SSDLC Training — How-To Guide

How to Scope and Execute a Penetration Test

From scoping through findings and remediation

Step 1: Define Scope

Clearly document what's in and out of scope:

- Target systems: URLs, IP ranges, API endpoints, mobile apps
- Test type: black box (no info), gray box (partial), white box (full access)
- Excluded systems: production databases, third-party services, specific IPs
- Time window: business hours only vs. 24/7, duration
- Rules of engagement: DoS testing allowed? Social engineering? Physical?

Step 2: Execute Using PTES Methodology

Follow the seven phases of the Penetration Testing Execution Standard:

- 1. Pre-engagement: scope, rules, emergency contacts
- 2. Intelligence gathering: OSINT, DNS, service enumeration
- 3. Threat modeling: identify high-value targets and attack vectors
- 4. Vulnerability analysis: automated scanning + manual testing
- 5. Exploitation: attempt to exploit identified vulnerabilities
- 6. Post-exploitation: assess impact, lateral movement, data access
- 7. Reporting: findings, evidence, risk ratings, remediation guidance

Step 3: Remediation Workflow

After receiving the report, triage and remediate:

- Critical/High: remediate within 7/30 days respectively
- Retest: schedule verification test after remediation
- Track findings to closure in vulnerability management system
- Share lessons learned with development teams (anonymized)