Web Application Security Expert / Penetration Testing (WASE/WAPT)

Duration: *30 Hrs. / Days*

Prerequisites: *Basic Knowledge of Programming languages such as JavaScript, HTML, SQL*

Module-1

- Introduction to WAPT
- WAPT Lab Environment Setup
- Other Tools
- Difference between Http 1.0 and Http 1.1 and Http 2.0
- HTTP Basics
- Web Technologies – An Overview
- General Web Application Architecture
- Brief about OWASP-10 2017
- Introduction to Burp suite
- Spidering
- Fuzz Testing

Module-2

- Website Reconnaissance and Footprinting.
- Vulnerability Analysis
- Understanding Types of vulnerability
- Scanning or crawling website using Automated Tools
- Wordlist Generation for Intrusion and Cracking
- Encryption and Hash Cracking
- Introduction to Metasploit
- Exploit Search and Payload Generation
- Attacking HTTP Basic Authentication with Nmap and Metasploit
- Understanding HTTP Session ID, HTTP Set-Cookie, HttpOnly

Module-3

- Input Validation techniques
- Blacklist VS. Whitelist Input Validation Bypassing
- Encoding Attacks

- Directory Traversal Vulnerability (Directories and Files)
- Automated Attack for Directory traversal
- Session fixation
- Session Management – Using URL Manipulation
- Session Management – Using Cookie Manipulation
- URL Encoding and Path Traversal Vulnerability
- Information leakage or Sensitive Data Exposure

Module-4

- Unrestricted File Upload
- File Upload Vulnerability Basic
- Bypassing Content-Type Verification in File Uploads
- Bypassing Extension Blacklist in File Upload
- Bypassing File Upload using Double Extensions
- Null Byte Injection in File Uploads
- Directory Listing
- Insecure Login Forms (Broken Authentication)
- Password Attacks (Broken Authentication)

Module-5

- HTTP Parameter manipulation
- Local File Inclusion (LFI) & Remote File Inclusion (RFI)
- Server Side Request Forgery (SSRF)
- Unvalidated Redirects and Forwards (URF)
- Insecure Direct Object Reference (IDOR)
- Clickjacking Attack
- Basics about Web Services
- XML and JSON based Web Services
- REST API SQL Injection.
- XML External Entity (XXE) Processing Vulnerability

Module-6

- PHP Code Injection
- HTML Injection – REFLECTED (GET)
- HTML Injection – REFLECTED (POST)
- OS Command Injection
- OS Command Injection (Blind)
- SQL Injection (GET – Union Based)

- SQL Injection (POST – Union Based)
- SQL Injection (Login Form)
- SQL Injection (Stored)
- SQL Injection (Boolean Based)
- SQL Injection (Blind and Time Based)
- SQL Injection using Automated Tools
- Cross Site Scripting (XSS) – DOM Based
- Cross Site Scripting (XSS) – REFLECTED (GET)
- Cross Site Scripting (XSS) – REFLECTED (POST)
- Cross Site Scripting (XSS) – Stored
- Cross Site Request Forgery (CSRF)
- CSRF Anti-Token Bypassing using XSS

Module-7

- WAPT Report Writing
- Sample Pentesting Reports