NIIT
India Enterprise Solutions

WAPT Course Curriculum

Day-1

1. Overview of the Course
    - Web Application Security Statistics
    - Introduction to Web Applications
    - Web Application Components
    - How Web Applications Work?
    - Web Application Architecture
    - Web 2.0 Applications
    - Vulnerability Stack
    - Web Attack Vectors
    - Web Application Threats - 1
    - Web Application Threats - 2
    - Unvalidated Input
    - Parameter/Form Tampering
    - Directory Traversal
    - Security Misconfiguration
2. Injection Flaws
    - SQL Injection Attacks
    - Command Injection Attacks
    - Command Injection Example
    - File Injection Attack
    - What is LDAP Injection?
        - How LDAP Injection Works?
        - Hidden Field Manipulation Attack
3. Cross-Site Scripting (XSS) Attacks
    - How XSS Attacks Work?
    - Cross-Site Scripting Attack Scenario: Attack via Email
    - XSS Example: Attack via Email
    - XSS Example: Stealing Users' Cookies
    - XSS Example: Sending an Unauthorized Request
    - XSS Attack in Blog Posting
    - XSS Attack in Comment Field
    - XSS Cheat Sheet

Day-2

4. Cross-Site Request Forgery (CSRF) Attack
    - How CSRF Attacks Work?
5. Web Application Denial-of-Service (DoS) Attack
    - What is Denial of Service Attack?
    - Denial of Service (DoS) Examples
    - How DoS Attacks Work?
6. Buffer Overflow Attacks
    - What is Buffer Overflow Attacks?
    - Buffer Overflow Examples

NIIT
India Enterprise Solutions

- How Buffer Overflow Attacks Work?

7. Cookie/Session Poisoning
   - How Cookie Poisoning Works?
8. Session Fixation Attack
   - How Session Fixation Works?
9. Insufficient Transport Layer Protection
   - What is Insufficient Transport Layer Protection?

Day-3

10. Improper Error Handling
11. Insecure Cryptographic Storage
12. Broken Authentication and Session Management
13. Unvalidated Redirects and Forwards
14. Web Services
    - Web Services Architecture
    - Web Services Attack
    - Web Services Footprinting Attack
    - Web Services XML Poisoning

Day-4

15. Footprint Web Infrastructure
    - Footprint Web Infrastructure: Server Discovery
    - Footprint Web Infrastructure: Server Identification/Banner Grabbing
    - Footprint Web Infrastructure: Hidden Content Discovery
16. Web Spidering Using Burp Suite
17. Hacking Web Servers
    - Web Server Hacking Tool: WebInspect
18. Analyze Web Applications
    - Analyze Web Applications: Identify Entry Points for User Input
    - Analyze Web Applications: Identify Server-Side Technologies
    - Analyze Web Applications: Identify Server-Side Functionality
    - Analyze Web Applications: Map the Attack Surface

Day-5

19. Attack Authentication Mechanism
    - Username Enumeration
    - Password Attacks: Password Functionality Exploits
    - Password Attacks: Password Guessing
    - Password Attacks: Brute-forcing
    - Session Attacks: Session ID Prediction/ Brute-forcing
    - Cookie Exploitation: Cookie Poisoning
20. Authorization Attack
    - HTTP Request Tampering
    - Authorization Attack: Cookie Parameter Tampering
21. Session Management Attack
    - Attacking Session Token Generation Mechanism
    - Attacking Session Tokens Handling Mechanism: Session Token Sniffing

NIIT
India Enterprise Solutions

22. Injection Attacks

Day-6

23. Attack Data Connectivity
    - Connection String Injection
    - Connection String Parameter Pollution (CSPP) Attacks
    - Connection Pool DoS
24. Attack Web App Client
25. Attack Web Services
26. Web Services Probing Attacks
    - Web Service Attacks: SOAP Injection
    - Web Service Attacks: XML Injection
27. Web Services Parsing Attacks
    - Web Service Attack Tool: soapUI
    - Web Service Attack Tool: XMLSpy
    - Web Application Hacking Tool: Burp Suite Professional
    - Web Application Hacking Tools: CookieDigger
    - Web Application Hacking Tools: WebScarab

Day-7

28. Web Application Hacking Tools

29. Encoding Schemes
    - How to Defend Against SQL Injection Attacks?
    - How to Defend Against Command Injection Flaws?
    - How to Defend Against XSS Attacks?
    - How to Defend Against DoS Attack?
    - How to Defend Against Web Services Attack?

30. Web Application Countermeasures

    - How to Defend Against Web Application Attacks?
    - Web Application Security Tool: Acunetix Web Vulnerability Scanner
    - Web Application Security Tool: Falcove Web Vulnerability Scanner
    - Web Application Security Scanner: Netsparker
    - Web Application Security Tool: N-Stalker Web Application Security Scanner

Day-8

31. Web Application Security Tools
    - Web Application Firewall: dotDefender
    - Web Application Firewall: IBM AppScan
    - Web Application Firewall: ServerDefender VP

Day-9

32. Web Application Pen Testing
    - Information Gathering
    - Configuration Management Testing
    - Authentication Testing

NIIT
India Enterprise Solutions

- Session Management Testing
- Authorization Testing
- Data Validation Testing
- Denial of Service Testing
- Web Services Testing
- AJAX Testing

Day-10

33. Case Study & Project

07/12/15

NIIT LIMITED
Kolkata
700 071
68, Pretoria Street