

Maintained by @vaib25vicky with contributions from the security and developer communities.

Android

General - Blogs, Papers, How To's

- Android: Gaining access to arbitrary* Content Providers
- Evernote: Universal-XSS, theft of all cookies from all sites, and more
- Interception of Android implicit intents
- TikTok: three persistent arbitrary code executions and one theft of arbitrary files
- Persistent arbitrary code execution in Android's Google Play Core Library: details, explanation and the PoC - CVE-2020-8913
- Android: Access to app protected components
- Android: arbitrary code execution via third-party package contexts
- Android Pentesting Labs - Step by Step guide for beginners
- An Android Hacking Primer
- Secure an Android Device
- Security tips
- OWASP Mobile Security Testing Guide
- Security Testing for Android Cross Platform Application
- Dive deep into Android Application Security
- Pentesting Android Apps Using Frida
- Mobile Security Testing Guide
- Mobile Application Penetration Testing Cheat Sheet
- Android Applications Reversing 101
- Android Security Guidelines
- Android WebView Vulnerabilities
- OWASP Mobile Top 10
- Practical Android Phone Forensics
- Mobile Reverse Engineering Unleashed
- Android Root Detection Bypass Using Objection and Frida Scripts
- quark-engine - An Obfuscation-Neglect Android Malware Scoring System
- Root Detection Bypass By Manual Code Manipulation.
- Application and Network Usage in Android
- GEOST BOTNET - the discovery story of a new Android banking trojan

-
- Mobile Pentesting With Frida
 - Magisk Systemless Root - Detection and Remediation
 - AndroDet: An adaptive Android obfuscation detector
 - Hands On Mobile API Security
 - Zero to Hero - Mobile Application Testing - Android Platform
 - How to use FRIDA to bruteforce Secure Startup with FDE-encryption on a Samsung G935F running Android 8
 - Android Malware Adventures
 - AAPG - Android application penetration testing guide
 - Bypassing Android Anti-Emulation
 - Bypassing Xamarin Certificate Pinning
 - Configuring Burp Suite With Android Nougat

Books

- SEI CERT Android Secure Coding Standard
- Android Security Internals
- Android Cookbook
- Android Hacker's Handbook
- Android Security Cookbook
- The Mobile Application Hacker's Handbook
- Android Malware and Analysis
- Android Security: Attacks and Defenses

Courses

- Learning-Android-Security
- Mobile Application Security and Penetration Testing
- Advanced Android Development
- Learn the art of mobile app development
- Learning Android Malware Analysis
- Android App Reverse Engineering 101
- Android Pentesting for Beginners

Tools

Static Analysis

-
- Amandroid – A Static Analysis Framework
 - Androwarn – Yet Another Static Code Analyzer
 - APK Analyzer – Static and Virtual Analysis Tool
 - APK Inspector – A Powerful GUI Tool
 - Droid Hunter – Android application vulnerability analysis and Android pentest tool
 - Error Prone – Static Analysis Tool
 - Findbugs – Find Bugs in Java Programs
 - Find Security Bugs – A SpotBugs plugin for security audits of Java web applications.
 - Flow Droid – Static Data Flow Tracker
 - Smali/Baksmali – Assembler/Disassembler for the dex format
 - Smali-CFGs – Smali Control Flow Graph's
 - SPARTA – Static Program Analysis for Reliable Trusted Apps
 - Thresher – To check heap reachability properties
 - Vector Attack Scanner – To search vulnerable points to attack
 - Gradle Static Analysis Plugin
 - Checkstyle – A tool for checking Java source code
 - PMD – An extensible multilanguage static code analyzer
 - Soot – A Java Optimization Framework
 - Android Quality Starter
 - QARK – Quick Android Review Kit
 - Infer – A Static Analysis tool for Java, C, C++ and Objective-C
 - Android Check – Static Code analysis plugin for Android Project
 - FindBugs-IDEA Static byte code analysis to look for bugs in Java code
 - APK Leaks – Scanning APK file for URIs, endpoints & secrets

