SECURITY TESTING TRAINING TOPICS

1. Web Application Security Testing (Hands-on Training)

- Introduction to Security Testing and its importance
- Basic concepts of Security Testing

    - ✓ CIA Triad
    - ✓ HTTP Methods
    - ✓ HTTP Response Code
    - ✓ Http Headers
    - ✓ Cookie VS Session
    - ✓ Cryptography- Encryption, Encoding, Hashing
    - ✓ Symmetric key algorithm
    - ✓ Asymmetric key algorithm
    - ✓ Input Validation
    - ✓ Output encoding
    - ✓ Black List Validation
    - ✓ Whitelist Validation
    - ✓ Client site Validation
    - ✓ Server Side Validation

- SDLC and Threat Modelling
- Security Testing process/Methodology
- SSL Handshaking Process
- SSL VS TLS
- SSL/TLS Version
- OWASP 2013-2017 Vulnerabilities

    - ✓ SQL Injection
    - ✓ Cross Site Scripting
    - ✓ Cross Site Request Forgery
    - ✓ Insecure Direct Object Reference
    - ✓ Failure to restrict URL Access
    - ✓ Security Misconfiguration
    - ✓ Unvalidated redirects and forwards
    - ✓ Broken Authentication and session management
    - ✓ Using components with knows vulnerabilities
    - ✓ Sensitive data exposure
    - ✓ Xml External Entity
    - ✓ Insecure Logging and Storage
    - ✓ Insecure Communication
    - ✓ Vulnerable SSL/TLS Versions

- Authentication related tests

    - ✓ Credentials transport over an encrypted channel/Insecure Communication
    - ✓ Testing for user enumeration
    - ✓ Default or guessable (dictionary) user account
    - ✓ Testing for Brute Force
    - ✓ Testing for Bypassing authentication schema
    - ✓ Testing for Vulnerable remember password and pwd reset
    - ✓ Testing for Logout and Browser Cache Management
    - ✓ Testing for CAPTCHA
    - ✓ Insufficient Password Policy
    - ✓ Insufficient Password change Policy
    - ✓ Password Stored in Plane test
    - ✓ Password History

- Authorization related tests

    - ✓ Path Traversals
    - ✓ Bypassing Authorization schema
    - ✓ Privilege Escalation

- Session Management Testing

    - ✓ Session Hijacking
    - ✓ Session Fixation
    - ✓ Session Timeout
    - ✓ Session replay
    - ✓ Session Invalidation
    - ✓ Exposed Session Variables

- Configuration related tests

    - ✓ Missing Http Only and Secure Flags
    - ✓ Clickjacking
    - ✓ HTTP Strict transport Security Header
    - ✓ Unsafe CORS Policy- HTML5
    - ✓ Cookie Scoped to parent domain
    - ✓ Improper error message

- Malicious File Upload
- Introduction to various Vulnerability Scanners
- Scanning application using BurpSuite and False positive elimination
- Bypassing client-Side Validations
- Risk Rating and Report preparation

2. Mobile Security Testing (Hands-on Training) - All the web application related test followed by the below:

- Jail breaking/Rooting
- Creating Virtual Devices
- Installing the APK/IPA file
- Decompiling the file
- SSH the device
- Local data storage for information leakage
- Intercepting the request using BurpSuite
- Reverse Engineering

3. Network Security Testing (Hands-on Training)

- Basic Concepts of Networking

    - ✓ OSI Layers
    - ✓ TCP VS UDP
    - ✓ What is an IP
    - ✓ IP Address Classes
    - ✓ IP V4 VS IP V6
    - ✓ Different Ports
    - ✓ Different Protocols
    - ✓ Hubs, Switches, Routers
    - ✓ Firewalls
    - ✓ DMZ

- Network Security Testing Methodology
- Scanning a network using Nessus
- Scanning and evidence gathering using Nmap
- Internal Vs External Network Security Testing
- Report Preparation

Tools Covered:

1. Web Application Security Testing:

- ✓ BurpSuite
- ✓ Acunetix
- ✓ Sslyze,
- ✓ Sqlmap

2. Network security Testing:

- ✓ Nmap
- ✓ Nessus

- ✓ SSLscan
- ✓ Sslyze

3. Mobile Security Testing:

- ✓ GenyMotion
- ✓ ADT Bundle
