
awesome-mobile-CTF

This is a curated list of mobile based CTFs, write-ups and vulnerable mobile apps. Most of them are android based due to the popularity of the platform.

Inspired by android-security-awesome, osx-and-ios-security-awesome and all the other awesome security lists on @github.

Mobile CTF challenges

- Google CTF 2021
- Google CTF 2020 writeup 1, writeup 2
- HacktivityCon CTF Mobile 2020
- Trend Micro CTF 2020
- KGB Messenger
- ASIS CTF — ShareL Walkthrough
- Android reversing challenges
- Android app for IOT CTF
- CyberTruck Challenge 2019 (Detroit USA)
- Matryoshka-style Android reversing challenge
- Cybertruckchallenge19
- You Shall Not Pass - BSides Canberra 2019
- Mobile challenges collection
- BSidesSF 2018 CTF
- h1-702-2018-ctf-wu
- THC CTF 2018 - Reverse - Android serial
- Android crack me challenges
- OWASP crack me
- Rednaga Challenges
- iOS CTF
- Android Hacking Event 2017: AES-Decrypt
- Android Hacking Event 2017: Token-Generator
- Android Hacking Event 2017: Flag-Validator
- Android Hacking Event 2017: You Can Hide – But You Cannot Run
- Android Hacking Event 2017: Why Should I Pay?
- Android Hacking Event 2017: Esoteric
- Android Hacking Event 2016: StrangeCalculator
- Android Hacking Event 2016: ReverseMe

-
- Android Hacking Event 2016: ABunchOfNative
 - Android Hacking Event 2016: DynChallenge
 - PicoCTF-2014: Pickle Jar - 30
 - PicoCTF-2014: Revenge of the Bleichenbacher
 - Android MIT LL CTF 2013
 - Evil Planner Bsides Challenge
 - Crack-Mes
 - GreHack-2012 - GrehAndroidMe
 - Hackplayers.com Crackmes (in Spanish so an extra challenge): crackme 1
 - Hackplayers.com Crackmes (in Spanish so an extra challenge): crackme 2
 - Hack.Lu's CTF 2011 Reverse Engineering 300
 - Androidcracking.blogspot.com's Crackme's: cracker 0
 - Androidcracking.blogspot.com's Crackme's: cracker 1
 - Insomnia'hack-2K11
 - CSAW-2011: Reversing101
 - Defcon-19-quals: Binary_L33tness
 - Crack me's
 - SeculInside: CTF2011
 - EnoWars-CTF2011: broken_droid
 - Anonim1133
 - Challenge4ctf
 - Ctfpro
 - CTFDroid
 - Android_ctf
 - Robot CTF Android
 - Cl.ctfk
 - Cryptax

CTF Writeups

2022

- NahamCon CTF 2022 Write-up: Click Me! Android challenge
- MRCTF2022-Stuuuuub

2021

- H@ctivityCon 2021 CTF - writeup 1, writeup 2

-
- Write-up du CTF Android
 - Cellebrite 2021 CTF – Investigating Heisenberg’s Android Device
 - Cellebrite 2021 CTF – Marsha’s iPhone (FFS and Backup)
 - Cellebrite 2021 CTF – Beth’s iPhone
 - Cellebrite CTF 2021 Writeup
 - H@cktivitycon 2021 — Mobile challenge writeup - writeup 1, writeup 2
 - CTF Write-Up: Kryptonite
 - NahamCon 2021 Writeups
 - BELKASOFT CTF MAY 2021: WRITE-UP

2020

- Trend Micro CTF 2020 — Keybox writeup
- STACK the Flags 2020: Mobile Challenges Write Up writeup 1, writeup 2
- HactivityCon CTF Mobile Writeup
- CyberSpaceKenya CTF
- Magnet Virtual Summit 2020 CTF (Anroid)
- Magnet Virtual Summit 2020 CTF (iOS) writeup 1, writeup 2
- Google CTF 2020: Android writeup 1, writeup 2
- RaziCTF 2020 WriteUp: Chasing a lock
- DFA/CCSC Spring 2020 CTF
- AppSecIL CTF)
- SunshineCTF 2020 write-up

2019

- DroidCon, SEC-T CTF 2019
- You Shall Not Pass - BSides Canberra 2019
- CyberTruck Challenge 2019 — Android CTF
- BsidesSF-ctf-2019-mobile-track
- BsidesSF CTF - Challenge: Part 1, Part 2
- CTF on a Budget - Magnet User Summit 2019 - Mobile

