

Application Penetration Testing FAQ for AIQ

Recommended guidance

Application penetration testing content must stay within approved scope and customer authorization. Use AIQ and Scenario Editor terminology for current workflows, and avoid documenting steps that could be interpreted as bypassing security controls outside an approved test.

Common questions

- **Can AIQ automate security checks?** Yes, when the checks are approved, repeatable, and safe for the target environment.
- **Can production systems be tested?** Only with explicit written authorization, controls, and an agreed test window.
- **Can real credentials or customer data be used?** Avoid them; use dedicated test accounts and masked/non-production data.
- **What evidence should be captured?** Capture results, logs, screenshots, and timestamps without exposing secrets.

Escalation checklist

1. Confirm scope, owner, target, environment, and allowed techniques.
2. Coordinate with security monitoring teams before execution.
3. Review findings with approved stakeholders only.
4. Document risks, remediation, and retest expectations.

Last updated: October 6, 2026

Revision #3

Created 2026-07-31 15:09:43 UTC by Admin

Updated 2026-10-07 04:10:39 UTC by mmora