HORIZONSHIELD ORIGINALS · BOOK 19

Mobile Security & App Hardening

iOS, Android Security Testing & Mobile Threat Defense

iOS and Android security testing using OWASP Mobile Top 10, mobile app hardening, MDM/EMM controls, mobile threat defense, and MSTG-aligned testing methodology.

HORIZONSHIELD

TECHNICAL

Contents

CHAPTER 01

OWASP Mobile Top 10 — 2024

Mobile applications handle the most sensitive user data — biometrics, payment information, health records, and location history. The OWASP Mobile Top 10 defines the most critical mobile security risks practitioners must test for.

OWASP Mobile Top 10 — 2024 Edition

Rank	Category	Key Risk	Test Method
M1	Improper Credential Usage	Hardcoded API keys, poor credential storage	Static analysis, strings extraction
M2	Inadequate Supply Chain Security	Vulnerable third-party SDKs and libraries	SCA scan, dependency audit
M3	Insecure Authentication/Authorization	Broken biometric, weak token validation	Auth bypass testing, token manipulation
M4	Insufficient Input/Output Validation	Injection via deep links, file uploads	Fuzzing, deep link injection
M5	Insecure Communication	Cleartext traffic, certificate pinning bypass	Network proxy, SSL stripping
M6	Inadequate Privacy Controls	Excessive data collection, poor consent	Traffic analysis, storage inspection
M7	Insufficient Binary Protections	No obfuscation, debug enabled, no jailbreak detection	Reverse engineering with objection/Frida
M8	Security Misconfiguration	Debug builds, exported components, world-readable storage	APK analysis, manifest review
M9	Insecure Data Storage	Sensitive data in plaintext on device	File system inspection, backup analysis
M10	Insufficient Cryptography	Weak algorithms, static IV, custom crypto	Binary analysis, traffic inspection

CHAPTER 02

Android Security Testing

Android's open architecture makes it both flexible and complex to secure. Security testing covers the APK binary, network communications, device storage, and inter-component communication.

Android Security Testing Toolkit

```
# APK static analysis — extract and analyze
apktool d target.apk -o extracted/
# Check manifest for exported components and permissions
cat extracted/AndroidManifest.xml | grep -E "exported|permission|debug"

# String extraction — find hardcoded secrets
grep -rE "(api_key|password|secret|token)" extracted/
grep -rE "https?://" extracted/  # Hardcoded URLs

# Decompile to Java source
jadx -d jadx_output/ target.apk
# Review decompiled code for crypto, storage, network calls

# Dynamic analysis with Frida
frida -U -f com.target.app --no-pause -l bypass_ssl.js
# SSL pinning bypass scripts: https://github.com/httptoolkit/frida-interception-and-unpinning

# ADB file system inspection (rooted device/emulator)
adb shell
run-as com.target.app
ls -la /data/data/com.target.app/
cat /data/data/com.target.app/shared_prefs/*.xml  # Find stored secrets
```

>

MobSF — Mobile Security Framework: Run MobSF (open source) for automated static and dynamic analysis of Android APKs and iOS IPAs. It generates a comprehensive report covering all OWASP Mobile Top 10 categories in under 5 minutes. Install via Docker: `docker run -it -p 8000:8000 opensecurity/mobile-security-framework-mobsf`

CHAPTER 03

MDM & Enterprise Mobile Security

Enterprise mobile security requires Mobile Device Management (MDM) to enforce security policies, protect corporate data, and enable remote wipe across the organization's device fleet.

MDM vs MAM vs EMM

Solution	Scope	Best For	Examples
MDM (Mobile Device Mgmt)	Full device management	Corporate-owned devices	Intune, Jamf, VMware Workspace ONE
MAM (Mobile App Mgmt)	App-level management only	BYOD — personal devices	Intune MAM, Citrix Endpoint
EMM (Enterprise Mobility Mgmt)	MDM + MAM + identity	Large enterprises, complex fleet	VMware Workspace ONE, MobileIron
MTD (Mobile Threat Defense)	Threat detection on device	High-security environments	Lookout, Zimperium, SentinelOne

MDM Policy Baseline

- Require PIN/passcode minimum 6 digits or biometric equivalent
- Enable full-device encryption (mandatory on iOS, configurable on Android)
- Screen lock after 5 minutes of inactivity
- Remote wipe capability — test quarterly
- Block jailbroken/rooted devices from corporate resources
- Enforce OS version minimum — block devices more than 2 major versions behind
- Certificate-based Wi-Fi and VPN authentication (no shared PSK)
- App allowlist for corporate profile apps (MAM container)

CHAPTER 04

Mobile App Secure Development

Secure mobile development must address data storage, network communication, authentication, and binary protection from the earliest design stages.

Secure iOS Development Checklist

```
// INSECURE: Storing sensitive data in UserDefaults
UserDefaults.standard.set(apiKey, forKey: "api_key")

// SECURE: Use Keychain for sensitive data
import Security
let query: [String: Any] = [
    kSecClass as String: kSecClassGenericPassword,
    kSecAttrAccount as String: "api_key",
    kSecValueData as String: apiKey.data(using: .utf8)!,
    kSecAttrAccessible as String: kSecAttrAccessibleWhenUnlocked
]
SecItemAdd(query as CFDictionary, nil)

// Certificate pinning (network layer)
class PinnedURLSessionDelegate: NSObject, URLSessionDelegate {
    func urlSession(_ session: URLSession,
                    didReceive challenge: URLAuthenticationChallenge,
                    completionHandler: @escaping (URLSession.AuthChallengeDisposition,
                                                  URLCredential?) -> Void) {
        // Validate server certificate against pinned hash
        guard let serverCert = challenge.protectionSpace.serverTrust,
              certificateMatchesPinnedHash(serverCert) else {
            completionHandler(.cancelAuthenticationChallenge, nil)
            return
        }
        completionHandler(.useCredential, URLCredential(trust: serverCert))
    }
}
```

>

OWASP MASTG: The OWASP Mobile Application Security Testing Guide (MASTG) is the definitive free reference for mobile app security. Use it alongside MASVS (Mobile Application Security Verification Standard) to define your app security requirements and test coverage. Available free at mas.owasp.org.

HS

HORIZONSHIELD ORIGINALS

Complete Security Library

HorizonShield Originals are practitioner-written guides designed for real-world implementation — from SMB security foundations to advanced threat hunting, cloud architecture, and regulatory compliance.

AVAILABLE IN THIS SERIES

01 SMB Cybersecurity Guide 2026
02 Penetration Testing Checklist
03 Incident Response Playbook
04 DORA Compliance Guide
05 Cloud Security Hardening
06 Zero Trust Architecture
07 Threat Hunting SOC Operations
08 DevSecOps Implementation
09 Web Application Security
10 Network Security Fundamentals
11 Linux & Systems Security
12 Social Engineering & Human Hacking
13 Malware Analysis & Reverse Engineering
14 Digital Forensics & Incident Response
15 Applied Cryptography
16 Compliance Audit & Risk Management
17 AI & LLM Security Guide
18 OT & ICS Security
19 Mobile Security
20 Kubernetes Security
21 Bug Bounty Methodology
22 Security Architecture for Startups

horizonshield.net/library

Download all 16 books · Access labs · Track your progress

horizonshield.net