# Penetration Testing Approach & Governance

## 1. Purpose

To define the process for planning, executing, and remediating penetration testing activities for customer-facing products, ensuring vulnerabilities are identified and mitigated before release.

## 2. Scope

This approach applies to:

- Web UI applications

- APIs supporting customer-facing functionality

- Supporting backend components required for functional validation

Internal-only tools are out of scope unless designated by the Security Team.

## 3. Roles & Responsibilities

• Product Owner: Initiates pen test request, prioritizes remediation, validates fixes

• Engineering: Remediates findings and supports retest

• Security Team: Coordinates testing, validates scope, reviews findings, governs remediation

• Authorized External Penetration Testing Vendor: Performs assessment and delivers report

## 4. Testing Trigger Points in the SDLC

Penetration testing must be performed at the following milestones:

- Pre-Release: Major feature launches or architectural changes affecting customers

- Annually: Minimum cadence for all customer-facing applications

- On-Demand: High-risk changes or incidents

Security Team must approve the readiness of environments prior to testing.

## 5. Testing Approach

Testing will cover, at minimum:

- OWASP Top 10 for Web Applications

- OWASP API Security Top 10

- Authentication, authorization, session management

- Business logic abuse scenarios

- System misconfigurations

- Data exposure and encryption controls

Testing includes both manual exploitation and automated scanning tools.

## 6. Findings Review & Risk Rating

All findings are risk-rated based on likelihood and impact, aligned with:

- OWASP Risk Rating Methodology

- NIST 800-53 considerations where applicable

## 7. Remediation & Release Governance

Severity | Required Action | Blocking for Production?

Critical | Must be fixed and retested prior to go-live | Yes

High | Must be fixed and retested prior to go-live | Yes

Medium | Must have documented remediation plan | No

Low | Address in backlog grooming | No

Remediation SLAs:

- Critical: < 15 days

- High: < 30 days

- Medium: < 90 days

- Low: < 180 days

## 8. Documentation & Evidence

The following must be retained:

- Final pen test report

- Vulnerability remediation record/tracker

- Retest confirmation

- Security sign-off for release

## 9. Continuous Improvement

Security Team reviews pen test results annually to:

- Update testing scope

- Improve controls and coding guidelines

- Adjust severity SLAs based on real-world threats