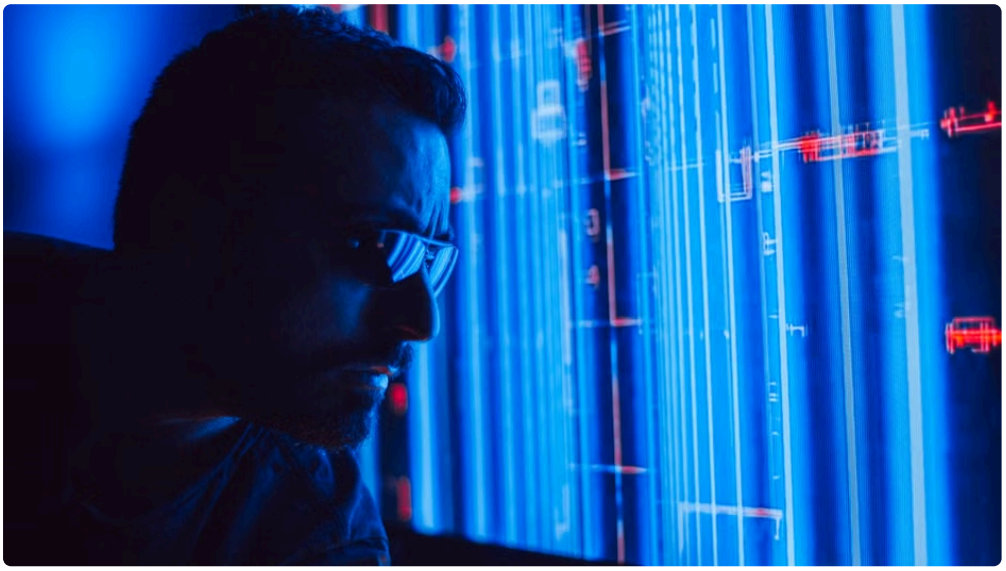
When organizations invest in a penetration test, one of the most common follow-up questions is: *do pentest companies verify fixes for free?* In other words, after vulnerabilities are found and reported, do penetration testers offer a **free retest** or vulnerability verification to confirm that remediation efforts were successful? This question goes beyond mere budgeting—it's about transparency, trust, and ensuring security investments deliver real risk reduction.

In this article, we explore the realities around pentest remediation checks and retesting, highlighting what reputable providers like **Hackeroo**, **binsec group GmbH**, and **Pentest Collective GmbH** offer in their engagements. We'll also dive into key differences between manual testing and scan-only assessments, the importance of OSCP-certified testers in your security team, and why greybox testing is often the most practical approach.



Understanding Pentest Remediation Checks and Retests

A **pentest remediation check** or **retest** refers to the follow-up process after initial vulnerabilities have been disclosed and fixes implemented by your development or operations teams. This step validates the effectiveness of

the applied patches or mitigations before a final security assessment report is closed.

Unfortunately, despite how critical this step is, the industry practice varies widely:

- Some companies include one or two rounds of retesting *for free* as part of the initial engagement.
- Others treat remediation verification as billable work, charging daily rates or fixed fees.
- There are even providers who only offer vulnerability scanning (not manual tests) and consider retests part of a separate project.

So, what should you expect from a professional pentest firm, especially when you're considering vendors like Hackeroo, binsec group GmbH, or Pentest Collective GmbH?

Transparent Pricing and Fixed-Price Quotes: What to Watch For

Pricing clarity is crucial when planning your budget for security testing and remediation verification. Some vendors publish transparent daily rates, often starting around **1.160€ per day**, with detailed pricing models that can accommodate retests within an agreed scope.

For example, Hackeroo offers clear daily rates with options to include multiple retesting phases, enabling clients to budget fixed-price engagements confidently. This contrasts sharply with vendors who provide vague pricing or sales calls that dodge technical questions, leaving clients uncertain about the true cost of retesting.

