📘 SEC542: Web Application Penetration Testing and Ethical Hacking

Duration: 6 Days | **8 Hours per Day**

Day 1 – Web Application Pentesting Fundamentals

- Web technologies and architectures
- HTTP/S fundamentals and request flows
- Penetration testing standards and methodologies
- Web application attack surface identification
- Reconnaissance and enumeration techniques
- Pentesting toolchain overview

Hands-On Labs

- Lab: Manual web application reconnaissance
- Lab: Application mapping and attack surface discovery
- Lab: Tool-assisted reconnaissance

Day 2 – Authentication, Session & Access Control Attacks

- Authentication design flaws
- Credential attacks and brute forcing
- Session management weaknesses
- Session hijacking and fixation
- Broken access control vulnerabilities

Hands-On Labs

- Lab: Exploit broken authentication
- Lab: Session hijacking and token analysis
- Lab: Privilege escalation via access control flaws

Day 3 – Injection & Input-Based Attacks

- SQL Injection (error-based, union, blind)
- Command injection
- Cross-site scripting (stored, reflected, DOM)
- File upload and file inclusion vulnerabilities

Hands-On Labs

- Lab: Exploit SQL injection vulnerabilities
- Lab: Perform stored and reflected XSS
- Lab: Exploit file upload flaws

Day 4 – Advanced Web Application Attacks

- Cross-Site Request Forgery (CSRF)
- Business logic vulnerabilities
- Insecure deserialization
- Web services and API exploitation

Hands-On Labs

- Lab: CSRF exploitation
- Lab: Abuse business logic flaws
- Lab: Exploit insecure deserialization
- Lab: Web API vulnerability testing

Day 5 – Exploitation, Chaining & Post-Exploitation

- Vulnerability chaining techniques
- Privilege escalation paths
- Sensitive data access and exfiltration
- Web shells and persistence
- Bypassing security controls

Hands-On Labs

- Lab: Chain multiple vulnerabilities

- Lab: Escalate privileges post-exploitation
- Lab: Deploy and interact with web shells

Day 6 – Reporting, Defense & Final Challenge

- Professional penetration testing reporting
- Risk scoring and business impact
- Remediation guidance and secure coding practices
- Defensive strategies and mitigation controls
- End-to-end pentesting workflow review

Hands-On Labs

- Lab: Create professional pentest report
- Lab: Map findings to remediation actions
- Final Challenge Lab: Full web application penetration test