



#BACK TO ROOT!

HOME SERIES DE ENTRADAS RETOS PODCAST AUTORES CONTACTO



CHECK LIST - MOBILE APPLICATION TESTING II

en **CheckList, Hacking, Hacking Mobile, OWASP, Pentesting** con **1 comentario**

Regularmente ando revisando y buscando algunos Check List para las diferentes tareas de pentesting como esta de [Check List - Web Application Testing](#) y hace un par de meses atras vinimos con uno semejante que es [Check List - Mobile Application Testing](#) debido a ello esta es una versión II y seguro se preguntan que tiene de diferente a la anterior.

The Mobile App Pentest cheat sheet was created to provide concise collection of high value information on specific mobile application penetration testing topics.

- [All-in-one Mobile Security Frameworks](#)
- [Android Application Penetration Testing](#)
 - [Android Testing Distributions](#)
 - [Reverse Engineering and Static Analysis](#)
 - [Dynamic and Runtime Analysis](#)
 - [Network Analysis and Server Side Testing](#)
 - [Bypassing Root Detection and SSL Pinning](#)
 - [Security Libraries](#)
- [iOS Application Penetration Testing](#)
 - [Access Filesystem on iDevice](#)
 - [Reverse Engineering and Static Analysis](#)
 - [Dynamic and Runtime Analysis](#)
 - [Network Analysis and Server Side Testing](#)
 - [Bypassing Root Detection and SSL Pinning](#)
 - [Security Libraries](#)
- [Contribution](#)
- [License](#)

🔗 [ALL-IN-ONE MOBILE SECURITY FRAMEWORKS](#)

- Mobile Security Framework - MobSF - Mobile Security Framework is an intelligent, all-in-one open source mobile application (Android/iOS) automated pen-testing framework capable of performing static and dynamic analysis.
- `python manage.py runserver 127.0.0.1:1337`

☞ ANDROID APPLICATION PENETRATION TESTING

☞ ANDROID TESTING DISTRIBUTIONS

- Appie - A portable software package for Android Pentesting and an awesome alternative to existing Virtual machines.
- Android Tamer - Android Tamer is a Virtual / Live Platform for Android Security professionals.
- AppUse - AppUse is a VM (Virtual Machine) developed by AppSec Labs.
- Mobisec - Mobile security testing live environment.
- Santoku - Santoku is an OS and can be run outside a VM as a standalone operating system. #####
Reverse Engineering and Static Analysis
- APKInspector - APKInspector is a powerful GUI tool for analysts to analyze the Android applications.
- APKTool - A tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications.
 - Disassembling Android apk file
 - `apktool d [apk file]`
 - Rebuilding decoded resources back to binary APK/JAR with certificate signing
 - `apktool b [modified folder]`
 - `keytool -genkey -v -keystore keys/test.keystore -alias Test -keyalg RSA -keysize 1024 -sigalg SHA1withRSA -validity 10000`

- jarsigner -keystore keys/test.keystore dist/test.apk -sigalg SHA1withRSA -digestalg SHA1 Test
- Dex2jar - A tool for converting .dex file to .class files (zipped as jar).
 - Converting apt file into jar file
 - dex2jar [apk file]
- Oat2dex - A tool for converting .oat file to .dex files.
 - Deoptimize boot classes (The output will be in "odex" and "dex" folders)
 - java -jar oat2dex.jar boot [boot.oat file]
 - Deoptimize application
 - java -jar oat2dex.jar [app.odex] [boot-class-folder output from above]
 - Get odex from oat
 - java -jar oat2dex.jar odex [oat file]
 - Get odex smali (with optimized opcode) from oat/odex
 - java -jar oat2dex.jar smali [oat/odex file]
- JD-Gui - A tool for decompiling and analyzing Java code.
- FindBugs + FindSecurityBugs - FindSecurityBugs is a extension for FindBugs which include security rules for Java applications.
- Qark - This tool is designed to look for several security related Android application vulnerabilities, either in source code or packaged APKs.
- AndroBugs - AndroBugs Framework is an efficient Android vulnerability scanner that helps developers or hackers find potential security vulnerabilities in Android applications. No need to install on Windows.
- Simplify - A tool for de-obfuscating android package into Classes.dex which can be use Dex2jar and JD-GUI to extract contents of dex file.

- `simplify.jar -i [input smali files or folder] -o [output dex file]`
- ClassNameDeobfuscator - Simple script to parse through the .smali files produced by apktool and extract the .source annotation lines.

