Cyber Security - Application Security - Penetration Testing

OWASP Top 10 Attacks

A1-Injection

A2-Broken Authentication

A3- Sensitive Data Exposure

A4-XML External Entities (XXE)

A5-Broken Access Control

A6- Security Misconfiguration

A7- Cross-Site Scripting (XSS)

A8-Insecure Deserialization

A9-Using Components with Known Vulnerabilities

A10-Insufficient Logging & Monitoring

1. Introduction to Hacking

Networking Basics

IP addressing, Routing, Network Configurations

OSI 7 Layer Model

Protocols, TCP, UDP, ICMP, Ports, DNS, DHCP, SMTP, POP3, IMAP, HTTP, HTTPS, FTP

Analyzing Network Protocols with Wireshark Tool

Operating System

Kali Linux OS installation and commands

Virtual machines- VMWare/Virtual Box Basics

Web Technologies Basics

Client-Side Technologies: HTML, HTML5, JavaScript

Server-Side Technologies: Java, .Net, PHP

Backend Technologies*:* MySQL

Cryptography Concepts

Encoding, Encryption

Symmetric, Asymmetric

Hashing, MAC, Digital Signatures, PKI

Security Testing

Black Box, Grey Box and White Box

SAST and DAST

Vulnerability Assessment and Penetration Testing

SDLC and Secure SDLC

Proxy, Tools, Kali Linux, Add-ons, Extensions

2. Information Gathering

Conduct Search Engine Discovery and Reconnaissance for Information Leakage

Port scanning

Fingerprint Web Server

Review Web server Meta files for Information Leakage

Enumerate Applications on Web server

Review Web page Comments and Meta data for Information Leakage

Identify application entry points

Fingerprint Web Application Framework

Fingerprint Web Application

3. Configuration and Deployment Management Testing

Test Application Platform Configuration

Test File Extensions Handling for Sensitive Information

Review Old, Backup and Unreferenced Files for Sensitive Information

Enumerate Infrastructure and Application Admin Interfaces

HTTP Methods

HTTP Strict Transport Security

Test RIA cross domain policy

4. Identity Management Testing

Test Role Definitions

Test User Registration Process

Test Account Provisioning Process

Testing for Account Enumeration and Guessable User Account

Testing for Weak or unenforced username policy

5. Authentication Testing

Testing for Credentials Transported over an Encrypted Channel

Testing for default credentials

Testing for Weak lock out mechanism

Testing for bypassing authentication schema

Test remember password functionality

Testing for Browser cache weakness

Testing for Weak password policy

Testing for weak password change or reset functionalities

Testing for Weaker authentication in alternative channel

6. Authorization Testing

Directory traversal/file inclusion attack

Bypassing authorization schema

Privilege Escalation

Insecure Direct Object Reference

7. Session Management Testing

Testing for Bypassing Session Management Schema

Testing for Cookies Security attributes

Testing for Session Fixation Vulnerability

Testing for Exposed Session Variables

Testing for logout functionality

Test Session Timeout

Testing for Session puzzling

8. Input Validation Testing

HTTP Verb Tampering

HTTP Parameter pollution

XML Injection

SQL Injection

XPath Injection

Local File Inclusion

Remote File Inclusion

Command Injection attack

Reflected Cross Site Scripting

Stored Cross Site Scripting

HTTP Splitting/Smuggling

9. Cryptography Attacks

Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection

Collision Attack

POODLE Attack

Heart-bleed Attack

Sensitive information sent via unencrypted channels

10. Business Logic Testing

Test Business Logic Data Validation

Test Ability to Forge Requests

Test Integrity Checks

Test for Process Timing

Test Number of Times a Function Can Be Used Limits

Testing for the Circumvention of Work Flows

Upload of Unexpected File Types

Upload of Malicious Files

11. Client Side Testing

DOM based Cross Site Scripting

Testing for JavaScript Execution

HTML Injection

Client Side URL Redirect

Cross Site Flashing

Click jacking

Test Local Storage

12. Automated Vulnerability Scanning Tools

Commercial Scanners

Nessus web vulnerability scanner

Acunetix WVS

BurpSuite Pro

HP Web Inspect

Open Source/ free Scanners

Nikto , Vega, W3af , wpscan, joomscan

13. Reporting

Various Tool Reports and Manual Reporting

Risk Analysis, CVSS 3.0 score system

OWASP Risk rating system

14. Mobile Application Security Testing

Android reverse engineering

Penetration Testing mobile application

15. Web Services Security Testing

SOAP Application Testing

Rest Application Testing