LIQUID
CLOUD & CYBER SECURITY

Services Brief

Mobile Application Penetration Testing

Identify Mobile Threats Before Attackers Do

Mobile applications have become a primary interface for customers and employees—making them a high-value target for cyber threats. Liquid C2's Mobile Application Penetration Testing helps uncover vulnerabilities in both client-side code and backend communications, using a methodology grounded in the OWASP Mobile Application Security Testing Guide.

We assess your iOS and Android apps for insecure storage, improper session handling, misconfigurations, reverse engineering risks, and more—before attackers can exploit them. This service ensures that mobile applications meet security and compliance standards across internal or internet-facing deployments by assessing Internet-facing or internal mobile applications.

Mobile Application Penetration Testing Packages		
Silver Package	**Gold Package**	**Platinum Package**
Best for: Teams looking to assess public-facing mobile apps with minimal internal engagement.	**Best for:** Organisations needing deeper insight into authenticated flows and backend communication risks.	**Best for:** Organisations with complex mobile applications requiring deep validation and business logic risks.
Includes:	**Includes:**	**Includes:**
☑ Black Box Testing with Minimal App Information ☑ Static and Dynamic Analysis of App Binary (APK/IPA) ☑ OWASP Mobile Top 10 Coverage (Basic): Insecure Storage, Insecure Communication ☑ Tool-Based Testing with Some Manual Validation Deliverables: Executive Summary + Technical Report with Vulnerabilities Risk Rating	☑ All Features of the Silver Package ☑ Grey Box Testing Using Test Credentials (Using Single User Role) ☑ API Endpoint Testing for Misconfigurations and Auth Issues ☑ Authentication & Session Management Review ☑ OWASP Mobile Top 10 Coverage (Moderate) ☑ Manual Validation of Key Issues Detected via Automation	☑ All Features of the Gold Package ☑ Business Logic Testing (Workflow Misuse, Role Manipulation, Process Abuse) ☑ In-Depth Access Control Testing (Horizontal & Vertical Privilege Escalation) ☑ API Abuse Scenarios: Rate-Limiting Bypass, Unauthorized Access, Data Exfiltration ☑ Reverse Engineering and Custom Exploit Scenarios Based on Business Risk
Deliverables: Executive Summary + Technical Report with Vulnerabilities Risk Rating		

Why Choose Liquid C2?

Certified Security Experts (OSWE, OSCE, OSCP, OSWP, GPEN, GWAPT, CEH, CISSP, among others)
Industry-Recognised Testing Methodologies (OWASP, MITRE ATT&CK)
Customisable Testing Approach Based on Your Business Risks
Detailed Remediation Guidance to Strengthen Your Security Posture

Get Started Today!

Secure your business before cyber attackers do. Contact us for a consultation and choose the right penetration testing package for your needs.

Email: C2_info@liquid.tech | **Website:** www.liquidC2.com