Dynamic Analysis

- Adhrit - Android Security Suite for in-depth reconnaissance and static bytecode analysis based on Ghera benchmarks
- Android Hooker - Opensource project for dynamic analyses of Android applications
- AppAudit - Online tool (including an API) uses dynamic and static analysis
- AppAudit - A bare-metal analysis tool on Android devices
- CuckooDroid - Extension of Cuckoo Sandbox the Open Source software
- DroidBox - Dynamic analysis of Android applications
- Droid-FF - Android File Fuzzing Framework
- Drozer
- Marvin - Analyzes Android applications and allows tracking of an app
- Inspeckage

-
- PATDroid - Collection of tools and data structures for analyzing Android applications
 - AndroL4b - Android security virtual machine based on ubuntu-mate
 - Radare2 - Unix-like reverse engineering framework and commandline tools
 - Cutter - Free and Open Source RE Platform powered by radare2
 - ByteCodeViewer - Android APK Reverse Engineering Suite (Decompiler, Editor, Debugger)
 - Mobile-Security-Framework MobSF
 - CobraDroid - Custom build of the Android operating system geared specifically for application security
 - Magisk v20.2 - Root & Universal Systemless Interface
 - Runtime Mobile Security (RMS) - is a powerful web interface that helps you to manipulate Android and iOS Apps at Runtime
 - MOBEXLER - A Mobile Application Penetration Testing Platform

Android Online APK Analyzers

- Oversecured - A static vulnerability scanner for Android apps (APK files) containing 90+ vulnerability categories
- Android Observatory APK Scan
- Android APK Decompiler
- AndroTotal
- NVISO ApkScan
- VirusTotal
- Scan Your APK
- AVC Undroid
- OPSWAT
- ImmuniWeb Mobile App Scanner
- Ostor Lab
- Quixxi
- TraceDroid
- Visual Threat
- App Critique

Labs

- OVAA (Oversecured Vulnerable Android App)
- DIVA (Damn insecure and vulnerable App)
- SecurityShepherd
- Damn Vulnerable Hybrid Mobile App (DVHMA)

-
- OWASP-mstg
 - VulnerableAndroidAppOracle
 - Android InsecureBankv2
 - Purposefully Insecure and Vulnerable Android Application (PIIVA)
 - Sieve app
 - DodoVulnerableBank
 - Digitalbank
 - OWASP GoatDroid
 - AppKnox Vulnerable Application
 - Vulnerable Android Application
 - MoshZuk
 - Hackme Bank
 - Android Security Labs
 - Android-InsecureBankv2
 - Android-security
 - VulnDroid
 - FridaLab
 - Santoku Linux - Mobile Security VM
 - Vuldroid

Talks

- Blowing the Cover of Android Binary Fuzzing (Slides)
- One Step Ahead of Cheaters – Instrumenting Android Emulators
- Vulnerable Out of the Box: An Evaluation of Android Carrier Devices
- Rock around the clock: Tracking malware developers by Android
- Chaosdata - Ghost in the Droid: Possessing Android Applications with ParaSpectre
- Remotely Compromising Android and iOS via a Bug in Broadcom's Wi-Fi Chipsets
- Honey, I Shrunk the Attack Surface – Adventures in Android Security Hardening
- Hide Android Applications in Images
- Scary Code in the Heart of Android
- Fuzzing Android: A Recipe For Uncovering Vulnerabilities Inside System Components In Android
- Unpacking the Packed Unpacker: Reverse Engineering an Android Anti-Analysis Native Library
- Android FakeID Vulnerability Walkthrough
- Unleashing D* on Android Kernel Drivers
- The Smarts Behind Hacking Dumb Devices
- Overview of common Android app vulnerabilities
- Android Dev Summit 2019

-
- Android security architecture
 - Get the Ultimate Privilege of Android Phone

Misc.

