Web Application Penetration Testing

Stop the Critical Security Weaknesses & Vulnerabilities.
Start Analyze, Secure & Defend

Course Brochure and Outline

CODEC Networks Pvt Ltd
507, New Delhi House, Barakhamba Road, New Delhi 110001
trainings@codecnetworks.com
+91 11 43752299, 9971676124

Web Application Penetration Testing
Training Program

Course Overview

Web Application penetration Testing (WAPT) is the Security testing techniques for vulnerabilities or security holes in corporate websites and web applications. These vulnerabilities leave websites open to exploitation. The Web Application Penetration Testing course from CODEC Networks is a totally hands-on learning experience. From the first day to the last day, you will learn the ins and outs of Web App Pen Testing by attending thought provoking lectures led by an expert instructor.

Every lecture is directly followed up by a comprehensive lab exercise (we also set up and provide lab workstations so you don't waste valuable class time installing tools and apps). Globally with the rising number of incidents of web defacement, the scope of Web Application penetration Tester is definitely rising. Today Web Application Penetration Testers are in very high demand in software companies, IT security firms, Government and Private Sectors etc.

By the end of the course, you should be able to meet the following objectives:

- An understanding of advanced web penetration techniques
- Skills to test and exploit specific target environments such as content management systems and infrastructure applications
- Understanding of encryption and its usage within web applications
- Methods to recognize and bypass application, platform, and WAF defences
- Skills to test and evaluate web services used in an enterprise
- Understanding how to test backend services for mobile applications

Target Audience

This course is suited for those candidates who want to pursue his/her career as a Web Penetration tester, Web security analyst/consultant, Web Application security analyst.

Course Duration: 40 Hours

Web Application Penetration Testing

Training Program

Course Content

- **Introduction**
  - Introduction to the course.
  - How to get most out of the course
  - Resources you will need for the course
  - What is WAPT?
- **Introduction to Web-application**
  - What is web application?
  - History of Web-Applications
  - Existing problems and challenges in present web applications
  - Overview of web application defences
- **Basics**
  - How a web application works
  - Architecture of web applications
  - Basics of HTML, CSS and Javascript
  - Basics of any server-side language (PHP/J2EE/ASP.NET)
- **HTTP Protocol**
  - Overview of RFC 2616
  - HTTP Messages & Entities
  - HTTP Request, HTTP Response
  - HTTP Status Codes
  - Various types of encoding schemes
- **Web servers and clients**
  - IIS Server, Apache Server and Other Servers
  - Browsers
  - Browser's same origin policy
  - Other Web enabled Clients
- **Server-side and Client-side security controls**
  - Input Validation & Output validation (encoding)
  - Insufficient input & output validations
  - Validation approaches
  - Bypass thin/thick(decompile) client validations
  - Leveraging Ajax and web 2.0 in attacks
  - Bypass Server-side validations
- **Mastering Burp suite**
  - Introduction to burp suite
  - Configuring burp suite
  - Burp proxy, Burp Spider, Burp Intruder, Burp Repeater, Burp Sequencer

Web Application Penetration Testing
Training Program

- **Injections**
  - SQL Injection, Blind SQL Injection, Command Injection, LDAP Injection, XPATH Injection, SOAP Injection
  - Other Injections
  - Implications of Injections
  - Test methodology for injections
  - Remediation
- **Cross-site Scripting**
  - Reflected XSS, Stored XSS, DOM XSS
  - Implications of XSS
  - Test Methodology for XSS
  - Remediation
- **Cross-site Request Forgery**
  - CSRF with GET method
  - CSRF with POST method
  - Implications of CSRF
  - Test methodology for CSRF
  - Remediation
- **Authentication testing**
  - Guessable Passwords
  - Failure Messages
  - Brute forcing login
  - Plain text password transmission
  - Improper implementation of forgot password functionality
  - Remember Me Functionality
  - Guessable User names
  - Multi factor authentication flaws
  - Fail-Open Login Mechanisms
  - Insecure Storage of Credentials
  - Remediation
- **Authorization testing**
  - Introduction to authorization
  - Implementation weaknesses in authorization
  - Horizontal privilege escalation
  - Vertical privilege escalation
  - URL, Form, cookie based escalation
- **Types of web application security testing**
  - Black box testing ,White box testing & Grey box testing

- Vulnerability Assessment vs Penetration testing
- Web application penetration test scope and process
- Legalities of the VAPT

- **Reconnaissance**
  - Foot printing Domain details (whois) - Technicalinfo.net
  - OS and Service fingerprinting – Netcraft.com, Banner grabbing, HTTPprint
  - Google hacking
  - Load balancer Identification
  - Spidering a web site (wget, Burp spider)
  - Application flow charting
  - Relationship analysis within an application
  - Software configuration discovery
- **SSL & Configuration testing**
  - Testing SSL / TLS cipher
  - Testing SSL certificate validity – client and server
  - Infrastructure and Application Admin Interfaces
  - Testing for HTTP Methods and XST
  - Testing for file extensions handling
  - Old, Backup and Unreferenced Files
  - Application Configuration Management Testing
- **Session Management testing**
  - Need for session and state
  - Ways to implement state
  - How session state work
  - What are cookies
  - Common Cookies and Session Issues
  - Man in the middle
- **Brute force web applications**
  - Brute force authentication, Brute force Authorization, Brute force web services, Brute force web server, Brute force .htaccess
- **Parameter Manipulation**
  - Query string manipulation, Form field manipulation, Cookie manipulation, HTTP header manipulation
- **Other Attacks**
  - Sniffing, Phishing & Vishing
  - D(D)OS Attacks
  - Invalidated Redirects and Forwards

Web Application Penetration Testing

Training Program

- **Samurai WTF**
  - Introduction to Samurai WTF
  - Various Tools in Samurai WTF
  - Nikto, w3af, BeEF Framework, Fuzzing and JBroFuzz, DirBuster, Netcat, Brutus and Hydra
  - Overview of various Proxies (zed, rat, paros, webscarab)
- **Firefox security Add-ons**
  - Tamper Data
  - SQL inject me
  - XSS me
  - Firebug
  - Live HTTP headers
  - Foxy Proxy
  - Web Developer
- **Automated Scanners**
  - Acunetix, IBM App Scan, Burp Scanner
  - Effectiveness of Automated tools
  - Reduction of False positives and false Negatives
- **VAPT Methodologies**
  - OWASP, SANS 25, WAHH, OWASP Check-list
- **Reporting**
  - Importance of documentation
  - OWASP Risk rating methodology
  - Creating managerial, technical VAPT reports
  - Open reporting standards