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

Kishor balan · Following
6 min read · Jan 14, 2023

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

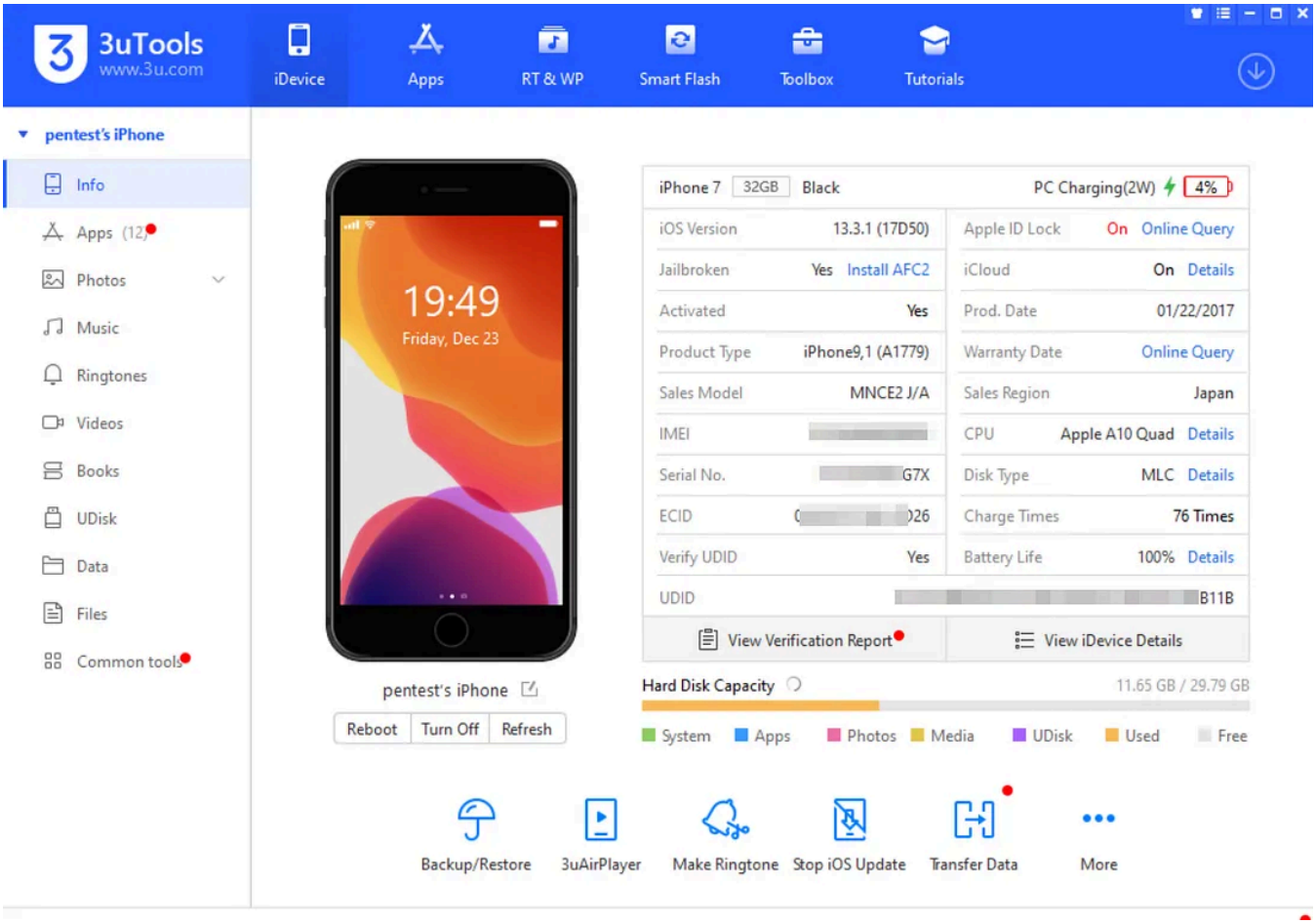
Releases · frida/frida (github.com)

