WEB APPLICATION SECURITY PROFESSIONAL CURRICULAM

OWASP Top 10 Attacks

A1-Injection

A2-Broken Authentication and Session Management

A3-Cross-Site Scripting (XSS)

A4-Insecure Direct Object References

A5-Security Misconfiguration

A6-Sensitive Data Exposure

A7-Missing Function Level Access Control

A8-Cross-Site Request Forgery (CSRF)

A9-Using Components with Known Vulnerabilities

A10-Unvalidated Redirects and Forwards

1. INTRODUCTION

Networking Basics

IP addressing, Routing, Network Configurations, DNS

OSI Layer, TCP/IP, RFC

Protocols, TCP, UDP, ICMP, Ports, Port types

DNS, DHCP, SMTP, POP3, IMAP, HTTP, HTTPS, FTP

Operating System

Windows OS and commands

Linux OS installation and commands

Virtual machines- VMWare/Virtual Box Basics

Cloud Concepts

Public, Private, Community Cloud, SaaS, PaaS, IaaS

Web Technologies Basics

Client Side Technologies: HTML, HTML5, JavaScript, VB Script

Server Side Technologies: Java, .Net, PHP, Python

Backend Technologies: MySQL, MS SQL, Oracle, SQLite

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, 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

Fingerprint Web Server

Review Webserver Metafiles for Information Leakage

Enumerate Applications on Webserver

Review Webpage Comments and Metadata for Information Leakage

Identify application entry points

Fingerprint Web Application Framework

Fingerprint Web Application

3. Configuration and Deployment Management Testing

Test Network/Infrastructure Configuration

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 security question/answer

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 References

7. Session Management Testing

Testing for Bypassing Session Management Schema

Testing for Cookies attributes testing for Session

Fixation

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

SSI Injection

XPath Injection

IMAP/SMTP Injection

Local File Inclusion

Remote File Inclusion

Command Injection attack

Reflected Cross Site Scripting

Stored Cross Site Scripting

HTTP Splitting/Smuggling

Testing for incubated vulnerabilities

Testing for Code Injection

Testing for HTTP Incoming Requests

9. Testing for Error Handling

Analysis of Error Codes

Analysis of Stack Traces

10. Cryptography Attacks

Weak SSL/TLS Ciphers, Insufficient Transport Layer Protection

Collison Attack

POODLE Attack

Heartbleed Attack

Sensitive information sent via unencrypted channels

11. 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 Test

Defenses Against Application Mis -use

Upload of Unexpected File Types

Upload of Malicious Files

12. Client Side Testing

DOM based Cross Site Scripting

Testing for JavaScript Execution

HTML Injection

Client Side URL Redirect

CSS Injection

Client Side Resource Manipulation

Cross Origin Resource Sharing

Cross Site Flashing

Clickjacking

Testing Web Sockets

Test Web Messaging

Test Local Storage

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 Architecture

IOS Architecture

Rooting/Jail Breaking

Reverse Engineering Apps

Security Testing with Proxy