2018

- H1 202 2018 / H1 202 CTF
- H1-702 CTF (Capture the Flag)

-
- BSidesSF 2018 CTF — Android Reversing/Forensic Challenge
 - Hack the Android4: Walkthrough (CTF Challenge)
 - Google CTF Quals 2018
 - Ilam CTF: Android Reverse WriteUp
 - 8st SharifCTF Android WriteUps: Vol I, Vol II
 - ASIS 2018 Finals: Gunshop
 - H1-202 CTF - Writeup
 - M1Con CTF Write up
 - AES decode with Cyberchef

2017

- BSides San Francisco CTF 2017 : pinlock-150
- BSides San Francisco CTF 2017 : flag-receiver-200
- BSidesSF CTF wrap-up
- itsC0rg1's mobile challenge and BSides SF CTF
- Insomni'hack Teaser 2017 : mindreader-250
- 2017_labyREnth: mob1_ezdroid
- 2017_labyREnth: mob2_routerlocker
- 2017_labyREnth: mob3_showmewhatyougot
- 2017_labyREnth: mob4_androidpan
- 2017_labyREnth: mob5_iotctf

2016

- LabyREnth
- 2016_labyREnth: mob1_lastchance
- 2016_labyREnth: mob2_cups
- 2016_labyREnth: mob3_watt
- 2016_labyREnth: mob4_swip3r
- 2016_labyREnth: mob5_ioga
- 2016_labyREnth: mob6_ogmob
- Holiday hack challenge: Part 01
- Holiday hack challenge: Part 02
- Holiday hack challenge: Part 04a
- Holiday hack challenge: Part 04b
- Holiday hack challenge: Part 04c

-
- Holiday hack challenge: Part 04d
 - Holiday hack challenge: Part 04e
 - Holiday hack challenge: Part 04f
 - Holiday hack challenge: Part 5
 - 0ctf-2016
 - Google-ctf-2016
 - Google-ctf-2016: ill intentions 1
 - Google-ctf-2016: ill intentions 2
 - Cyber-security-challenge-belgium-2016-qualifiers
 - Su-ctf-2016 - android-app-100
 - Hackcon-ctf-2016 - you-cant-see-me-150
 - RC3 CTF 2016: My Lil Droid
 - Cyber Security Challenge 2016: Dexter
 - Cyber Security Challenge 2016: Phishing is not a crime
 - google-ctf-2016 : little-bobby-application-250

2015

- Rctf-quals-2015
- Insomni-hack-ctf-2015
- 0ctf-2015
- Cyber-security-challenge-2015
- Trend-micro-ctf-2015: offensive-200
- codegate-ctf-2015: dodocrackme2
- Seccon-quals-ctf-2015: reverse-engineering-android-apk-1
- Seccon-quals-ctf-2015 - reverse-engineering-android-apk-2
- Pragyan-ctf-2015
- Volgactf-quals-2015
- Opentoall-ctf-2015: android-oh-no
- 32c3-ctf-2015: libdroid-150
- Polictf 2015: crack-me-if-you-can
- lcectf-2015: Husavik

2014

- Qiwi-ctf-2014: not-so-one-time
- Fdfpico-ctf-2014: droid-app-80

-
- Su-ctf-quals-2014: commercial_application
 - defkthon-ctf 2014: web-300
 - secuinside-ctf-prequal-2014: wooyataalk
 - Qiwi-ctf-2014: easydroid
 - Qiwi-ctf-2014: stolen-prototype
 - TinyCTF 2014: Ooooooh! What does this button do?
 - 31c3-ctf-2014: Nokia 1337
 - Asis-ctf-finals-2014: numdroid
 - PicoCTF-2014: Droid App
 - NDH2k14-wargames: crackme200-ChunkNorris

2013

- Hack.lu CTF 2013: Robot Plans
- CSAW Quals CTF 2015: Herpderper

2012

- Atast CTF 2012 Bin 300

Misc

- Nuit du Hack's 2k12 & 2k11 (pre-quals and finals) Android Crackme's 2

Vulnerable Mobile apps:

