

Start your first iOS Application Pentest with me.. (Part- 1)



Kishor balan · Following

6 min read · Jan 14, 2023

Listen

Share

More

Hola Heckers,

Hope y'all doing good. So today we are going to prepare a jailbroken iOS device to start an iOS pentesting. This article won't be covering the complete methodologies, Will be sliced into two parts. Only the following things will be covered today.

1: Installing the required tools and Cydia tweaks

Note:- There are a plenty of different tools and methodologies when its coming to the iOS pentesting and I won't be able to explain all of them, only my methodology will be shared here.

Prerequisites:

1: A Jailbroken iOS device

Setting up the lab and installing basic tools:

1: Hope you already have **Frida** and **Objection** tools in your system, If not , install them

[Releases · frida/frida \(github.com\)](#)

[GitHub – sensepost/objection: 📺 objection – runtime mobile exploration](#)

2: iTunes: We know iTunes will help us to work with iOS environments in several ways.

3: 3uTools: This one has a lot of useful features such as **Direct SSH connection**, **Screen mirroring**, **iOS application installer**, etc..

[3uTools | The best all-in-one tool for iOS users](#)

The screenshot shows the 3uTools interface with the following details:

- Device Info:** iPhone 7, 32GB, Black. PC Charging (2W) [4%]
- Hardware & System:**
 - iOS Version: 13.3.1 (17D50)
 - Jailbroken: Yes (Install AFC2)
 - Activated: Yes
 - Product Type: iPhone9,1 (A1779)
 - Sales Model: MNCE2 J/A
 - IMEI: [REDACTED]
 - Serial No.: G7X
 - ECID: [REDACTED]026
 - Verify UDID: Yes
 - UDID: [REDACTED]B11B
- Performance & Status:**
 - View Verification Report
 - View iDevice Details
- Storage:** Hard Disk Capacity: 11.65 GB / 29.79 GB. Legend: System (green), Apps (blue), Photos (pink), Media (yellow), UDisk (purple), Used (orange), Free (grey).
- Bottom Tools:**
 - Backup/Restore (umbrella icon)
 - 3uAirPlayer (play button icon)
 - Make Ringtones (ringing phone icon)
 - Stop iOS Update (stop sign icon)
 - Transfer Data (H icon)
 - More (three dots icon)

The screenshot shows the 3uTools website interface. At the top, there's a navigation bar with icons for iDevice, Apps, RT & WP, Smart Flash, Toolbox, and Tutorials. Below the navigation bar, a search bar contains the text "pentest's iPhone". A "Find tool" button and a magnifying glass icon are also present. The main content area is divided into sections: "Common tools" and "More tools".

Common tools:

- Backup/Restore: Easily backup and restore de...
- VirtualLocation: Globally modify device GPS ...
- Realtime Screen: Real-time display of the devi...
- 3uAirPlayer: Computer display device scr...
- Erase All Data: Restore the device to factory ...
- Batch activation: Support multiple devices to a...
- iTunes Utility: Install and repair iTunes and ...
- Clean Garbage: Quickly clean up device junk ...
- Update IPCC file: Update IPCC operator files
- Transfer Data: Migrate data to new equipm...
- Stop iOS Update: Block iOS update message
- Make Ringtone: DIY ringtones
- Accessibility: Turn on or off accessibility fe...
- Delete Invalid Icon: Delete all kinds of stubborn i...
- Realtime Log: Real-time display of log infor...

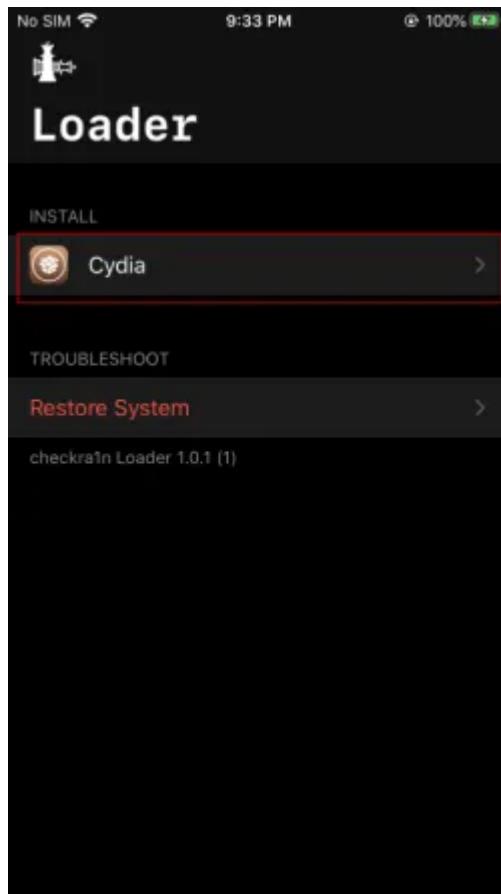
More tools:

