IOS 安全学记资料汇总

By 熊猫正正

(1) IOS 安全学习网站收集：
http://samdmarshall.com
https://www.exploit-db.com
https://reverse.put.as
http://security.ios-wiki.com
https://truesecdev.wordpress.com/
http://resources.infosecinstitute.com/ios-application-security-part-1-setting-up-a-mobile-pentesting-platform/
http://esoftmobile.com/2014/02/14/ios-security/
http://bbs.iosre.com
http://bbs.chinapyg.com
http://blog.pangu.io/
http://yonsm.net/
http://nianxi.net/
https://github.com/pandazheng/iOSAppReverseEngineering
http://drops.wooyun.org
http://bbs.pediy.com

(2) IOS 安全优秀博客文章
https://github.com/secmobi/wiki.secmobi.com
http://bbs.iosre.com/t/debugserver-lldb-gdb/65
http://bbs.pediy.com/showthread.php?t=193859
http://bbs.pediy.com/showthread.php?t=192657&viewgoodnees=1&prefixid=
http://blog.darkrainfall.org/2013/01/os-x-internals/
http://dvlabs.tippingpoint.com/blog/2009/03/06/reverse-engineering-iphone-appstore-binaries
http://drops.wooyun.org/papers/5309
https://www.safaribooksonline.com/library/view/hacking-and-securing/9781449325213/ch08s04.html
http://soundly.me/osx-injection-override-tutorial-hello-world/
https://nadavrub.wordpress.com/2015/07/23/injecting-code-to-an-ios-appstore-app/

(3) IOS 安全优秀 GitHub
XCodeGhost 清除脚本
https://github.com/pandazheng/XCodeGhost-Clean
Apple OS X ROOT 提权 API 后门
https://github.com/tihmstar/rootpipe_exploit
Dylib 插入 Mach-O 文件

https://github.com/Tyilo/insert_dylib
OSX dylib injection
https://github.com/scen/osxinj
IOS IPA package refine and resign
https://github.com/Yonsm/iPAFine
ROP Exploitation
https://github.com/JonathanSalwan/ROPgadget
Scan an IPA file and parses its info.plist
https://github.com/apperian/iOS-checkIPA
A PoC Mach-O infector via library injection
https://github.com/gdbinit/osx_boubou
IOS-Headers
https://github.com/MP0w/iOS-Headers
Interprocess Code injection for Mac OS X
https://github.com/rentzsch/mach_inject
OS X Auditor is a free Mac OS X computer forensics tool
https://github.com/jipegit/OSXAuditor
remove PIE for osx
https://github.com/CarinaTT/MyRemovePIE
A TE executable format loader for IDA
https://github.com/gdbinit/TELoader
Mobile Security Framework
https://github.com/ajinabraham/Mobile-Security-Framework-MobSF
A library that enables dynamically rebinding symbols in Mach-O binaries running on iOS
https://github.com/facebook/fishhook
OSX and iOS related security tools
https://github.com/ashishb/osx-and-ios-security-awesome
Introspy-Analyzer
https://github.com/iSECPartners/Introspy-Analyzer
Dumps decrypted mach-o files from encrypted iPhone applications from memory to disk
https://github.com/stefanesser/dumpdecrypted
Simple Swift wrapper for Keychain that works on iOS and OS X
https://github.com/kishikawakatsumi/KeychainAccess
idb is a tool to simplify some common tasks for iOS pentesting and research
https://github.com/dmayer/idb
Pentesting apps using Parse as a backend
https://github.com/igrekde/ParseRevealer
The iOS Reverse Engineering Toolkit
https://github.com/Vhacker/iRET
XNU - Mac OS X kernel
https://github.com/opensource-apple/xnu
Code injection + payload communications for OSX

https://github.com/mhenr18/injector
iOS related code
https://github.com/samdmarshall/iOS-Internals
OSX injection tutorial: Hello World
https://github.com/arbinger/osxinj_tut
Reveal Loader dynamically loads libReveal.dylib (Reveal.app support) into iOS apps on jailbroken devices
https://github.com/heardrwt/RevealLoader
NSUserDefaults category with AES encrypt/decrypt keys and values
https://github.com/NZN/NSUserDefaults-AESEncryptor
Blackbox tool to disable SSL certificate validation
https://github.com/iSECPartners/ios-ssl-kill-switch
应用逆向工程 抽奖插件
https://github.com/iosre/iosrelottery
Untested iOS Tweak to hook OpenSSL functions
https://github.com/nabla-c0d3/iOS-hook-OpenSSL
IOS *.plist encryptor project. Protect your *.plist files from jailbroken
https://github.com/FelipeFMMobile/ios-plist-encryptor
Re-codesigning tool for iOS ipa file
https://github.com/hayaq/recodesign
Scans iPhone/iPad/iPod applications for PIE flags
https://github.com/stefanesser/.ipa-PIE-Scanner
xnu local privilege escalation via cve-2015-1140 IOHIDSecurePromptClient injectStringGated heap overflow | poc||gtfo
https://github.com/kpwn/vpwn
MachOView
https://github.com/gdbinit/MachOView
A cross-platform protocol library to communicate with iOS devices
https://github.com/libimobiledevice/libimobiledevice

(4) IOS 安全优秀书籍
《Hacking and Securing iOS Applications》
《Mac OS X and iOS Internals:To the Apple's Core》
《OS X and iOS Kernel Programming》
《OS X ABI Mach-O File Format》
《The Mac Hacker's Handbook》
《Mac OS X Interals:A Systems Approach》
《黑客攻防技术宝典-IOS 实战篇》
《IOS 应用安全攻防实战》
《IOS 应用逆向工程》
《IOS 取证实战》
《安全技术大系：IOS 取证分析》

(5) IOS 安全 Twitter
https://twitter.com/Technologeeks
https://twitter.com/osxreverser