Android

- Allsafe
- InsecureShop
- OWASP: OMTG-Hacking-Playground
- Damn insecure and vulnerable App (DIVA)
- Damn-Vulnerable-Bank
- Damn Vulnerable Hybrid Mobile App (DVHMA)
- Owasp: Goatdroid Project
- InjuredAndroid
- ExploitMe labs by SecurityCompass

-
- InsecureBankv2
 - Sieve (Vulnerable 'Password Manager' app)
 - sievePWN
 - ExploitMe Mobile Android Labs
 - Hacme Bank
 - Android Labs
 - Digitalbank
 - Dodo vulnerable bank
 - Oracle android app
 - Urdu vulnerable app
 - MoshZuk File
 - Appknox
 - Vuln app
 - Damn Vulnerable FirefoxOS Application
 - Android security sandbox

ios

- ExploitMe Mobile iPhone Labs
- Owasp: iGoat
- Damn Vulnerable iOS App (DVIA)
- Damn Vulnerable iOS App (DVIA) v2

Vulnerable APIs:

- Vapi
- VAmPI
- Vulnerable-api
- vAPI

Vulnerable Web apps:

Node

- Damn Vulnerable Web Service
- Damn Vulnerable NodeJS Application
- Damn Vulnerable Serverless Application

-
- OWASP: Juice Shop
 - Damn Vulnerable Node Application
 - Intentionally Vulnerable node.js application
 - Vulnode
 - OWASP: NodeGoat
 - Vulnerable-node
 - Xtreme Vulnerable Web Application (XVWA)

PHP

- OWASP: Broken Web Applications(BWA)
- Damn Vulnerable Web Application (DVWA)
- Damn Vulnerable Web Services(DVWS)
- OWASP Hackademic Challenges
- OWASP: Insecure Web App Project
- OWASP: WebGoat
- Bwapp
- Beebox
- XVWA - Badly coded web application
- Drunk Admin Web Hacking Challenge
- Peruggia
- Mutillidae
- Btslab
- OWASP: Bricks
- The ButterFly Security Project
- WackoPicko
- Vicnum
- GameOver
- LAMPSecurity Training
- Metasploitable
- Metasploitable 2
- Metasploitable 3
- Hackazon
- Twiterlike
- UltimateLAMP

Sql

- [SQLI-labs](#)
- [Testenv](#)

Python

- [Google Gruyere](#)

Java

- [Owasp: WebGoat](#)
- [Puzzlemall](#)
- [Hacme Books](#)
- [Bodgeit](#)
- [OWASP: Web Goat](#)

Ruby on Rails

- [Hacme Casino](#)
- [RailsGoat](#)

C++

- [Hacme Travel](#)

.NET

- [OWASP: WebGoat.NET](#)
- [Hacme Bank](#)
- [VulnApp](#)

ColdFusion

- [Hacme Shipping](#)

Mobile security resources

- [Mobile app pentest cheatsheet](#)
- [Android security awesome](#)
- [Android security reference](#)
- [Awesome-linux-android-hacking](#)
- [iOS security awesome](#)
- [awesome-iOS-resource](#)
- [Mobile security wiki](#)
- [iPhone wiki](#)
- [Nyxbone](#)
- [Nowhere](#)
- [Secmobi](#)

Infosec resources

- [OSX-iOS-reverse-engineering](#)
- [OSX-security-awesome](#)
- [Awesome-web-hacking](#)
- [Awesome-windows-exploitation](#)
- [windows-privesc-check](#)
- [Awesome-Hacking](#)
- [Awesome-reversing](#)
- [Awesome-Frida](#)
- [Awesome-security](#)
- [Awesome-fuzzing](#)
- [Awesome-wifi-security](#)
- [Android vulnerabilities overview](#)
- [OSX-security-awesome](#)
- [Infosec_Reference](#)
- [PayloadsAllTheThings](#)
- [Awesome-malware-analysis](#)
- [Linux-reverse-engineering-101](#)

Mobile security standards

- [OWASP Mobile Security Project](#)

-
- OWASP Top 10 - 2016
 - OWASP Mobile Application Security Verification Standard (MASVS)
 - OWASP Mobile Security Testing Guide (MSTG)

Credits

- <http://carnal0wnage.attackresearch.com/2013/08/want-to-break-some-android-apps.html>
- <https://www.owasp.org/index.php>
- <https://github.com/ctfs>
- <http://shell-storm.org/repo/>