Beagle Security

How to outsource penetration testing: the checklist

Most organizations know they need penetration testing, but few have the internal expertise or headcount to run it consistently, and a single qualified tester is expensive to hire and hard to retain. Outsourcing solves the access problem, but only when scope, vendor selection, and deliverables are handled well. Done poorly, it produces reports that look thorough but drive no real remediation.

This checklist is a companion to our guide on how to outsource penetration testing the right way in 2026. Work through it before you sign a statement of work, or use it as your evaluation criteria when comparing vendors.

Scope and objectives

- [ ] **Define what needs testing**

  Confirm whether the engagement covers web applications, APIs, mobile apps, internal networks, or cloud, and document the business objective behind it. An annual compliance audit, a vendor review before an acquisition, and a pre production release each call for a different scope, even on the same systems.

- [ ] **Choose the right testing methodology**

  Confirm black box, gray box, or white box, aligned to your security maturity and testing goal. Black box mirrors an outside attacker with no prior knowledge, white box gives testers full access to surface deeper logic flaws, and gray box sits in between for teams that want realistic results without starting from zero.

- [ ] **Match the engagement to the scenario**

  Outsourcing fits annual compliance audits and vendor due diligence well, since third party reports satisfy most regulatory requirements. Highly sensitive data systems are usually better kept in house, and continuous CI/CD testing is better handled by an automated platform between outsourced engagements.

Vendor evaluation

- [ ] **Verify credentials and track record**

  Confirm certifications such as OSCP, CEH, GPEN, or CREST, and request sample reports plus references from past clients in your industry. A vendor unwilling to share a redacted sample report before you sign is worth treating as a warning sign, not a formality to skip.

- [ ] **Confirm compliance framework alignment**

  Confirm the vendor maps findings to PCI DSS, HIPAA, SOC 2, ISO 27001, or other relevant frameworks before the engagement starts. Standardized reporting aligned to these frameworks doubles as documented proof of due diligence for your auditors.

Data handling and legal

- [ ] **Clarify data handling terms**

  Confirm encryption in transit and at rest, a signed NDA, artifact deletion after the engagement, and any data residency requirements. Exploitation evidence such as screenshots and payloads can be sensitive in its own right, so confirm how long the vendor retains it and who can access it.

- [ ] **Review legal and insurance coverage**

  Confirm the vendor holds cyber liability insurance and meets your legal and regulatory requirements before granting system access. This matters most when testing touches production systems or customer data directly.

Budget and deliverables

- [ ] **Set a realistic budget**

  Most engagements fall between $5,000 and $25,000, with black box web application tests at the lower end and large scale infrastructure or red team engagement at the higher end. Evaluate proposals on deliverables and expertise, not price alone.

- [ ] **Define deliverables upfront**

  Ask for a sample report covering executive summary, findings, severity ratings, proof of concept, and remediation guidance before signing. A report that reads well but does not map cleanly to your compliance framework will cost you extra work later.

Reporting expectations

- [ ] **Executive summary**

  Confirm the report opens with a concise, business friendly overview of key findings and overall security posture. This is the section leadership actually reads, so it should stand on its own without requiring the technical appendix.

- [ ] **Technical findings and severity ratings**

  Confirm each vulnerability includes affected systems, potential impact, and a severity rating of critical, high, medium, or low, so your team can prioritize the most serious risks first.

- [ ] **Proof of concept**

  Confirm the report includes screenshots, payloads, or logs that demonstrate successful exploitation, not just a description of theoretical risk. This is what separates a penetration test from a vulnerability scan: a scan flags what might be exploitable, a test proves what actually is.

- [ ] **Remediation guidance**

  Confirm actionable steps are provided for each finding, ideally referencing OWASP or NIST standards rather than generic advice that does not account for your stack.

- [ ] **Attack narrative**

  Confirm whether the report describes how an attacker could chain multiple vulnerabilities together to reach greater impact, since individual low severity findings can add up to a critical path on their own.

- [ ] **Stakeholder debrief**

  Confirm an executive presentation or walkthrough session is included to explain findings and remediation priorities directly, rather than leaving stakeholders to interpret the report alone.

Retesting and ongoing validation

- [ ] **Plan for retesting**

  Confirm follow up testing is included to verify vulnerabilities are actually fixed after remediation, not just reported as closed. Factor this into your timeline, since it adds time beyond the one to three weeks a focused web application test typically takes.

- [ ] **Agree on a communication cadence**

  Set a cadence for progress updates before the project begins, so critical findings surface early instead of waiting for the final report at the end of a four to six week infrastructure engagement.

- [ ] **Decide where continuous testing fits**

  Confirm whether an annual outsourced engagement is enough, or whether CI/CD pipelines and pre production environments need testing between engagements. A test that runs once a year misses everything that changes in the months in between.

Put continuous testing into practice

Outsourcing penetration testing works best as an ongoing relationship, not a one time engagement you revisit only when an audit forces the question. Beagle Security runs agentic AI penetration tests against your web applications and APIs, including GraphQL, with business logic testing and CI/CD integration built in, so testing continues between outsourced engagements rather than stopping at the final report.

Start a 14 day free trial with Advanced plan features, no credit card required.