- Reboot iDevice
- Turn Off iDevice
- Deactivate
- Close SSH Tunnel
- Enter Rec Mode
- Backup BootSec
- Screen Time
- Crash Analysis
- Manage Icon
- Convert HEIC
- Compress Photo
- Photo Deduplication
- Firmware
- UDisk
- Edit Audio Tags
- Convert Audio
- Convert Video
- 3uPlayer
- IPA Signature
- Social App Backup
- Manage Desc File
- Genuine Accessori...
- Skip MDM Lock
- Screen Recording
- Jailbreak

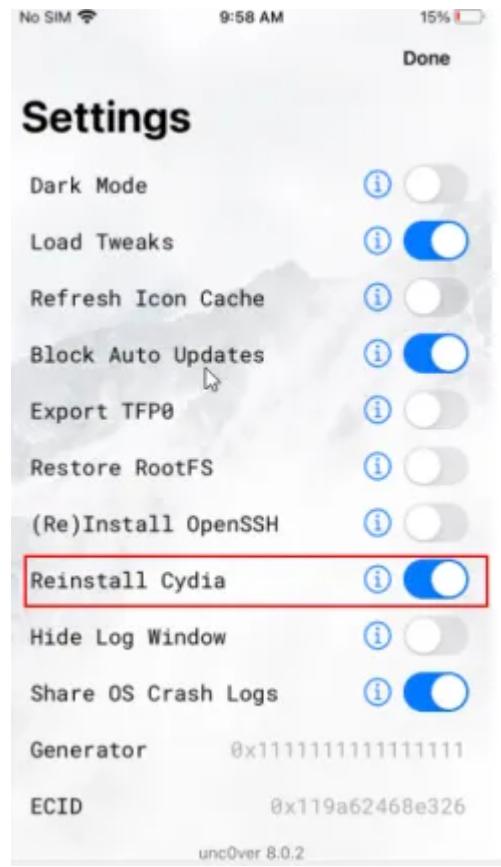
4: Cydia Application:- Basically, Cydia is a third-party application installer which is similar to the App Store and developed for the jailbroken iOS iDevices. If you are jailbreaking your device with Checkra1n or Uncover, The cydia app will automatically get installed into your device.

What if the Cydia haven't installed during the jailbreak:

In case of Checkra1n, you can manually install the Cydia from the Checkra1n app.



In case of Uncover, you can enable the **Reinstall Cydia** option from the Uncover app settings and start jailbreaking.

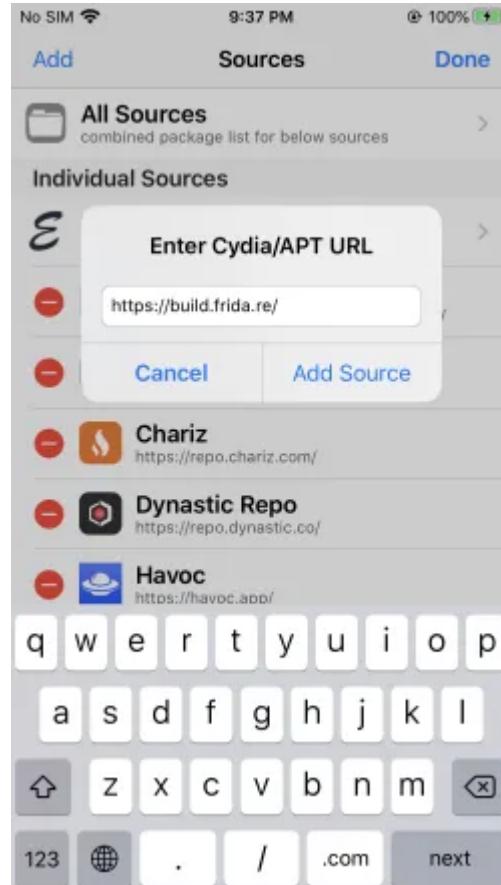
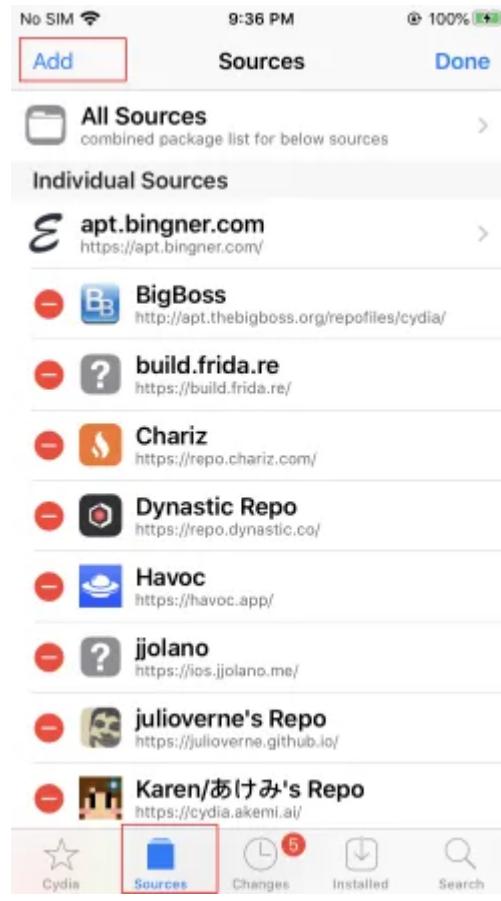


After the jailbreaking process, the Cydia app can be found in the device.

