

BUYER'S GUIDE

Penetration Testing Buyer's Checklist

Not all “penetration tests” are equal. Many are a vulnerability scan with a cover page. Use this checklist when choosing a provider — the answers separate real testing from scanner output.

Before you buy — ask the provider

- ✓ Who performs the testing, and what hands-on certifications do they hold?
- ✓ Can I see an anonymised sample report?
- ✓ Will you find business-logic and access-control flaws, not just known CVEs?
- ✓ How many days of manual testing are included?
- ✓ Is a remediation retest included at no extra cost?
- ✓ How do you scope, and is the price fixed before work starts?
- ✓ How are critical findings communicated during the test?
- ✓ Can you map findings to our framework (ISO 27001, SOC 2, PCI DSS, DORA, NIS2)?

Red flags

- A quote based only on the number of IPs or URLs, with no conversation about goals.
- No named tester — the work is “assigned to the team.”
- A report that's a severity table with no reproduction steps or business impact.
- No retest, or a retest sold as an expensive add-on.
- Vague answers about business-logic or access-control testing.

Green flags

- ✓ Senior, named testers with practical certifications (OSCP, OSWE, CRT0, CREST...).
- ✓ A sample report with chained findings, evidence and concrete fixes.
- ✓ A fixed scope and price, agreed in writing, with a retest included.
- ✓ Clear rules of engagement and same-day reporting of critical issues.

This checklist is from PXL Security — an independent offensive-security firm testing since 2014. Questions? Email hello@pxlsec.com or see pxlsec.com/methodology.