🌀 DYNAMIC AND RUNTIME ANALYSIS

- Introspy-Android - Blackbox tool to help understand what an Android application is doing at runtime and assist in the identification of potential security issues.
- Cydia Substrate - Cydia Substrate for Android enables developers to make changes to existing software with Substrate extensions that are injected in to the target process's memory.
- Xposed Framework - Xposed framework enables you to modify the system or application aspect and behaviour at runtime, without modifying any Android application package(APK) or re-flashing.
- CatLog - Graphical log reader for Android.
- Droidbox - DroidBox is developed to offer dynamic analysis of Android applications.
- Frida - The toolkit works using a client-server model and lets you inject in to running processes not just on Android, but also on iOS, Windows and Mac.
- Drozer - Drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

- Starting a session
 - `adb forward tcp:31415 tcp:31415`
 - `drozer console connect`
- Retrieving package information
 - `run app.package.list -f [app name]`
 - `run app.package.info -a [package name]`
- Identifying the attack surface

- - run app.package.attacksurface [package name]
- Exploiting Activities
 - run app.activity.info -a [package name] -u
 - run app.activity.start --component [package name] [component name]
- Exploiting Content Provider
 - run app.provider.info -a [package name]
 - run scanner.provider.finduris -a [package name]
 - run app.provider.query [uri]
 - run app.provider.update [uri] --selection [conditions] [selection arg] [column] [data]
 - run scanner.provider.sqltables -a [package name]
 - run scanner.provider.injection -a [package name]
 - run scanner.provider.traversal -a [package name]
- Exploiting Broadcast Receivers
 - run app.broadcast.info -a [package name]
 - run app.broadcast.send --component [package name] [component name] --extra [type] [key] [value]
 - run app.broadcast.sniff --action [action]
- Exploiting Service
 - run app.service.info -a [package name]
 - run app.service.start --action [action] --component [package name] [component name]
 - run app.service.send [package name] [component name] --msg [what] [arg1] [arg2] --extra [type] [key] [value] --bundle-as-obj

🌀 NETWORK ANALYSIS AND SERVER SIDE TESTING

- Tcpdump - A command line packet capture utility.
- Wireshark - An open-source packet analyzer.
 - Live packet captures in real time
 - adb shell "tcpdump -s 0 -w - | nc -l -p 4444"
 - adb forward tcp:4444 tcp:4444
 - nc localhost 4444 | sudo wireshark -k -S -i -
- Canape - A network testing tool for arbitrary protocols.
- Mallory - A Man in The Middle Tool (MiTM) that use to monitor and manipulate traffic on mobile devices and applications.
- Burp Suite - Burp Suite is an integrated platform for performing security testing of applications.
- Proxydroid - Global Proxy App for Android System.

🌀 BYPASSING ROOT DETECTION AND SSL PINNING

- Android SSL Trust Killer - Blackbox tool to bypass SSL certificate pinning for most applications running on a device.
- Android-ssl-bypass - an Android debugging tool that can be used for bypassing SSL, even when certificate pinning is implemented, as well as other debugging tasks. The tool runs as an interactive console.
- RootCoak Plus - Patch root checking for commonly known indications of root.

🌀 SECURITY LIBRARIES

- PublicKey Pinning - Pinning in Android can be accomplished through a custom X509TrustManager. X509TrustManager should perform the customary X509 checks in addition to performing the pinning

configuration.

- Android Pinning - A standalone library project for certificate pinning on Android.
- Java AES Crypto - A simple Android class for encrypting & decrypting strings, aiming to avoid the classic mistakes that most such classes suffer from.
- Proguard - ProGuard is a free Java class file shrinker, optimizer, obfuscator, and preverifier. It detects and removes unused classes, fields, methods, and attributes.
- SQL Cipher - SQLCipher is an open source extension to SQLite that provides transparent 256-bit AES encryption of database files.
- Secure Preferences - Android Shared preference wrapper that encrypts the keys and values of Shared Preferences.
- Trusted Intents - Library for flexible trusted interactions between Android apps.

🌀 IOS APPLICATION PENETRATION TESTING

🌀 ACCESS FILESYSTEM ON IDEVICE

- FileZilla - It supports FTP, SFTP, and FTPS (FTP over SSL/TLS).
- Cyberduck - Libre FTP, SFTP, WebDAV, S3, Azure & OpenStack Swift browser for Mac and Windows.
- itunnel - Use to forward SSH via USB.
- iFunbox - The File and App Management Tool for iPhone, iPad & iPod Touch.