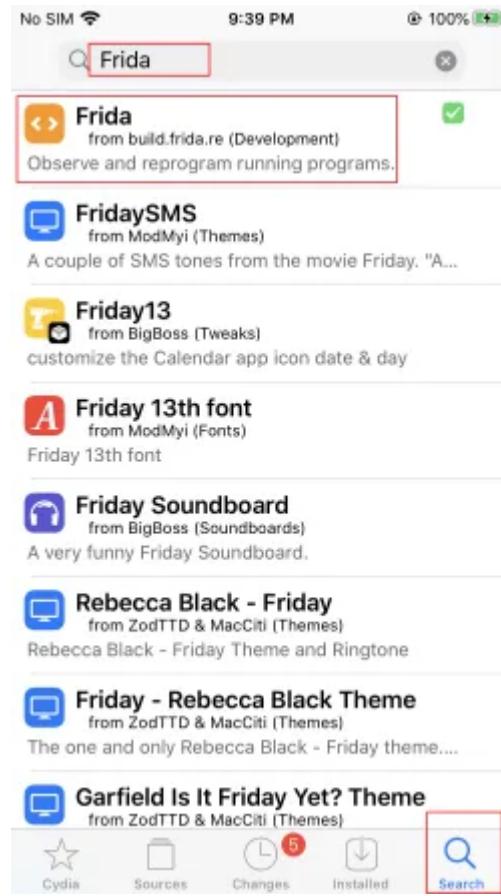
Method for installing Tweaks on the Jailbroken iOS device:

1: With the help of Cydia

Step 1: Add the repo URL of the required cydia tweak in the source section



Step 2: After adding the Source, You can find search the tweak from the search section



Step 3: Select the tweak and install, Respring the device if it is needed.

2: Direct method:

Installing the Tweaks with their .deb files through the OpenSSH terminal

Step 1: Find the Tweak's deb file from its source.

Step 2: Copy the file link and SSH to the iOS device as root user

Step 3: Download the deb file using wget

```
Using username "root".
pentests-iPhone:~ root# wget https://github.com/frida/frida/releases/download/16.0.7/frida_16.0.7_iphoneos-arm.deb
--2023-01-10 21:54:42-- https://github.com/frida/frida/releases/download/16.0.7/frida_16.0.7_iphoneos-arm.deb
Resolving github.com... 20.207.73.82
Connecting to github.com|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/9405122/97718949-dc29-47ab-b
JYAX4CSVEH53A%2F20230110%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230110T152525Z&X-Amz-Expires=300&X-Amz-Signat
-SignedHeaders=host&actor_id=0&key_id=0&repo_id=9405122&response-content-disposition=attachment%3B%20filename%3Dfrid
m [following]
--2023-01-10 21:54:42-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/9405122/97718
dential=AKIAIWNJYAX4CSVEH53A%2F20230110%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20230110T152525Z&X-Amz-Expires=3
d84aea8c2&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=9405122&response-content-disposition=attachment%3B%2
n%2Foctet-stream
Resolving objects.githubusercontent.com... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to objects.githubusercontent.com|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 17540732 (17M) [application/octet-stream]
Saving to: 'frida_16.0.7_iphoneos-arm.deb'

frida_16.0.7_iphoneos-arm.deb          100%[=====] 2023-01-10 21:54:46 (5.50 MB/s) - 'frida_16.0.7_iphoneos-arm.deb' saved [17540732/17540732]

pentests-iPhone:~ root# 
```

Step 4: Make the file executable with the permission command “`chmod +x file.deb`” and install it using “`dpkg`” command

```
pentests-iPhone:~ root# chmod +x
pentests-iPhone:~ root# chmod +x frida_16.0.7_iphoneos-arm.deb
pentests-iPhone:~ root# dpkg -i frida_16.0.7_iphoneos-arm.deb
(Reading database ... 4203 files and directories currently installed.)
Preparing to unpack frida_16.0.7_iphoneos-arm.deb ...
Unpacking re.frida.server (16.0.7) over (15.1.24) ...
/Library/LaunchDaemons/re.frida.server.plist: Operation now in progress
Setting up re.frida.server (16.0.7) ...
pentests-iPhone:~ root# 
```

Step 5: That's it, Now the tweak will be installed on your device

Dependencies:

The following packages should be installed on the device:

- Cydia Substrate
- PreferenceLoader

Installing the required Cydia Tweaks:

Tweaks are basically third party applications which can be used to outrun some sort of fences set up in the target iOS applications. A lot of tweaks are available but here I am listing out the necessary ones.

