PENETRATION TESTING OF MOBILE APPLICATIONS

With the growing mobile device market, many companies make their services and data accessible through mobile apps.

These applications may be vulnerable to various types of attacks that can lead to data leakage, as well as to unwanted code execution on devices or servers.

Our team of professional penetration testers is ready to help businesses secure their apps on iOS, Android, and Windows Mobile platforms.

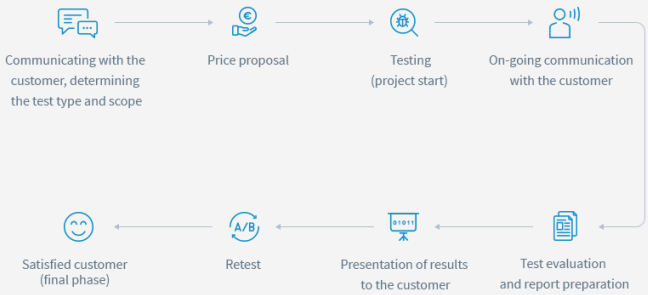
GENERAL SERVICE OVERVIEW

The purpose of the mobile app penetration test is to discover vulnerabilities in apps and their communication interfaces, demonstrate exploitation of identified vulnerabilities, identify their risk, and recommend solutions to eliminate detected vulnerabilities.

The penetration test results in a report that does not contain any "false-positive" findings, but only verified vulnerabilities.

The penetration test can be performed using the BLACK BOX (the app source code is not available), GRAY BOX (partial information about the tested app), or WHITE BOX (the source codes of the app are provided at the start of the testing).

The cost of the penetration test depends on the size and complexity of the tested application. This price is determined after customer consultation, which determines the scope, type of test, and other requirements from the customer.



DETAILED OVERVIEW OF THE SERVICE AND METHODOLOGY

Binary House uses a methodology based on OWASP Top 10 Mobile Risks with respect to current mobile platform research. If you are interested, we can customize your test according to the OWASP Mobile Security Testing Guide and the OWASP Mobile Application Security Verification Standard (ASVS) methodologies. The testing is performed using specialized tools with additional manual code review.

The testing includes a broad range of tests aimed at the locally running application, communication with the server, and testing of services on the server (REST API, SOAP, etc.). The combinantion of static and dynamic analysis with specific fuzzing techniques allows us to cover vulnerabilities from all major categories from OWASP Top 10 Mobile Risks:

- M1 - Improper Platform Usage
- M2 - Insecure Data Storage
- M3 - Insecure Communication
- M4 - Insecure Authentication
- M5 - Insufficient Cryptography
- M6 - Insecure Authorization
- M7 - Poor Code Quality
- M8 - Code Tampering
- M9 - Reverse Engineering
- M10 - Extraneous Functionality