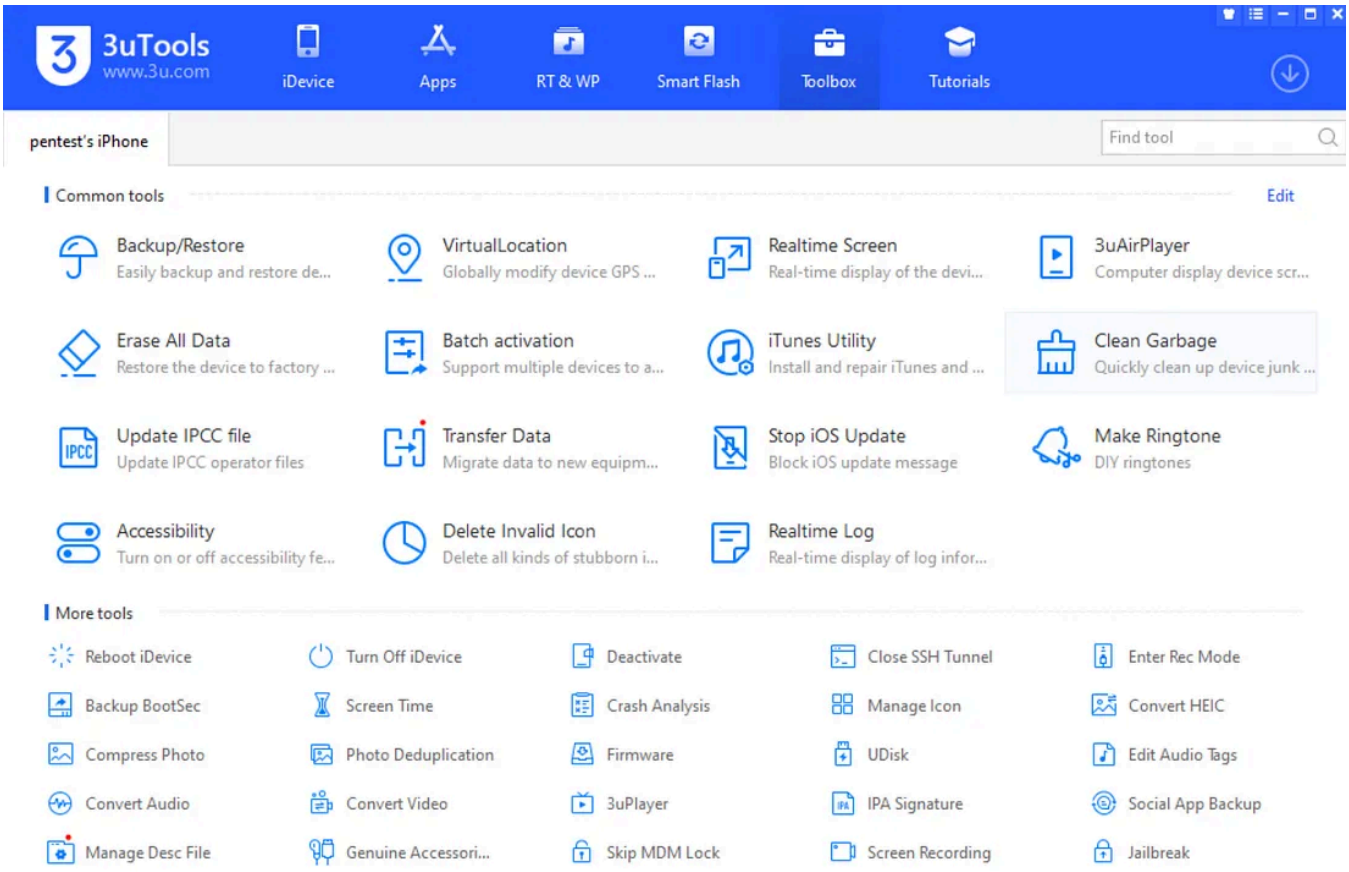
GitHub — sensepost/objection: 📱 objection — runtime mobile exploration

