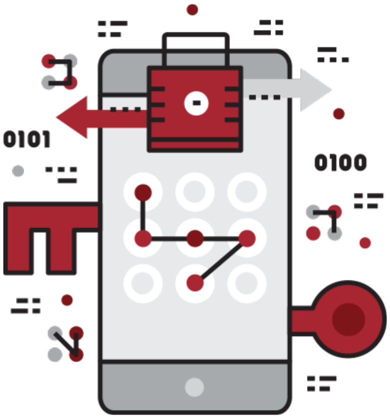
MOBILE PENETRATION TESTING

Identify Mobile App Risks

Mobile is the new standard platform for application development – from banking applications to healthcare platforms. However, managing risk on these new devices is also a growing challenge, with new app vulnerabilities found every day.

Rhino Security Labs offers best-in-class mobile security analysis, providing a risk-based approach to mobile security. With industry-leading researchers in both iOS and Android, we provide deep dive testing into localized security issues, back-end web services, and the API's which connect them.



SERVICE BENEFITS

- Identify and remediate iOS, Android, and Windows Phone application risks
- Assess and report on mobile application security to executive management and other stakeholders
- Identify critical information exposures attributed to mobile apps in your environment
- Evaluate the security posture of new mobile technologies in development

CODE REVIEW – IDENTIFY FLAWS EARLIER IN DEVELOPMENT

Penetration testing on production mobile apps offers increased awareness of current vulnerabilities and the potential damage if they are exploited. Augmenting this with regular code reviews ensures you identify bugs before they get pushed to production apps – and found by attackers.

With Rhino Security's penetration testing and detailed assessment reports, you can ensure your apps are production ready. In addition to our technical expertise, each security assessment report reveals actionable steps for patching the vulnerabilities in your mobile app.

> *" 75% of mobile applications fail basic security checks. "*
>
> **– Gartner Report**

ASSESSMENT DETAILS AND METHODOLOGY

For mobile penetration testing, we use the same tools and techniques as malicious hackers, providing detailed visibility into security vulnerabilities - without the associated business risk. Our customized methodology ensures each test is conducted safely and is focused on the unique needs of your environment. Our methodology uses the following steps:

Information gathering on target environment

1. Reconnaissance

Each assessment begins by identifying the attack surface of the app and its associated servers. We identify both how your application exposes itself to the underlying mobile platform, and how it connects to backend servers.

Identify and map vulnerabilities in app and infrastructure

2. Vulnerability Detection

Once the target has been fully enumerated, Rhino Security Labs uses both vulnerability scanning tools and manual analysis to identify security flaws. With decades of experience and custom-built tools, our security engineers find weaknesses automated tools miss.

Safe and controlled exploitation of vulnerabilities

3. Attack and Post-Exploitation

Once our security analysts have noted all potential weaknesses, focus turns to the controlled exploitation of all vulnerabilities, noting false positives and confirming the impact of positive hits. During each phase of the compromise, we keep client stakeholders informed of testing progress, ensuring asset safety and stability.

Detailed, risk-prioritized report with remediation steps

5. Assessment Reporting

Once the engagement is complete, Rhino Security Labs delivers a detailed analysis and threat report, including remediation steps. Our consultants set an industry standard for clear and concise reports, prioritizing the highest risk vulnerabilities first.

The assessment includes the following:

- Executive Summary
- Identified Vulnerabilities and Risk Ratings
- Detailed Risk Remediation Steps
- Strategic Strengths & Weaknesses

ABOUT RHINO SECURITY LABS

Rhino Security Labs is a top penetration testing and security assessment firm, with a focus on web applications, cloud/AWS, network, mobile apps and phishing testing. With manual, deep-dive engagements, we identify and demonstrate security vulnerabilities which put clients at risk.

Endorsed by industry leaders, Rhino Security Labs is a trusted security advisor to the Fortune 500.