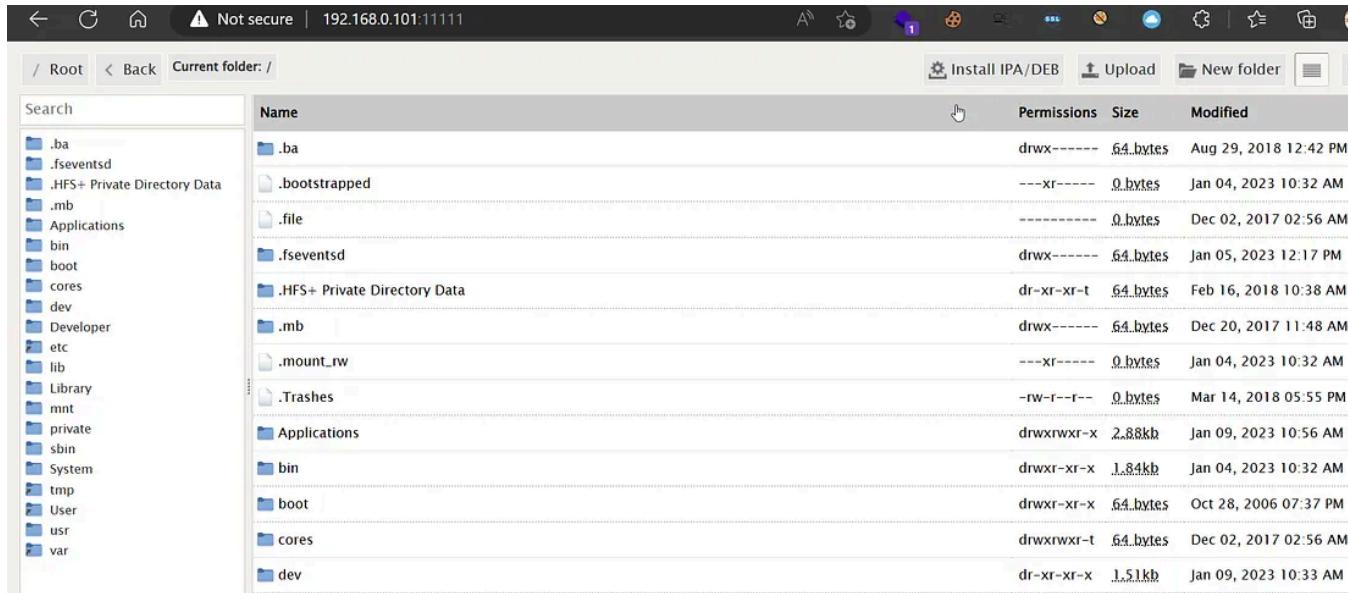
A: Filza:

Repo: <https://tigisoftware.com/cydia/>

Filza is a file manager for exploring directories including root's directories.



Filza also provides WebDav server so we can access the application on our other local machines.



Current folder: /				
	Name	Permissions	Size	Modified
	.ba	drwx-----	64.bytes	Aug 29, 2018 12:42 PM
	.fseventsds	---xr----	0.bytes	Jan 04, 2023 10:32 AM
	.HFS+ Private Directory Data	-----	0.bytes	Dec 02, 2017 02:56 AM
	.mb	drwx-----	64.bytes	Jan 05, 2023 12:17 PM
	Applications	dr-xr-xr-t	64.bytes	Feb 16, 2018 10:38 AM
	bin	drwx-----	64.bytes	Dec 20, 2017 11:48 AM
	boot	---xr----	0.bytes	Jan 04, 2023 10:32 AM
	cores	drwxr-xr-x	2.88kb	Jan 09, 2023 10:56 AM
	dev	drwxr-xr-x	1.84kb	Jan 04, 2023 10:32 AM
	Developer	drwxr-xr-x	64.bytes	Oct 28, 2006 07:37 PM
	etc	drwxr-xr-t	64.bytes	Dec 02, 2017 02:56 AM
	lib	dr-xr-xr-x	1.51kb	Jan 09, 2023 10:33 AM
	Library			
	mnt			
	private			
	sbin			
	System			
	tmp			
	User			
	usr			
	var			

B: App Sync Unified

Repo: <https://cydia.akemi.ai/>

The tweak helps to install IPA files which are ad-hoc signed, fakesigned, or unsigned.



C: IPA installer

Repo: <http://apt.thebigboss.org/repofiles/cydia/>

This one can be used to install/Backup IPA files directly to our jailbroken iOS device.



D: OpenSSH

Repo: <http://apt.saurik.com/>

We know why we need an OpenSSH feature. We can get a terminal access to our iOS device with root privileges.