🌀 REVERSE ENGINEERING AND STATIC ANALYSIS

- otool - The otool command displays specified parts of object files or libraries.
- Clutch - Decrypts the application and dump specified bundleID into binary or .ipa file.
- Dumpdecrypted - Dumps decrypted mach-o files from encrypted iPhone applications from memory to disk. This tool is necessary for security researchers to be able to look under the hood of encryption.

- iPod:~ root# DYLD_INSERT_LIBRARIES=dumpdecrypted.dylib
/var/mobile/Applications/xxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx/Scan.app/Scan
- class-dump - A command-line utility for examining the Objective-C runtime information stored in Mach-O files.
- Weak Classdump - A Cycrypt script that generates a header file for the class passed to the function. Most useful when you cannot classdump or dumpdecrypted, when binaries are encrypted etc.
 - iPod:~ root# cycrypt -p Skype weak_classdump.cy; cycrypt -p Skype
 - #cy weak_classdump_bundle([NSBundle mainBundle],"/tmp/Skype")
- IDA Pro - IDA is a Windows, Linux or Mac OS X hosted multi-processor disassembler and debugger that offers so many features it is hard to describe them all.
- HopperApp - Hopper is a reverse engineering tool for OS X and Linux, that lets you disassemble, decompile and debug your 32/64bits Intel Mac, Linux, Windows and iOS executables.
- iRET - The iOS Reverse Engineering Toolkit is a toolkit designed to automate many of the common tasks associated with iOS penetration testing.

🌀 DYNAMIC AND RUNTIME ANALYSIS

- cycrypt - Cycrypt allows developers to explore and modify running applications on either iOS or Mac OS X using a hybrid of Objective-C++ and JavaScript syntax through an interactive console that features syntax highlighting and tab completion.
 - Show current view
 - cy#
UIApp.keyWindow.rootViewController.topViewController.visibleViewController
 - Get an array of existing objects of a certain class
 - cy# choose(UIViewController)
 - List method at runtime

- `cy# [classname].messages or`
- `cy# function printMethods(className) { var count = new new Type("I"); var methods = class_copyMethodList(objc_getClass(className), count); var methodsArray = []; for(var i = 0; i < *count; i++) { var method = methods[i]; methodsArray.push({selector:method_getName(method), implementation:method_getImplementation(method)}); } free(methods); free(count); return methodsArray; }`
- `cy# printMethods("[classname]")`
- Prints out all the instance variables
- `cy# function tryPrintIvars(a){ var x={}; for(i in a){ try{ x[i] = (a)[i]; } catch(e){} } return x; }`
- `cy# a=#0x15d0db80`
- `cy# tryPrintIvars(a)`
- Manipulating through property
 - `cy# [a pinCode]`
 - `cy# [a setPinCode: @"1234"]`
 - `cy# [a isValidPin]`
 - `cy# a->isa.messages['isValidPin'] = function(){return 1;}`
- iNalyzer - AppSec Labs iNalyzer is a framework for manipulating iOS applications, tampering with parameters and method.
- idb - idb is a tool to simplify some common tasks for iOS pentesting and research.
- snoop-it - A tool to assist security assessments and dynamic analysis of iOS Apps.
- Introspy-iOS - Blackbox tool to help understand what an iOS application is doing at runtime and assist in the identification of potential security issues.
- gdb - A tool to perform runtime analysis of IOS applications.

- keychaindumper - A tool to check which keychain items are available to an attacker once an iOS device has been jailbroken.
- BinaryCookieReader - A tool to dump all the cookies from the binary Cookies.binarycookies file.

🌀 NETWORK ANALYSIS AND SERVER SIDE TESTING

- Canape - A network testing tool for arbitrary protocols.
- Mallory - A Man in The Middle Tool (MiTM) that use to monitor and manipulate traffic on mobile devices and applications.
- Burp Suite - Burp Suite is an integrated platform for performing security testing of applications.
- Charles Proxy - HTTP proxy / HTTP monitor / Reverse Proxy that enables a developer to view all of the HTTP and SSL / HTTPS traffic between their machine and the Internet.

🌀 BYPASSING ROOT DETECTION AND SSL PINNING

- SSL Kill Switch 2 - Blackbox tool to disable SSL certificate validation - including certificate pinning - within iOS and OS X Apps.
- iOS TrustMe - Disable certificate trust checks on iOS devices.
- Xcon - A tool for bypassing Jailbreak detection.
- tsProtector - Another tool for bypassing Jailbreak detection.

