Vulnerability lifecycle

Connect scan findings to risk, remediation and a same-scope retest.

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

Authorized organizational assets and permitted validation. Live exploitation or unauthorized access attempts are not recommended.

Process and expected evidence

1. Validate the finding

Asset-bound validation

2. Prioritize business impact

Justified priority and owner

3. Manage the change

Change or time-bound exception

4. Retest the same scope

Retest and closure rationale

Work record

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

Example and closure

Fictional example; not evidence of actual work.

Asset: TEST-WEB-01

Finding: Fictional version finding

Business impact: Customer portal

Priority rationale: Exposure + critical service

Owner / action: Application owner / patch

Retest: Same permission and scope pending

Closure checklist

[ ] Asset and test authorization verified.

[ ] Business priority justified beyond score.

[ ] Exceptions have owners and expiry.

[ ] Closure tested in the same scope.

Official sources

CISA — Known Exploited Vulnerabilities Catalog

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

NIST Cybersecurity Framework 2.0

https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final