Root credential: — root: alpine

The screenshot shows the Cydia application interface. At the top, there are status icons for signal strength, battery level (100%), and time (10:03 PM). Below the header, the word "Installed" is highlighted in blue. The main content area displays the "OpenSSH" package details. The package icon is a yellow gear with a black skull. The name "OpenSSH" is displayed in bold, followed by the version "8.4-2" and file size "8 kB". There are three interactive links: "Change Package Settings", "Author" (Sam Bingner), and "This is a console package!". A section titled "INSTALLED PACKAGE" contains "Version" (8.4-2) and "Filesystem Content". The "Filesystem Content" link leads to a page showing the path "openssh" under "apt.bingner.com · Networking".

Open in app ↗



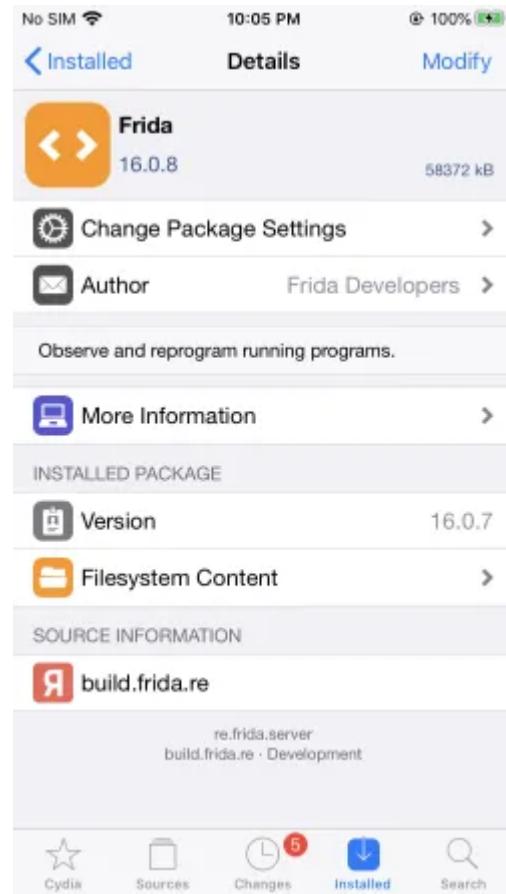
Search



E: Frida

Repo: <https://build.frida.re/>

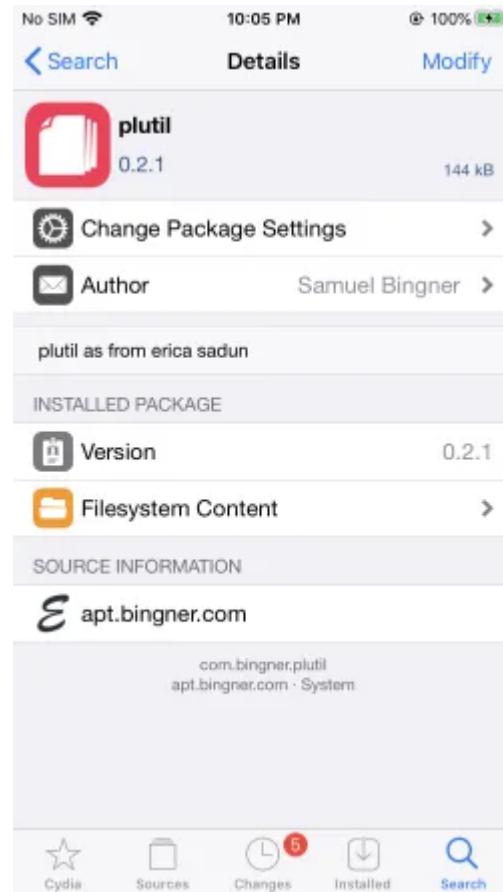
To work with frida tools, a frida server must be installed on our iOS device.



F: Plutil

Repo: <https://apt.bingner.com/>

This tool can be used to read .plist files (Similar to xml files in android)



G: fsmon

Repo: [GitHub – nowsecure/fsmon: monitor filesystem on iOS / OS X / Android / FirefoxOS / Linux](https://github.com/nowsecure/fsmon)

This is a FileSystem Monitor utility that can be used in environments such as Linux, Android and iOS.

