Web and Mobile Application Security

Duration: 5 Days

1: Foundations of Web and Mobile Application Security

- Introduction to Web and Mobile Security
- Importance of securing applications in today's digital landscape.
- Common attack surfaces and security challenges.

- Understanding OWASP Top 10 Vulnerabilities (Web Applications)
- Injection flaws (e.g., SQL Injection).
- Broken Authentication and Session Management.
- Cross-Site Scripting (XSS).
- Insecure Direct Object References.
- Security Misconfigurations.
- Sensitive Data Exposure.
- Missing Function Level Access Control.
- Cross-Site Request Forgery (CSRF).

- Using Components with Known Vulnerabilities.
- Insufficient Logging and Monitoring.

- Setting Up the Security Environment
- Tools and configurations needed for web security testing.

2: Web Application Testing and Vulnerability Analysis

- Web Application Architecture and Threat Modelling

- Overview of web app components (Frontend, Backend, APIs).
- Identifying and prioritizing threats.
- Testing Methodologies and Tools

- Static and Dynamic Analysis Tools (e.g., Burp Suite, OWASP ZAP).
- Manual testing strategies.
- Authentication, Authorization, and Session Security Testing • Common vulnerabilities in login systems and session handling.

- Hands-On Labs
- Conducting vulnerability scans using Burp Suite and OWASP ZAP.

3: Mobile Application Security (Without Lab)

- Understanding OWASP Top 10 Mobile Risks
- Improper Platform Usage.

- Insecure Data Storage.
- Insecure Communication.
- Insecure Authentication.
- Insufficient Cryptography.
- Insecure Authorization.
- Client Code Quality Issues.
- Code Tampering.
- Reverse Engineering.
- Extraneous Functionality.

- Introduction to Mobile Application Testing Frameworks
- Mobile Application Vulnerability Identification
- Identifying risks in mobile apps based on OWASP guidelines.

4: Advanced Application Security Concepts

- Secure Software Development Lifecycle (SDLC)
- Integrating security into the SDLC.
- Automated security testing in CI/CD pipelines. • Tools and Techniques for Secure Development
- Secure coding practices and vulnerability remediation techniques.

5: Incident Handling and Best Practices

- Incident Detection and Response for Web and Mobile Applications
- Identifying security incidents.
- Steps to respond to and recover from attacks.
- Security Best Practices for Web and Mobile Applications
- Checklist for securing web and mobile apps.