

BUYER'S GUIDE

How to Read a Penetration Test Report

A good report is written to be acted on. Here's what each part means, how to prioritise, and the questions to bring to your debrief.

The sections you'll see

- **Executive summary** — overall risk and themes, for leadership. Two pages, no jargon.
- **Scope & methodology** — what was tested, how, and what wasn't.
- **Findings** — each with severity, affected component, evidence, reproduction and a fix.
- **Remediation plan** — findings ranked by real risk, not just raw CVSS.
- **Retest results** — written confirmation of what's been fixed.

How to prioritise

Severity is a starting point, not the answer. A “medium” on your payment flow can matter more than a “high” on an internal tool. Combine the finding's severity with the value of what it exposes and how reachable it is.

- ✓ Fix anything that leads to account or data compromise first.
- ✓ Group findings by root cause — one fix often closes several.
- ✓ Track remediation and schedule the retest.
- ✓ Keep the report; your auditor and customers may ask for it.

Questions for your debrief

- What's the single most important thing to fix this week?
- Which findings are chained — and does fixing one break the chain?
- What would stop these issues recurring, not just this instance?
- What did you not have time to test that we should scope next?

From PXL Security. Every report we deliver includes a live debrief and a free retest. See a sample at pxlsec.com/sample-report.