Desktop app penetration test scoping questions

These are the questions a SilentGrid consultant asks when scoping a desktop application penetration test. Answering them first makes the call shorter and the quote more accurate.

"Not sure" is a fine answer. The scoping call helps resolve unknowns.

Questions marked **Sizing** help us prepare an accurate quote.

01 Before any test

What prompted the test, and what date does the result need to meet?

Why we ask: the reason sets the depth and report format, and the date fixes the testing window and any retest.

Will testing run against production, staging or a dedicated test copy?

Why we ask: production needs tighter limits on load, data and timing. A test copy allows more thorough techniques.

When can testing run, and are there change freezes or peak periods to avoid?

Why we ask: the schedule is built around them.

Will you want fixes retested?

Why we ask: retesting is agreed at scoping, so it is scheduled and priced from the start.

02 Desktop applications

Which operating systems and versions, and how is it installed? MSI, EXE, PKG or an app store. SIZING

Why we ask: each platform is tested on its own build.

What is it written in: .NET, Java, Electron, C or C++?

Why we ask: each is decompiled and instrumented differently.

Does it talk to a server through an API, or straight to a database?

Why we ask: clients that connect directly to a database often expose credentials or queries to every user.

Does it install services or helpers that run with elevated privileges?

Why we ask: privileged components are the usual path from standard user to administrator.

Does it communicate with other processes through named pipes, local sockets, COM or XPC?

Why we ask: these channels often accept commands from any local user.

How does it update itself, and are updates signed?

Why we ask: a weak update mechanism gives code execution on every machine it is installed on.

Discuss your testing priorities

www.silentgrid.com/contact