Releasing a product is an exciting milestone—but before API penetration testing company going live, ensuring your application's security is crucial. Conducting a thorough **web app pentest** and **API pentest** can identify vulnerabilities that might otherwise lead to costly breaches or reputational damage. However, deciding *what to test first* requires strategy, balance, and clear communication with your security provider.

Drawing insights from leading pentest firms like **Hackeroo**, **binsec group GmbH**, and **Pentest Collective GmbH**, this article will walk you through how to prioritize your pentest scope, why transparent pricing matters, the importance of manual testing by OSCP-certified experts, and why a greybox approach is often the optimal starting point.

Why Prioritize Critical Paths in Your Pentest?

When preparing for a pentest ahead of your product launch, one common question is:

In one sentence, what scope best represents your business-critical functionality?

Focusing your scope in a single, concise sentence helps ensure the pentesters target the areas that matter most. Typically, the priority is the functionality that directly impacts your users' core workflows—your **critical paths**. Testing these pathways first maximizes risk reduction.

Examples of Critical Paths

- User authentication and session management
- Payment processing or transaction workflows
- API endpoints responsible for data input and retrieval
- Admin interfaces with elevated privileges

These areas often attract attackers because they control sensitive data or core features. Concentrating testing efforts here during a **web app pentest** or **API pentest** yields the highest value.

Manual Pentesting vs Scan-only Assessments

You might have heard promises of “penetration tests” that are really just automated scans. It’s important to call this out because scanning tools alone don’t find complex logic flaws, chained attack paths, or nuanced privilege escalations.

While automated scanners are valuable for coverage, a thorough manual pentest by skilled experts is essential to uncover subtle vulnerabilities. Leading providers like **Hackeroo** and **binsec group GmbH** emphasize manual testing led by human judgment.

What Manual Testing Brings to the Table

- Creative exploitation of business logic flaws
- Customized attack chains across APIs and web interfaces
- Verification of scan results to eliminate false positives
- Insightful recommendations tailored to your architecture

Don’t settle for scan-only “pentests” under the guise of manual assessments—they are far less reliable and might miss critical issues that surface post-release.

OSCP-Certified Testers: Why Specialist Expertise Matters

One of the strongest indicators of a pentest team’s capability is recognized certifications. The **Offensive Security Certified Professional (OSCP)** is widely regarded as a gold standard for practical penetration testing skills.

Important to note is team composition:

- **Senior testers** with OSCP or higher certifications guide the scope, methodology, and delivery of findings.
- **Junior testers** supporting the team help ensure expansive coverage and assist with repetitive tasks under senior oversight.

Companies like **Pentest Collective GmbH** leverage experienced senior OSCP holders alongside well-trained junior staff to provide balanced, thorough audits. This approach blends expertise with efficiency—resulting in higher quality outcomes and actionable recommendations for your release.

Transparent Pricing and Fixed-Price Quotes

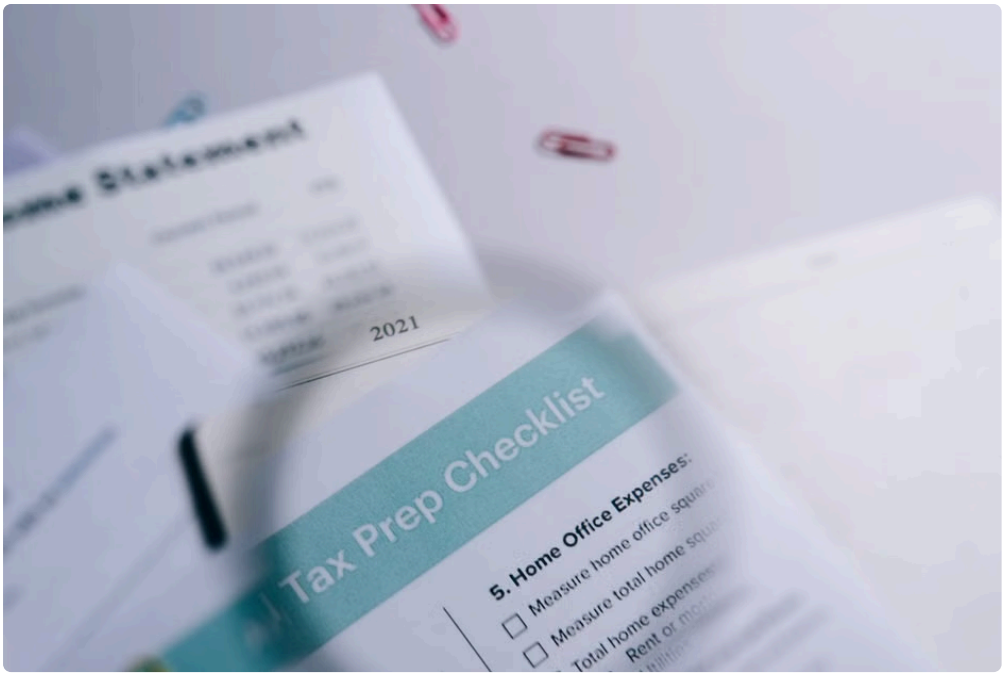
Nothing frustrates teams more than vague pricing during pentest negotiations. Thankfully, more providers now offer **transparent pricing** and fixed-price quotes that help you budget confidently.

Provider Service Pricing Example Hackeroo Web app + API pentest (manual) Daily rate starts at 1.160€ per day binsec group GmbH Greybox pentesting Fixed-price quotes based on scope Pentest Collective GmbH Comprehensive manual pentest Transparent daily rates and bundle offers

Be sure to request fixed-price quotes rather than time-and-materials estimates that can balloon unexpectedly. A clear scope paired with upfront pricing avoids last-minute surprises that can derail your release timeline.

Why Greybox Testing is the Practical Default

There are three main testing approaches:



1. **Blackbox:** Testers have no prior knowledge—simulating external attackers.
2. **Whitebox:** Full access to source code and design docs—maximizes coverage but most resource-intensive.
3. **Greybox:** Partial knowledge provided—access to API documentation, user credentials, and architecture details.

For product release pentests, **greybox testing** is typically the most efficient and effective. It allows pentesters to focus on **prioritized critical paths** with enough insider info to discover logic flaws, without drowning in source code review.

Providers like **binsec group GmbH** often recommend greybox engagements because they balance realistic attack scenarios with efficient use of pentest time.

Summary: How to Approach Pentest Prioritization Before Release

- **Define your scope in one clear sentence** that focuses on the most critical user workflows.
- **Insist on manual pentesting** by OSCP-certified testers to avoid shallow scan-only assessments.
- **Request transparent, fixed-price quotes** like the 1.160€ per day starting rates from firms such as Hackeroo.
- **Utilize greybox testing** as the practical default to maximize ROI while uncovering subtle, real-world attack vectors.
- **Engage teams with senior and junior testers** for balanced coverage and expertise, following examples like Pentest Collective GmbH.

Approaching your product release pentest with these best practices maximizes security benefits while respecting budget and timelines. Partner with reputable providers who communicate clearly and focus on your critical paths, setting you up for a confident, secure launch.

If you found this guide useful, consider reaching out to experts from Hackeroo, binsec group GmbH, or Pentest Collective GmbH to discuss your tailored pentest needs—starting with defining a clear scope for your project.