

Create an Application Penetration Scenario in Scenario Editor

Recommended guidance

Create application penetration scenarios only in approved test environments and with explicit customer authorization. Use Scenario Editor terminology for current AIQ workflows; keep “Designer Script” only when maintaining older assets or historical file names.

Before creating the scenario

- Confirm written scope, target application, environment, accounts, data, and allowed test windows.
- Define which checks are safe to automate and which require manual security review.
- Use dedicated test accounts and non-production data.
- Coordinate with monitoring, security, and application owners to prevent false incidents.

Scenario guidance

1. Start with a controlled login and navigation path.
2. Add assertions that prove expected application behavior and safe failure handling.
3. Record evidence without exposing secrets, personal data, or exploit details beyond the approved audience.
4. Review results with security stakeholders before sharing externally.

Last updated: October 6, 2026

Revision #3

Created 2026-07-31 15:09:42 UTC by Admin

Updated 2026-10-06 13:26:19 UTC by mmora