# What to Expect During Your Application Penetration Test

**Client Guide – Free Resource**

Created by **BlackBox Pentesters**

**Introduction**

If you've never commissioned an application penetration test before, it can feel unclear, technical, or even disruptive.

The reality is simple: a well-run penetration test should be structured, transparent, and aligned to your business, not something that causes stress or confusion.

This guide explains exactly what happens during an application penetration test, what you need to do, and what you will get back.

**The Goal of Your Application Penetration Test**

Your test is designed to answer three key questions:

**1. Can attackers break into your application?**
**2. If they can, what could they actually do?**
**3. How do you fix it quickly and properly?**

This is about real-world risk, not just technical vulnerability lists.

**Before Testing Starts — Preparation Phase**

**What We Will Ask From You**

- Application URLs or environments to test
- Test accounts (user / admin if possible)
- Key contact for testing communications
- Any "no-go" areas or sensitive systems
- Preferred testing window (if required)

**What You Can Expect From Us**

- Clear scope confirmation

- Legal authorisation documentation
- Named tester or testing team
- Start and end dates
- Emergency stop contact process

**Client Tip:**
If something worries you, raise it early. Good testing is collaborative, not disruptive.

### During Testing — What Is Actually Happening

During testing, security specialists simulate how real attackers would target your application.

**This May Include**

- Testing login and authentication controls
- Attempting to access other users' data
- Testing APIs and backend services
- Checking file uploads and data handling
- Testing business logic (how workflows can be abused)
- Looking for ways to escalate access privileges

**What You Will Notice**

Most clients notice **nothing at all** during testing.
Testing is controlled, authorised, and designed to avoid disruption.

If something unexpected happens, you will be informed immediately.

### Will Testing Break My Application?

In normal circumstances: **No.**

Professional penetration testing:

- Avoids destructive payloads
- Avoids data corruption
- Avoids denial-of-service activity unless specifically agreed

If higher-risk testing is needed, it is always agreed in advance.

## Communication During the Test

You will always have:

- A primary contact
- Progress updates (if requested)
- Immediate notification of critical findings (if agreed)

You are never left wondering what is happening.

## After Testing, Your Report

You will receive a clear, structured report designed for both leadership and technical teams.

### Your Report Will Include

**Executive Summary**
Clear explanation of overall risk and security posture.

**Technical Findings**
Each issue explained in plain English and technical detail.

**Business Impact**
What attackers could realistically do if the issue was exploited.

**Remediation Guidance**
Practical, developer-ready fix recommendations.

**Evidence**
Proof where vulnerabilities were safely demonstrated.

## What Happens After You Receive the Report?

Good testing doesn’t end at delivery.

You can expect:

- Clarification support for developers
- Risk discussions if needed
- Retesting after fixes (if included or agreed)

The goal is not just to find problems, it’s to help you remove them properly.

### How Long Does an Application Test Take?

Typical ranges (varies by size and complexity):

| Application Size | Typical Test Duration |
|---|---|
| Small app / single API | 2–4 days |
| Medium application | 5–8 days |
| Large / complex platform | 10+ days |

### How Should We Prepare Internally?

Good preparation includes:

- Informing internal teams testing is authorised
- Ensuring test accounts are ready
- Making sure monitoring teams don’t block testing traffic unnecessarily
- Planning developer availability for post-report fixes

### Common Client Concerns (And Honest Answers)

**“Will this create lots of work for our developers?”**
→ Possibly, but it prevents far bigger work during a breach.

**“Will this expose us as insecure?”**
→ No organisation is vulnerability-free. Testing proves you are taking security seriously.

**“Can we fail a penetration test?”**
→ No. Testing is about improvement, not pass/fail.

### How This Fits Into Your Wider Security Strategy

Application penetration testing works best alongside:

- Secure development practices
- Code reviews
- Vulnerability management

- Staff security awareness
- Infrastructure testing

Security is strongest when it is layered.

**Quick Checklist — Are You Ready for an App Pentest?**

You're ready if you can:
✓ Define which applications need testing
✓ Provide test accounts
✓ Nominate a technical contact
✓ Confirm testing windows
✓ Confirm authorisation

If you can do these, you're ready to start.

**Final Message**

A penetration test should never feel like a black box exercise.

You should always:

- Understand what is happening
- Know what risks exist
- Know exactly how to fix them

That's how real security improvement happens.

**About BlackBox Pentesters**

BlackBox Pentesters is a boutique cybersecurity testing firm focused on realistic attack simulation, senior-led testing, and clear, actionable reporting.

Our mission is simple:
**Raise standards in cybersecurity testing and make real security accessible to every organisation.**