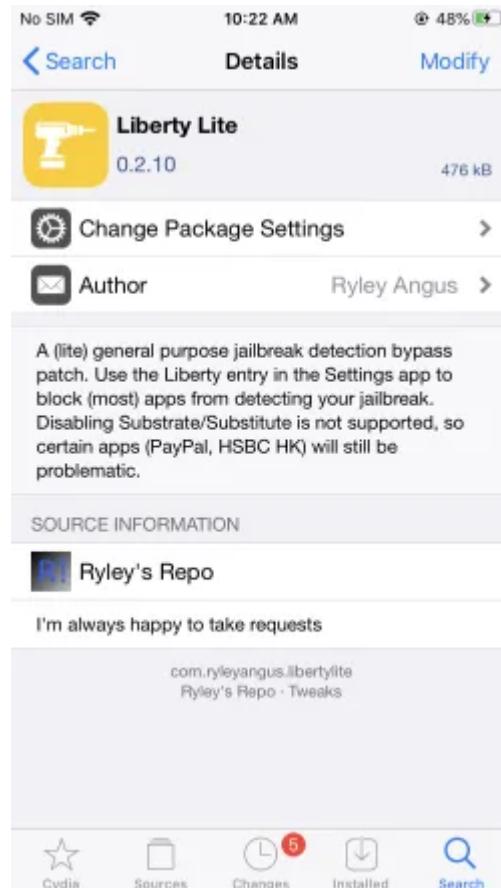
```
pentests-iPhone:~ root# fsmon
FSE_XATTR_MODIFIED      38      "logd"   /private/var/db/diagnostics/Persist/000000000000000026f.tracev3
FSE_XATTR_MODIFIED      38      "logd"   /private/var/db/diagnostics/Special/0000000000000000131.tracev3
FSE_XATTR_MODIFIED      38      "logd"   /private/var/db/diagnostics/Persist/000000000000000026f.tracev3
FSE_XATTR_MODIFIED      38      "logd"   /private/var/db/diagnostics/Persist/000000000000000026f.tracev3
FSE_XATTR_MODIFIED      38      "logd"   /private/var/db/diagnostics/Signpost/000000000000000025.tracev3
FSE_CREATE_FILE 6126  "Cydia"  /private/var/tmp/clearsigned.message.VUrO3Z
FSE_DELETE      6126  "Cydia"  /private/var/tmp/clearsigned.message.VUrO3Z
FSE_CREATE_FILE 6126  "Cydia"  /private/var/tmp/clearsigned.message.2Z1LT6
FSE_DELETE      6126  "Cydia"  /private/var/tmp/clearsigned.message.2Z1LT6
FSE_CREATE_FILE 6126  "Cydia"  /private/var/tmp/clearsigned.message.7MlhpE
FSE_DELETE      6126  "Cydia"  /private/var/tmp/clearsigned.message.7MlhpE
FSE_CREATE_FILE 6126  "Cydia"  /private/var/tmp/clearsigned.message.2Bm7cG
FSE_DELETE      6126  "Cydia"  /private/var/tmp/clearsigned.message.2Bm7cG
FSE_CREATE_FILE 100   "cfprefsd" /private/var/mobile/Library/Preferences/com.apple.sharingd.plist
FSE_CHOWN       100   "cfprefsd" /private/var/mobile/Library/Preferences/com.apple.sharingd.plist
FSE_CHOWN       100   "cfprefsd" /private/var/mobile/Library/Preferences/com.apple.sharingd.plist
FSE_XATTR_MODIFIED      38      "logd"   /private/var/db/diagnostics/Persist/000000000000000026f.tracev3
FSE_CREATE_FILE 39    "assistantd" /private/var/mobile/Library/Assistant/SiriAnalytics.db-journal
FSE_CREATE_FILE 112   "securityd" /private/var/tmp/SOSBackup-OtherSyncable-tomb
FSE_CHOWN       100   "assistantd" /private/var/mobile/Library/Assistant/SiriAnalytics.db-journal
```

Tweaks for Bypassing Jailbreak detection:

Following are the mostly used tweaks used for bypassing Jailbreak detections.

A: Liberty Lite

Repo: <https://rleyangus.com/repo/>



B: A-Bypass

Repo: <https://repo.co.kr/>

No SIM 10:23 AM 48%

[Search](#) [Details](#) [Modify](#)

A-Bypass
1.5.8 960 kB

[Change Package Settings](#) >

[Author](#) Baw Appie >

A-Bypass

Dependencies

If A-Bypass cannot be installed due to a dependency error, add the following repository:

- libMRYIPC - [Dynamic Repo](#) or BigBoss
- applist - [Rpetrich Repo](#) or BigBoss
- RocketBootstrap - [Rpetrich Repo](#) or BigBoss

[Cydia](#) [Sources](#) [Changes](#) [Installed](#) [Search](#)

C: HideJB

Repo: <http://apt.thebigboss.org/repofiles/cydia/>

No SIM 10:24 AM 48%

[Search](#) [Details](#) [Install](#)

HideJB
2.1.1 1929 kB

[Change Package Settings](#) >

[Author](#) TTJB Team >

Advertisements

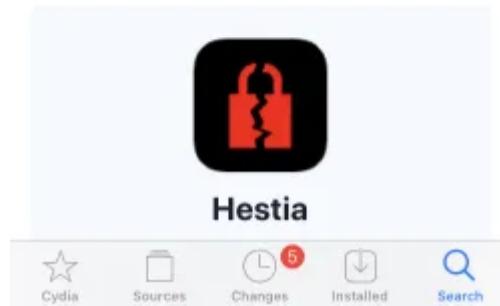
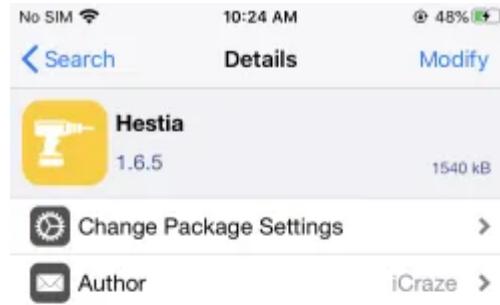
Description

