Web Application Penetration Tester (CZ-WAPT)

Module 1: Introduction to Web Application and Technologies

Module 2: Client Server Architecture

Module 3: Working with Protocol

Module 4: Web Server and Client

Module 5: Web Application Attacks

- 5.1 OWSAP TOP 10 Vulnerabilities
  - 5.1.1 Injection
  - 5.1.2 Broken Authentication and Session Management
  - 5.1.3 Cross Site Scripting (XSS)
    - 5.1.3.1 Hands-on-Practice
  - 5.1.4 IDOR(Insecure Direct Object References)
  - 5.1.5 Security Misconfiguration
  - 5.1.6 Sensitive Data Exposure
  - 5.1.7 Missing Function Level Access Control
    - 5.1.7.1 Hands-on-Practice
  - 5.1.8 Cross Site Request Forgery
  - 5.1.9 Using Known Vulnerable Components
  - 5.1.10 Unvalidated redirects and forwards

- 5.2 NIC Vulnerability Standards
  - 5.2.1 Malicious File Upload
  - 5.2.2 No lockout & Password Policy
  - 5.2.3 Directory Browsing

Hands-on-Practice

5.2.4 Password Auto Complete

5.2.5 Auto fill Feature

5.2.6 Audit Trail for Admin User

5.2.7 Click Jacking

5.2.8 HTTP Response splitting

5.3 Internet Information Service Attack

Module 6: Web Application Security Audit and Exploitation Tool

6.1 Acunetix Web Vulnerability Scanner

6.2 BurpSuite

6.3 Dirbuster

6.4 Havij

6.5 SQLMap

6.6 SQL Poizon

6.7 Hands-on-Practice

Module 7: Web Application Security Patching

7.1 Brief Introduction of Security Patching

7.2 Patching codes

7.3 Hands-on-Practice

Module 8: Reporting

8.1 Introduction to Reporting Standards

8.2 First Level Reporting

8.3 Second Level Reporting

8.4Web Application vulnerability Audit

8.5 Website Penetration testing Project

Course Duration - 2 Weeks