Software, APIs and supply chain

Manage object authorization, dependencies and release provenance in one product trail.

Printable workpaper. The detailed guide and all scenario branches are in the Markdown file.

Authorized test environments and synthetic accounts only. This pack is not a conformity assessment or an attack target.

Process and expected evidence

1. Map data and objects

Authorization matrix and negative test

2. Trace dependencies

Release-bound component inventory

3. Connect build and delivery

Build trail and verified digest

4. Verify remediation and acceptance

Release-specific retest

Work record

Scope / date:
Business / technical owner:
Decision and rationale:
Evidence reference / retest:

Example and closure

Fictional example; not evidence of actual work.

Release: demo-1.2

Object / action: Report export

Tenant: A → B

Expected: Reject

Observed: Test pending

Ticket / test: Fictional APP-018

Closure checklist

[ ] Negative authorization tests exist.

[ ] SBOM bound to release.

[ ] Delivered artifact provenance verified.

[ ] Correction tested in the same scope.

Official sources

OWASP API Security Top 10 — 2023

https://api-security.owasp.org/editions/2023/en/0x03-introduction/

NIST SP 800-161 Rev. 1, November 2024 update

https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

European Commission — Cyber Resilience Act

https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act