

Vulnerability Report Template

Write findings that are clear, scoped, and defensible.

North Star Security

Use this template when turning a scanner result, manual finding, or lab discovery into a useful vulnerability report.

1. Finding summary

Finding title:

Affected asset/system:

Environment/scope:

Severity: Low / Medium / High / Critical

Status: New / Validated / Remediated / Retested / Accepted Risk

2. Plain-English summary

Write 2-4 sentences that explain:

- What is the issue?
- Where was it found?
- Why does it matter?
- What should happen next?

3. Evidence

- Screenshot/export:
- Command or tool output:
- Version/build/configuration observed:
- CVE/reference if applicable:
- Date captured:
- Validation notes:

4. Technical detail

Describe what was found and how it was identified. Keep tool output separate from your explanation.

5. Impact

Explain what could happen if the issue is exploited or left unresolved. Tie impact to actual scope and exposure.

6. Recommendation

- Primary remediation:
- Compensating control if remediation is delayed:

Vulnerability Report Template

Write findings that are clear, scoped, and defensible.

- Suggested owner:
- Suggested priority:
- Retest method:

7. Retest notes

Retest date:

Retest result: Pass / Fail / Partial

Evidence captured:

Remaining gap:

Better finding formula

- > [Asset] has [issue], confirmed by [evidence]. This matters because [impact].
- > Recommended action is [specific remediation], followed by [retest/evidence].