



iOS Pentesting Tools

 2018-03-11  Trelis  [iOS](#)  [iOS tools](#)

This is a quick guide of the tools used to do iOS pentesting.

Cydia Impactor

Tool to install IPA files in iOS.

- Installation: <http://www.cydiaimpactor.com/>

Phoenix Jailbreak

Tool I used to do the jailbreak. However, depending on the version and the device, there are more tools available.

- Installation: <https://phoenixpwn.com/>
- More information: https://en.wikipedia.org/wiki/IOS_jailbreaking
- Installation2: <http://www.tutuapp.vip/index.php?appId=3102329&lang=en&r=shareAppVip%2Findex&type=zb>

Otool

Content

- [Cydia Impactor](#)
- [Phoenix Jailbreak](#)
- [Otool](#)
- [Ipa Installer](#)
- [App Sync](#)
- [Class-Dump](#)
- [Cycrypt](#)
- [Frida](#)
- [Clutch](#)
- [App Cake](#)
- [Damn Vulnerable App](#)
- [Keychain Dumper](#)
- [Similar Posts](#)

Tool used to obtain information of the application.

- Cydia repository: <http://apt.thebigboss.org/repofiles/cydia/>
- Installation: search for “Big Boss Recommended Tools” on Cydia
- Installation2: search for “Darwin CC tools” on Cydia

Ipa Installer

Allows to install IPAs from the device filesystem.

- Cydia repository: <http://apt.thebigboss.org/repofiles/cydia/>
- Installation: search for “IPA installer” on Cydia

App Sync

Allows to install unsigned or cracked apps on jailbroken iOS devices.

- Cydia repository: <http://cydia.angelxwind.net/>
- Installation: search for “AppSync Unified” on Cydia

Class-Dump

Used to gather information of the application classes. Rip apart an Objective-C binary and generate .h interface definitions.

- Installation: search for “Class Dump” on Cydia

Cycript

Used for the dynamic test of an application. When used as an execution frontend, Cycrypt bridges access to Objective-C primitives using an extended syntax, providing for memory allocation, pointer indirection, and message dispatch.

- Installation: search for “Cycrypt” on Cydia

Frida

Used for the dynamic test of an application.

- Cydia repository: <https://build.frida.re>
- Installation: search for “Frida” on Cydia
- Linux installation: via terminal “\$ sudo pip install frida”
- More information: <https://www.frida.re/docs/home/>

Clutch

Used to decrypt applications.

- Cydia repository: <http://repo.xarold.com>
- Installation: search for “Clutch” on Cydia

App Cake

Free download of cracked iOS & Mac OSX Apps.

- Cydia repository: <http://cydia.iphonecake.com>
- Installation: search for “App Cake” on Cydia

Damn Vulnerable App

Vulnerable application.

- Cydia repository: <http://repo.kyelevin.com>
- Installation: search for “Damn Vulnerable App” on Cydia

Keychain Dumper

It dumps all the data of the Keychain



- Installation: <https://github.com/ptoomey3/Keychain-Dumper>

Similar Posts

- [Frida iOS](#)
- [iOS Pentesting - Reversing Jailbreak](#)
- [iOS Pentesting - Introduction](#)
- [iOS Pentesting - Static analysis](#)

Previous post [Chntpw SAM](#)

Next post [iOS Pentesting - Static analysis](#)

Contact me at:  

This site has been visited: times, Number of visitors: , This post has been viewed times

Site powered by [Jekyll](#) & [Github Pages](#). Theme designed by [HyG](#).