When evaluating pentest providers, ask upfront:

1. Is retesting included in the fixed price or quoted separately?
2. How many remediation verification cycles are covered?
3. Are retests performed manually, or are they automated scan-only checks?

Answers to these questions help avoid surprises and ensure your pentest budget reflects complete coverage.

Manual Pentesting vs Scan-Only Assessments: Why It Matters for Retests

Not all pentests are created equal. A scan-only assessment uses automated vulnerability scanners to identify common issues, whereas manual penetration testing combines automated tools with skilled human analysis, creativity, and exploitation techniques.

Manual testing is critical for uncovering complex vulnerability chains, misconfigurations, or business logic flaws that scanners miss. It's also essential during retesting to verify that fixes are robust and do not introduce new weaknesses.

Aspect Scan-Only Assessment Manual Penetration Testing Depth of Findings Surface-level, common vulnerabilities In-depth, complex vulnerabilities and exploit paths Retest Effectiveness May miss subtle misconfigurations Higher confidence in vulnerability verification Cost Lower Higher due to labor intensity

Companies such as binsec group GmbH and Pentest Collective GmbH emphasize manual testing as a core service. They staff OSCP-certified testers who validate vulnerabilities and retest fixes through hands-on methods, increasing your security assurance.

The Role of OSCP-Certified Testers in Retesting and Team Composition

The **Offensive Security Certified Professional (OSCP)** is a widely respected technical certification demonstrating a pentester's ability to exploit real-world vulnerabilities under strict conditions. Hiring pentest firms that deploy OSCP-certified testers means you can expect a thorough, technical approach not just in discovery but also in retesting.

Furthermore, reputable providers often leverage a team mix combining senior and junior testers. For example, Pentest Collective GmbH assembles teams where senior OSCP or even OSCE-certified professionals mentor junior testers, balancing cost efficiency with quality. This structure ensures that:

- Initial tests are comprehensive.
- Retests maintain technical rigor.
- Knowledge transfer occurs to support continuous improvement.

This depth in team composition positively impacts remediation verification—fixes are validated from multiple professional perspectives before engagement conclusion.

Greybox Testing: The Practical Default for Verification

Greybox testing offers a practical balance between blackbox (no prior knowledge) and whitebox (full disclosure) approaches. Testers receive partial access or knowledge about the system, allowing them to efficiently simulate real attacker scenarios while targeting critical assets.

During retesting, greybox methods prove advantageous since the security team usually understands system changes and can guide testers to verify applied fixes precisely.

Companies like Hackeroo advocate greybox as the default testing method, helping clients achieve optimal coverage while keeping timelines and costs manageable.

Summary: What to Expect Regarding Free Fix Verification in Pentesting

- **"Free retests" are sometimes included but often limited or conditional.** Confirm scope and coverage beforehand with your pentest provider to avoid unexpected charges.
- **Manual retesting is superior to scan-only verification.** It provides better assurance your vulnerabilities are genuinely resolved.
- **Providers with OSCP-certified testers, like binsec group GmbH and Pentest Collective GmbH, bring technical depth during remediation checks.**
- **Transparent pricing starting around 1.160€ per day** with fixed-price options, like those from Hackeroo, enable clear budgeting for initial and retest phases.
- **Greybox testing is often the most effective approach** to verify fixes pragmatically in complex environments.

Final Thoughts

In summary, the answer to "do pentest companies verify fixes for free?" is: *it depends*. Many top-tier vendors include at least one remediation verification cycle within a well-defined scope as part of the overall engagement fee. However, extensive retesting cycles or unplanned verification usually incur additional fees.

Your best bet is to engage pentest firms with transparent pricing and proven methodologies—such as Hackeroo, binsec group GmbH, or Pentest Collective GmbH—who staff OSCP-certified testers and employ manual, hackeroo

greybox testing approaches. That way, you ensure your pentest is not just a checklist exercise but a thorough security validation with reliable vulnerability verification and real risk reduction.