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

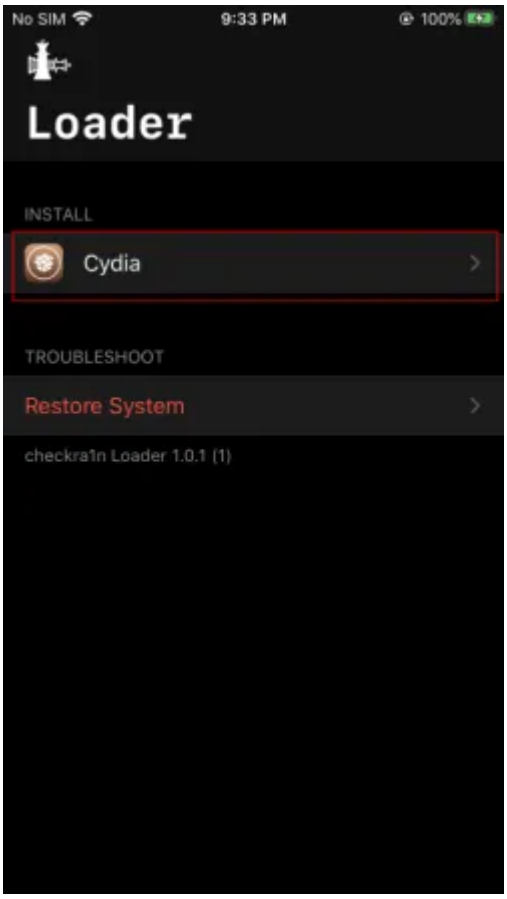




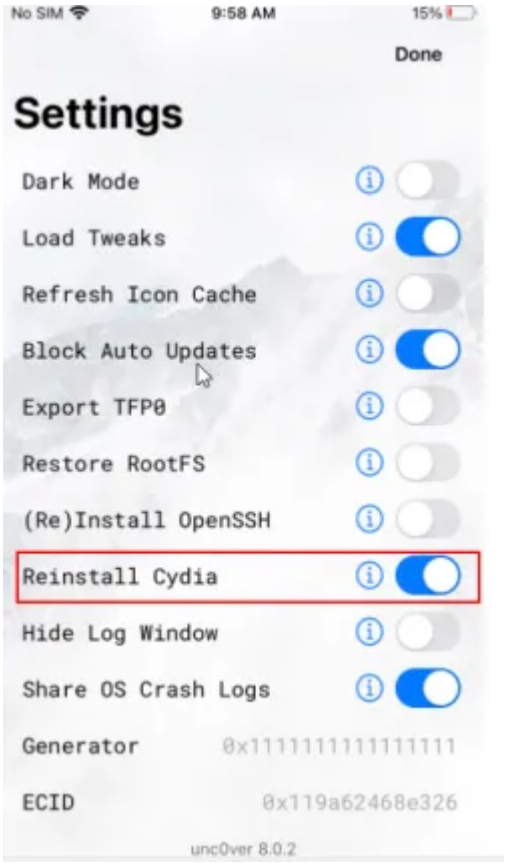
4: **Cydia Application:**- Basically, Cydia is a third-party application installer which is similar to the App Store and developed for the jailbroken iOS iDevices. If you are jailbreaking your device with Checkra1n or Uncover, The cydia app will automatically get installed into your device.

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.