- Android-Reports-and-Resources
- android-security-awesome
- Android Penetration Testing Courses
- Lesser-known Tools for Android Application PenTesting
- android-device-check - a set of scripts to check Android device security configuration
- apk-mitm - a CLI application that prepares Android APK files for HTTPS inspection
- Andriller - is software utility with a collection of forensic tools for smartphones
- Dexofuzzy: Android malware similarity clustering method using opcode sequence-Paper
- Chasing the Joker
- Side Channel Attacks in 4G and 5G Cellular Networks-Slides
- Shodan.io-mobile-app for Android
- Popular Android Malware 2018
- Popular Android Malware 2019
- Popular Android Malware 2020

iOS

General - Blogs, Papers, How to's

- iOS Security
- Basic iOS Apps Security Testing lab
- iOS Application security – Setting up a mobile pentesting platform
- Collection of the most common vulnerabilities found in iOS applications
- IOS_Application_Security_Testing_Cheat_Sheet
- OWASP iOS Basic Security Testing
- Dynamic analysis of iOS apps w/o Jailbreak
- iOS Application Injection
- Low-Hanging Apples: Hunting Credentials and Secrets in iOS Apps
- Checkra1n Era - series
- BFU Extraction: Forensic Analysis of Locked and Disabled iPhones
- HowTo-decrypt-Signal.sqlite-for-IOs
- Can I Jailbreak?

-
- How to Extract Screen Time Passcodes and Voice Memos from iCloud
 - Reverse Engineering Swift Apps
 - Mettle your iOS with FRIDA
 - A run-time approach for pentesting iOS applications
 - iOS Internals vol 2
 - Understanding usbmux and the iOS lockdown service
 - A Deep Dive into iOS Code Signing
 - AirDoS: remotely render any nearby iPhone or iPad unusable
 - How to access and traverse a #checkra1n jailbroken iPhone File system using SSH
 - Deep dive into iOS Exploit chains found in the wild - Project Zero
 - The Fully Remote Attack Surface of the iPhone - Project Zero

Books

- Hacking and Securing iOS Applications: Stealing Data, Hijacking Software, and How to Prevent It
- iOS Penetration Testing
- iOS App Security, Penetration Testing, and Development
- iOS Hacker's Handbook
- Hacking iOS Applications a detailed testing guide
- Develop iOS Apps (Swift)
- iOS Programming Cookbook

Courses

- Pentesting iOS Applications
- Reverse Engineering iOS Applications
- App Design and Development for iOS

Tools

- Cydia Impactor
- checkra1n jailbreak
- idb - iOS App Security Assessment Tool
- Frida
- Objection - mobile exploration toolkit by Frida
- Bfinject

-
- iFunbox
 - Libimobiledevice - library to communicate with the services of the Apple ios devices
 - iRET (iOS Reverse Engineering Toolkit) - includes oTool, dumpDecrypted, SQLite, Theos, Key-chain_dumper, Plutil
 - Myriam iOS
 - iWep Pro - wireless suite of useful applications used to turn your iOS device into a wireless network diagnostic tool
 - Burp Suite
 - Cycrypt
 - needle - The iOS Security Testing Framework
 - iLEAPP - iOS Logs, Events, And Preferences Parser
 - Cutter - Free and Open Source RE Platform powered by radare2
 - decrypt0r - automatically download and decrypt SecureRom stuff
 - iOS Security Suite - an advanced and easy-to-use platform security & anti-tampering library

Labs

- OWASP iGoat
- Damn Vulnerable iOS App (DVIA) v2
- Damn Vulnerable iOS App (DVIA) v1
- iPhoneLabs
- iOS-Attack-Defense

Talks

- Behind the Scenes of iOS Security
- Modern iOS Application Security
- Demystifying the Secure Enclave Processor
- HackPac Hacking Pointer Authentication in iOS User Space
- Analyzing and Attacking Apple Kernel Drivers
- Remotely Compromising iOS via Wi-Fi and Escaping the Sandbox
- Reverse Engineering iOS Mobile Apps
- iOS 10 Kernel Heap Revisited
- KTRW: The journey to build a debuggable iPhone
- The One Weird Trick SecureROM Hates
- Tales of old: untethering iOS 11-Spoiler: Apple is bad at patching
- Messenger Hacking: Remotely Compromising an iPhone through iMessage

-
- Recreating An iOS 0-Day Jailbreak Out Of Apple's Security Updates
 - Reverse Engineering the iOS Simulator's SpringBoard
 - Attacking iPhone XS Max

Misc.

- Most usable tools for iOS penetration testing
- iOS-Security-Guides
- osx-security-awesome - OSX and iOS related security tools

- Trust in Apple's Secret Garden: Exploring & Reversing Apple's Continuity Protocol-Slides
- Apple Platform Security
- Mobile security, forensics & malware analysis with Santoku Linux