🌀 SECURITY LIBRARIES

- PublicKey Pinning - iOS pinning is performed through a NSURLConnectionDelegate. The delegate must implement connection:canAuthenticateAgainstProtectionSpace: and connection:didReceiveAuthenticationChallenge:. Within connection:didReceiveAuthenticationChallenge:, the delegate must call SecTrustEvaluate to perform customary X509 checks.

🌀 CONTRIBUTION

Your contributions and suggestions are welcome.

~LICENSE



This work is licensed under a [Creative Commons Attribution 4.0 International License](#)
LABS

Veran que el Check List es bastante completo, por mi parte cuando tenga la oportunidad de usarlo en campo de batalla lo tendre en cuenta y comentare el uso del mismo con todo lo que engloba a continuación les dejo la fuente en GITHUB.

•

Fuente

*Regards,
Snifer*

Regards,
Snifer

Compartir: [f](#) [t](#) [G+](#)

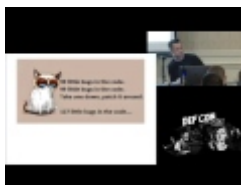
TE PUEDES INTERESAR:



CEH I - Un vistazo a la Seguridad de la Información



Writeup De-ICE_S1.140 por @BalderramaEric



Wireless Pentesting: So Easy A Cave Man Can Do It with N4P A



BurpSuite XXVIII - Trabajando con



Pwneando OpenELEC

[Entrada más reciente](#)

[Página principal](#)

[Entrada antigua](#)

1 COMENTARIO:



Barry Queen 27 sept. 2016 1:56:00

Muchas gracias por la información.

[Responder](#)

Introduce tu comentario...



Comentar como:

Cuenta de Goo ▼

[Publicar](#)


[Vista previa](#)




Hola visitante! deja tu comentario sobre la entrada no spam!

ENLACES A ESTA ENTRADA

Crear un enlace

#HTB



Snifer Hacker
Rank: 615  10  5
hackthebox.eu 

ABOUT ME



#INDEXADOS

Geek Scripting

Se me Cayo un Exploit!

Overload

Isseu

Neebits

World of Wargame

¿Quien es Snifer?

DONACIONES

Donar



Ingresa tu correo electronico:

CATEGORIES

Subscribe

BLOG ARCHIVE

► 19 (12)

► 18 (26)

► 17 (97)

▼ 16 (163)

► diciembre (15)

0day 0xword 101 GbdeInfo 1Libro a la Semana 4n6 8.8 Bolivia 8dot8 Acertijo Aclaraciones Active Directory /
Análisis Forense Android Angelucho Anonimato Anonymous AntiForensic Antivirus Apache APK Aplic
Argentina ARM Arp Atacando al atacante Ataque Físico AUDITtool Autoit Automation Automatización Avira I
Datos Bash Bash Bunny Bashert Beamer Big Data Bing Bitcoin BlackHat Bolivia Bookmarks Bootnet Bots B
Bugtraq BurpSuite Buscadores Buster C C++ C2 Capacitaciones Cápsulas de Seguridad Capture the Fla
Charlas Cheat Sheet CheckList Chema Alonso Chile Chinoogawa Chrome Chromium CICADA Cifrado Cisco
Compiladores Comunicado Conasol Conceptos Conferencias Conky Conociendo sobre Malware Cons
Cracking Craft CraftBooks Criptografia Crypter Css CTF Cube Craft Curiosidades Curl Curso Online Dar
Debian Debugging Dedalo Deface Defcon Dendroid Dennis Ritchie Desafios Desarrollo Seguro Desvariaciones
Dibujando Dirbuster Diseño Distribuciones Django DNSCrypt Docker Documentacion Documentales Docu
DragonJar Drivers DROWN Drupal Easy Scripts Eavesdrooping Ebook Eclipse eJPT Ekoparty El mundo loco
EnelPC English Entel Entrevistas Enumeration Escalamiento de Privilegios Escaner de Vulnerabilidades Estegan
Exploiting Explotación ExtJS Ezines Facebook Faraday Fasm FastTrack FBHT Fedora FFoS Fideos de Pythor
Forensic Formato PE Frameshock Framework Fuerza Bruta FullDisclosure Fuzzer GAE GameBoy GDB Gedit G
Google App Engine Gr2Dest Grampus Grep Guia Guia de Shodan Hackeado Hacker Hacker Épico Hackers Hack
Hacking Fisico Hacking Kids Hacking Lab Hacking Mexico Hacking Mobile Hacking Web Hack
Hackmeeting HackStory HackTheBox HackToPy Hangout Hardening Hash HashCat Haskell hdbreaker Heartble
HoneyNets Honeybots Hotel Hotmail HP Html HTML5 HTMLi Humor i3 i3-wm IDA PRO IDE IDS ImageMagick
Informática Forense Information Gathering Ingenieria de Sistemas Ingenieria Inversa Ingeniería Social Ir
JackTheStripper Jalasoft Jaqi-Aru Java Joomla Jose Moruno Cadima Jquery Juegos Jugando con mi Raspber
L4bsForAndroid L4bsForEzine L4bsForShell La Paz La Trinchera Laboratorio SniferL4bs Latch LaTeX LI
Locos por Wifi LOLBins LPI Mac OS X Magazine Malware Malware 101 Man in the Middle Manjaro Manua
MaratonLinuxero Mashups Medussa Mega Meld Memorias Metadatos Metagoofil Metasploit Metasploitable Mete
modding ModSecurity Modular Modularidad Monero MongoDB Monitoreo Mozilla Firefox Mr Robot msfenc