Giới thiệu HideJB, một tweak có chức năng bỏ qua phát

[Cydia](#) [Sources](#) [Changes](#) [Installed](#) [Search](#)

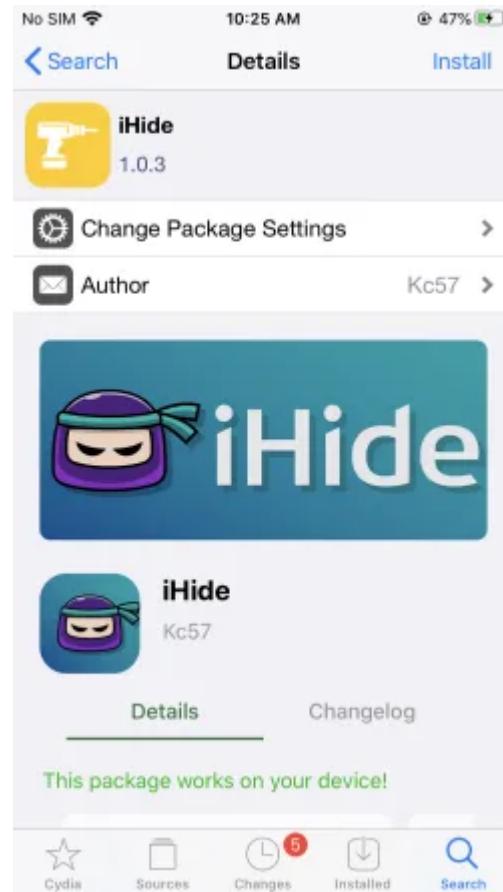
D: Hestia

Repo: <https://havoc.app/>



E: iHide

Repo: <https://repo.kc57.com/>



Alternatively, You can use frida scripts to bypass the JB detection

Frida CodeShare

Tweaks for Bypassing SSL Pinning Bypass:

Following are the most used tweaks used for bypassing SSL certificate pinning.

A: SSL Kill Switch

Repo: <https://julioverne.github.io/>



B: SSLBypass

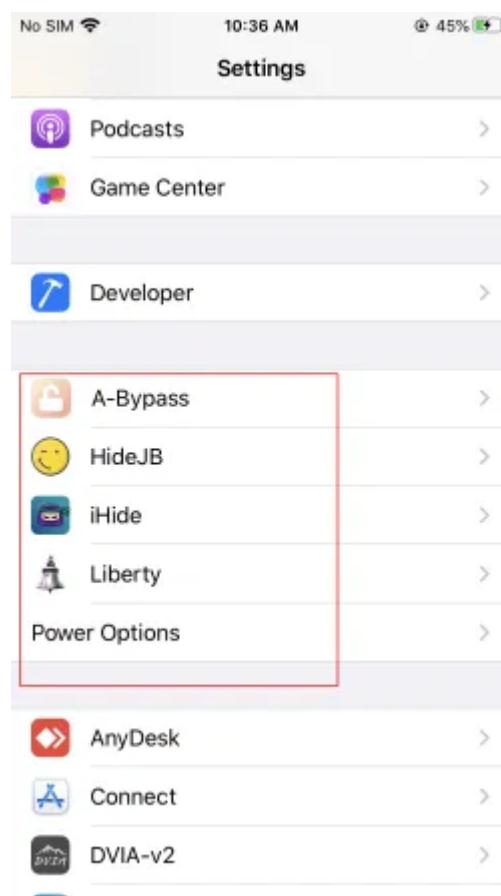
Repo: [SSLBypass/packages at main · evilpenguin/SSLBypass · GitHub](#)



Alternatively, You can use frida scripts to bypass the SSL pinning

Frida CodeShare

Note:- Most of the Jailbreak Detection Bypass and SSL Bypass tweaks can be found in the device settings after the installation.



