

FREE TOOL

The Pentest Vendor Evaluation Scorecard

12 questions that separate real pentesters from scanner operators

Use this scorecard when evaluating any penetration testing provider. Score each answer, total the points, and know within one call whether you are talking to a partner or a report printer.

The 12 questions (1 to 6)

Ask every vendor the same questions. Score: 2 for a strong answer, 1 for partial, 0 for a red flag.

Q1. Who actually performs the test?

+ **Strong:** Named senior researchers with years of offensive experience, not rotating junior analysts.

! **Red flag:** "Our team" with no names, or a platform where you never meet the tester.

Q2. Is the testing manual, automated, or hybrid?

+ **Strong:** Human-led testing, optionally accelerated by proprietary tooling, with a clear explanation of what the human layer adds.

! **Red flag:** "Our AI scans everything" with no human exploitation step.

Q3. Do you chain vulnerabilities to prove real impact?

+ **Strong:** Yes. We demonstrate attack paths, not isolated findings. A medium bug chained with another can be critical.

! **Red flag:** Findings delivered as a scanner-style list, severity copied from CVSS without context.

Q4. Can we see a sample report before signing?

+ **Strong:** Immediately, here it is.

! **Red flag:** Any hesitation. If the report is the product, a vendor confident in it shows it.

Q5. Is a retest included after we fix?

+ **Strong:** Yes, a free retest round is included. A pentest is not done until fixes are verified.

! **Red flag:** Retests billed separately, or "you can book another engagement".

Q6. How long from kickoff to final report?

+ **Strong:** A committed number in weeks, with a defined process for deadline-driven projects (audits, enterprise deals).

! **Red flag:** "It depends" with no upper bound.

The 12 questions (7 to 12)

Ask every vendor the same questions. Score: 2 for a strong answer, 1 for partial, 0 for a red flag.

Q7. How do you map findings to compliance frameworks?

+ **Strong:** Every finding mapped to the controls of SOC 2, ISO 27001, or NIS2, so your auditor sees coverage directly.

! **Red flag:** "Compliance is on you, we just test."

Q8. Will our auditor accept your report?

+ **Strong:** Yes, and here are examples of audit firms and frameworks our reports have passed.

! **Red flag:** No track record with external auditors.

Q9. How do you handle scope changes mid-test?

+ **Strong:** Fixed scope agreed upfront, changes handled transparently with written approval.

! **Red flag:** Vague scoping that becomes surprise invoices.

Q10. What happens if you find something critical on day one?

+ **Strong:** Immediate notification, same day, with severity and mitigation guidance. You do not wait for the final report.

! **Red flag:** "Everything is delivered in the final report."

Q11. What support do we get after the report?

+ **Strong:** Direct access to the researchers for remediation questions and a verification retest.

! **Red flag:** The engagement ends at PDF delivery.

Q12. Can you share references from companies at our stage?

+ **Strong:** Yes, companies similar to you in size and industry.

! **Red flag:** Only logos, no referenceable customers.

How to score

For each question: 2 points for a strong answer, 1 for a partial answer, 0 for a red flag. Maximum 24.

20 to 24	Strong vendor. Move to scoping.
14 to 19	Probe deeper before signing anything.
Under 14	Walk away.

One more thing

If you are evaluating pentest vendors right now, we are happy to be scored. We built this scorecard around the standards we hold ourselves to: senior researchers, human-led testing, free retest, audit-ready reports in 2-4 weeks.

Book a 15-minute scoping call sayfer.io

About Sayfer: 300+ startups secured. Original vulnerability research, incl. CVE-2020-10831.