Mobile App Security Testing | IRONSCAN

DIAGNOSE & IDENTIFY VULNERABLE POINTS IN YOUR MOBILE APPLICATION ECOSYSTEM IN PREVENTING POTENTIAL CYBERSECURITY THREATS.

Highlights

BLACK BOX TESTING	HACKER'S APPROACH	COMPREHENSIVE ASSESSMENT	DETAILED REPORTING
Upload APK/IPA file, no source code required.	Detect runtime and environment vulnerabilities, minimize false positive.	Assessment based on OWASP Mobile Top 10, CVE, CWE	Report with visual graphs, finding details and recommended solution.

Our mobile application security testing is designed and innovated to expose security vulnerabilities in smart mobile applications. We make use of various tools and techniques to check for specific weaknesses in the application that could potentially leave your application vulnerable to attacks. Apart from identifying these weak spots, we also let you know about the possible solutions to fix them in order to secure your app in the long run.

Simplified Process For Quicker Assessments

1 UPLOAD FILES FOR TESTING

IronSCAN supports multiple applications to be assessed for vulnerabilities. Simply login to the platform and upload the files required for testing.

2 BEGIN FILE SCANNING

Once uploaded, you can test the security of your app on different security checks including OWASP Top 10 vulnerabilities, Cross-Application Attacks, and more.

3 DOWNLOAD REPORT

Comprehensive summary that is easy to read and follow up for your business, with full audit log records of the analysis with details on every security test performed.

IronSCAN Simplifies The Process of Locating & Prioritizing Application Vulnerabilities

By reducing the need for manual efforts by security experts, speeding up scanning tasks and enabling auditors to better identify vulnerabilities. IronSCAN will also enable IT organizations to carry out application risk management activities including software security assessments, root cause analysis, remediation planning and validation, as well as creating custom reports to provide visibility into critical data, helping to comply with ISO 27001, NIST 800-53, PCI-DSS, GDPR and more.

business@seciron.com www.seciron.com

Thorough Inspection of Mobile Applications

Supports APK (Android) & IPA (iOS) Files

IronSCAN scans the compiled application at the end of the SDLC to identify any runtime vulnerabilities without needing the source code. By using device emulation, IronSCAN is able to test applications under various conditions. This allows for detection of malicious activity during the deployment phase of an applications lifecycle.

Multi-Threat Security Detection

By detecting critical issues and items in applications through an automated process utilizing OWASP recommended best practices and techniques, such as static code analysis and dynamic behaviour testing, IronSCAN enables organisations to reduce the time and cost of validating the security of their code.

Customisable Threat Analysis Report

Autonomous detection and reporting features that provides a full audit of your mobile application within minutes with accurate assessment results. By incorporating full customisation to reporting features, you can instantly define your own customised reports, which are then easily distributed to the team members involved.

For Android APK Files

- Self-Security Class
- Program Source File Security
- Local Data Storage Security
- Communication Data Transmission Security
- Identify Verification Security
- Internal Data Interaction Security
- HTML 5 Security
- Defense Against Malicious Attacks

For iOS IPA Files

- Self-Security Class
- Binary Code Protection
- Client Data Storage Security
- Data Transmission Security
- Encryption Algorithm & Password Security
- Program Source File Security
- iOS Application Security Specification

business@seciron.com
www.seciron.com

ATTRIBUTES	FEATURE HIGHLIGHTS		
Platform Dashboard	- Simplified UI - Self-serving console - Home page with summary of activities	- Security testing report information with statistics, timelines, and classifications. - Task Template customisation	
Easy Deployment	- Online SaaS Platform with intuitive dashboard - Upload files for security testing		
Security Testing Duration	- < 80MB file = 5 minutes - > 80MB file = 15 minutes	- Multiple file combination > 80MB = 20 minutes	
Security Checking Templates	- OWASP Mobile Top 10 Vulnerabilities - Android Full Detection - iOS Full Detection	- Static & Dynamic Tests - Customised (User selection)	
Detailed Reporting	- Simple and easy to read with charts, graphs, and statistics - Export report in selected language selection (English, Chinese, Japanese) - Preview report online - Download report in PDF, WORD - Export detected threat data by custom date range		
Automated Assessment Items	**Security Assessment** - App information - Permission - Malicious behaviour	- Sensitive Words - Virus	- Third party SDK - Advertisement SDK
	Risk Assessment - Reverse engineering of Java code - Decipher shared objects (.so) files - Tampering and repackaging - Dynamic injection attack - Screen hijacking - Key logger - Insecure transport layer protocol	- Webview security: Passwords stored in plaintext - Presenting digital certificate in plaintext - Information disclosure through log debugging - Exposure of resource files - Dynamic debugger attack - Activity component security	- Broadcast Receiver security - Unrestricted backup/restore file - Sensitive function call - Risk of dynamic debugging at java layer - Loading .dex file from SD cards - Implicit calls of Intent component - Service component security
	Vulnerability Assessment - Webview security: remote code execution - SQL injection - Content Provider data leakage - Encryption algorithm mode check	- SSL certificate validation - Unrestricted APK download through app - World readable and writable files - In device denial of service attack	- Webview security: bypass certificate validation - Random number vulnerability check - Intent scheme URL attack - Fragment injection attack - Internal network testing information

SECIRON

Over A Decade of Providing Security Solutions Across Asia

We are the industry leader in mobile application security across Asia. With over 10,000 applications across 9 countries protected using our End-to-End solutions, industries across Banking, FinTech, Insurance, Gaming & Government choose us to secure their applications across end-devices.

Get In Touch

business@seciron.com

www.seciron.com

Connect with us to know more