So that's it guys, We almost ready to go. We will kickstart on our first iOS application pentesting in the Part-2. If I have missed something in this part, we will cover 'em up in the next part. Stay tuned, Happy hacking :)


[Following](#)


Written by Kishor balan

418 Followers

Security Analyst || eWPTXv2 || ejPT

More from Kishor balan

```
(iPhone: 16.4.1) [usb] # env
-----
r/Containers/Bundle/Application/73335472-A448-4367-B0E5-1607F438F81D/DamnVulnerableIOSApp.app
/Containers/Data/Application/8722EAC6-06EC-4665-A854-24DBCB5D1FD6/Library/Caches
/Containers/Data/Application/8722EAC6-06EC-4665-A854-24DBCB5D1FD6/Documents
/Containers/Data/Application/8722EAC6-06EC-4665-A854-24DBCB5D1FD6/Library
(iPhone: 16.4.1) [usb] # cd /var/mobile/Containers/Data/Application/8722EAC6-06EC-4665-A854-24DBCB5D1FD6/Library/Caches
(iPhone: 16.4.1) [usb] # cd com.highaltitudehacks.dvia
(iPhone: 16.4.1) [usb] # ls
action          Read  Write  Owner           Group        Size   Creation
-----          ----  ----  -----           -----        ---   -----
ilFirstUserAuthentication  True   True   mobile (501)  mobile (501)  128.0 B  2023-08-13 13:54:59
ilFirstUserAuthentication  True   True   mobile (501)  mobile (501)  64.0 B   2023-08-13 13:54:59
ilFirstUserAuthentication  True   True   mobile (501)  mobile (501)  48.0 KiB 2023-08-13 12:42:57
ilFirstUserAuthentication  True   True   mobile (501)  mobile (501)  0.0 B   2023-08-13 12:42:57
ilFirstUserAuthentication  True   True   mobile (501)  mobile (501)  32.0 KiB 2023-08-13 12:42:57
```



Kishor balan

iOS Pentesting Series Part 2- Into The Battlefield..

Hola Peeps,

6 min read · Aug 14, 2023



44



2



...

```

on="1.0" encoding="utf-8"?>
<security-config>
<-config>
<main includeSubdomains="true">example.com</domain>
<!-- set expiration="2018-01-01">
<pin digest="SHA-256">7HIpactkIAq2Y49orF00QKurWxmmSFZhBCoQYcRhJ3
<!-- backup pin -->
<pin digest="SHA-256">fwza0LRMXouZHRC8Ei+4PyuldPDcf3UKg0/04cDM1d
</in-set>
</config>
<security-config>
```

 Kishor balan

It's all about Bypassing Android SSL Pinning and Intercepting Proxy Unaware applications.

Hola H3ckers,

6 min read · Nov 27, 2022

 243

 2


...

```

[lab] For command suggestions
com.highaltitudehacks.dvia on (iPhone: 16.4.1) [usb] # ios hooking generate simple JailbreakDetectionVC
var target = ObjC.classes.JailbreakDetectionVC;

Interceptor.attach(target['- isJailbroken'].implementation, {
  onEnter: function (args) {
    console.log('Entering - isJailbroken!');
  },
  onLeave: function (retval) {
    console.log('Leaving - isJailbroken!');
  },
});

Interceptor.attach(target['- readArticleTapped:'].implementation, {
  onEnter: function (args) {
    console.log('Entering - readArticleTapped:');
  },
  onLeave: function (retval) {
    console.log('Leaving - readArticleTapped:');
  },
});
```

 Kishor balan

iOS Pentesting Series Part 3- The Ceasefire

Hola mates,

7 min read · Aug 19, 2023

 22

...



```
Type help for options

Available devices:
0) Device(id="local", name="Local System", type='local')
1) Device(id="socket", name="Local Socket", type='remote')
```

 Kishor balan

My fav 7 methods for Bypassing Android Root detection

Hola H3ck3rs,

6 min read · Oct 16, 2022

 185

...

See all from Kishor balan

Recommended from Medium



 DianaOpanga

A beginners guide to using Frida to bypass root detection.

This is a simple use case to bypass root detection using Frida. For this example we have created a sample APK that has implemented root...

3 min read · Nov 28, 2023



 Sharat Kaikolamthuruthil

Configure XCode iOS Simulator + Burpsuite for pentesting on MacOs

Pre-requisites :-

1 min read · Feb 1, 2024



...

Lists



Apple's Vision Pro

7 stories · 65 saves



Tech & Tools

16 stories · 212 saves



Icon Design

36 stories · 284 saves



Interesting Design Topics

257 stories · 489 saves



 Chinmay Talad

Pass eJPT with Tryhackme Challenge Room

Below is the list of free Tryhackme rooms which will help you to pass the exam, The lists contains both walkthroughs and CTF challenges, I...

2 min read · Nov 22, 2023



...



Luxeedd

Mobile Pentest Dynamic Analysis - Hooking with Frida

Introduction

3 min read · Nov 22, 2023



...

Android





Sandeep Vishwakarma in InfoSec Write-ups

A step-by-step Android penetration testing guide for beginners

Greetings fellow hackers, my name is Sandy, Security Analyst and Bug bounty hunter.

18 min read · Nov 3, 2023

678

4



...



Shayan Ahmed Khan

Decrypting the Mystery of MedusaLocker

In this analysis, I will not cover the stage1 and stage2 of MedusaLocker which includes initial access using a maldoc and execution using a...

9 min read · Nov 13, 2023

8



...

See more recommendations