► noviembre (8)

► octubre (6)

▼ septiembre (11)

Penetration Testing with Nmap I - Consultado Whois...

CTF DragonJAR 2016 - Writeup por Amnesia Team

Repositorio de herramientas forenses

Game Of Hacks: Entorno Online para practicar la au...

Check List - Mobile Application Testing II

Conociendo sobre Malware XXI - Awesome Malware Ana...

Dame una Shell - 2x01 - Security Week 0x14 Hackeo ...

K0sasp - Hacking con OS X

Colección de Retos sobre XSS - Cross Site Scriptin...

Hacking Soft Tokens Advanced Reverse Engineering ...

CMSmap: Escaner de Vulnerabilidades para Drupal, W...

► agosto (9)

► julio (7)

NetworkProgramming NFCC Nginx Ngrok **Nmap** NodeJS NodeOS NoSQL Noticias Nox NSA Nugget Nvidia Obfusca
OpenCV OpenELEC OpenOffice OpenSSL Opiniones OSCP OSINT OSMTD **OWASP** OWASP Day **Paper** Paramete
Pdf peframe Peliculas Pentaho **Pentesting** Pentesting con Bash Pentesting con Metasploit Pentesti
Personal Gabriela Phishing **PHP** PirateBay Pivoting Plugin PoC **Podcast** Pokemon PokemonGO Potencias P
Preguntas y Respuestas **Principiante en Linux** Privacidad Private **Programación** Programas Prox
Linux PyQT PyTesting **Python** PythonForensic QMAIL Qt Radare Radare2 Ransomware Raspberry PI RCEe
Sociales Regex Reportes Research Resumen Semanal **Retos** Retos Criptográficos Retos Forenses Ret
Narvaja RizelTane RoadToOSCP RTFM Rubber Ducky **Ruby** RVM Saber Libre SafeKids SandBox Sass S
SeguridadJabali Sencha Serveo Session Shaka shellcode ShellShock **Shodan** SickOS Silver Sin 0 ni1 Skype S
SniferL4bs Sniffee Sniffer Softonic **Software** Software Libre Solución Reto Solución Underc0de Sorte
Steve Jobs SubgraphOS Sublime Text SubVersion Sw-Craft SysAdmin Taller TDD Telegram Teoría **Termi**
ThePastryBox Tigo TINT2 **Tip Tip's Tool** Tor Touchpad Traducción Troopers Troyano TrueCrypt **Tutorial**
Underdocs Unix Friday Day Uremix USB **Videos** **VideoTutoriales** Viernes de LaTeX Vim Viñetas Viper Virt
VulnHub WAF Wardriving Wargame **Web** WebCast WebShell WebSploit Wep Whatsapp Who is Mr Robot
Wireless **Wireless Penetration Tools** Wireless Pentesting desde 0 Wireshark Wireshark 101 Wordpre
Xss Yersenia Youtube ZAP **Zaproxy** Zentyl

- ▶ **junio** (15)
- ▶ **mayo** (13)
- ▶ **abril** (16)
- ▶ **marzo** (21)
- ▶ **febrero** (15)
- ▶ **enero** (27)
- ▶ **15** (255)
- ▶ **14** (336)
- ▶ **13** (124)
- ▶ **12** (177)
- ▶ **11** (79)

#FORENSIC AND SECURITY

Sysforensics

Forensic Contest

Underc0de

Forensic Focus

Python Tools for Pentesting

Debian Hackers

Un Informatico del Lado del Mal

Conexion Inversa

Seguridad a lo Jabali

Hackplayers

Comunidad DragonJAR

Segu-Info



