injection
      5.1 Introduction to SQL Injection
      5.2 Automating SQL Injection
      5.3 Remediation

Day 2 – Module 6 to 9

Module 6: Cross-Site Scripting (XSS)
      6.1 Types of XSS
      6.2 Mitigation

Module 7: Cross-Site Request Forgery (CSRF)
      7.1 How to test?
      7.2 Sample X-CSRF Token Implementation
      7.3 Fixing the Right Way

Module 8: File Inclusion Attacks
      8.1 Local File Inclusion
      8.2 Remote File Inclusion
      8.3 Prevention

Module 9: Mastering Burp Suite
      9.1 Burp Suite as a Proxy
      9.2 Community Version vs. Licensed
      9.3 Components of Burp Suite