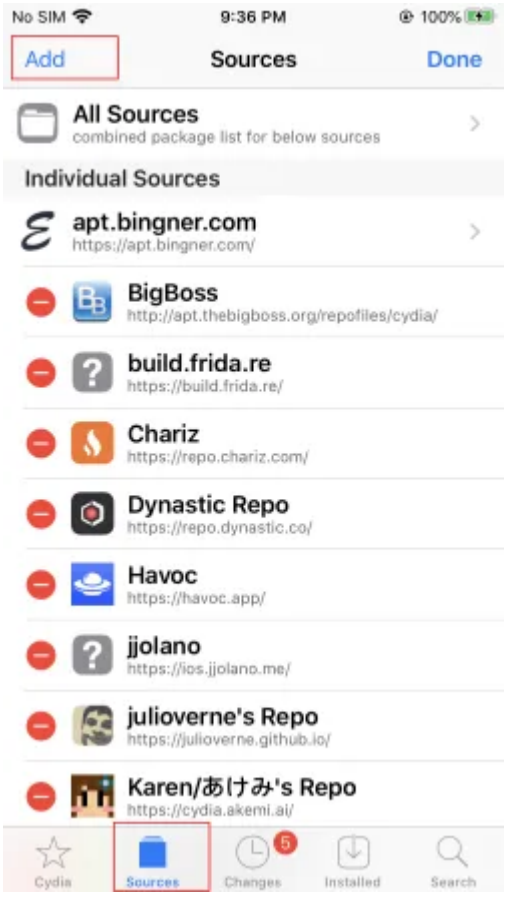


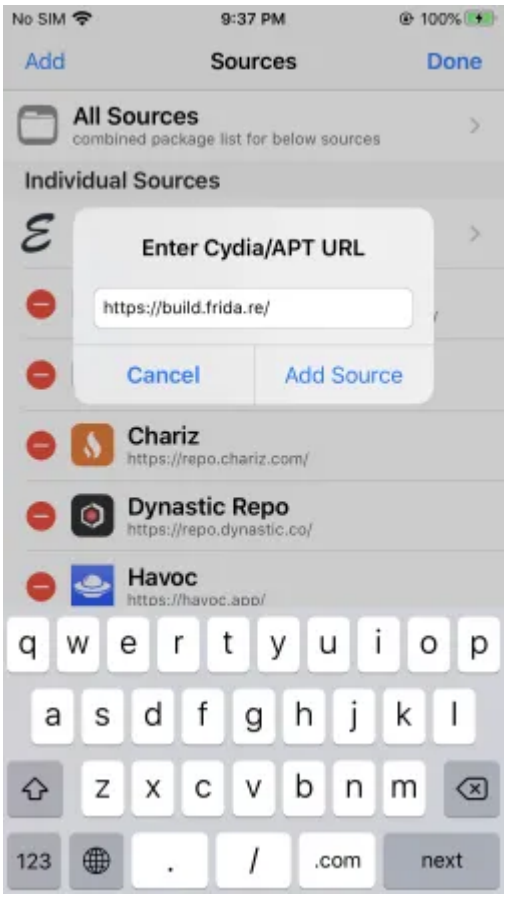
After the jailbreaking process, the Cydia app can be found in the device.

Method for installing Tweaks on the Jailbroken iOS device:

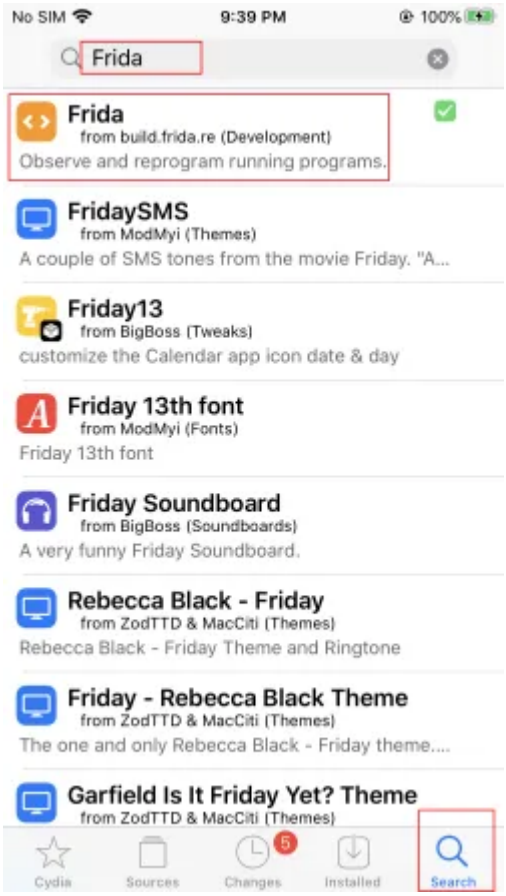
1: With the help of Cydia

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.

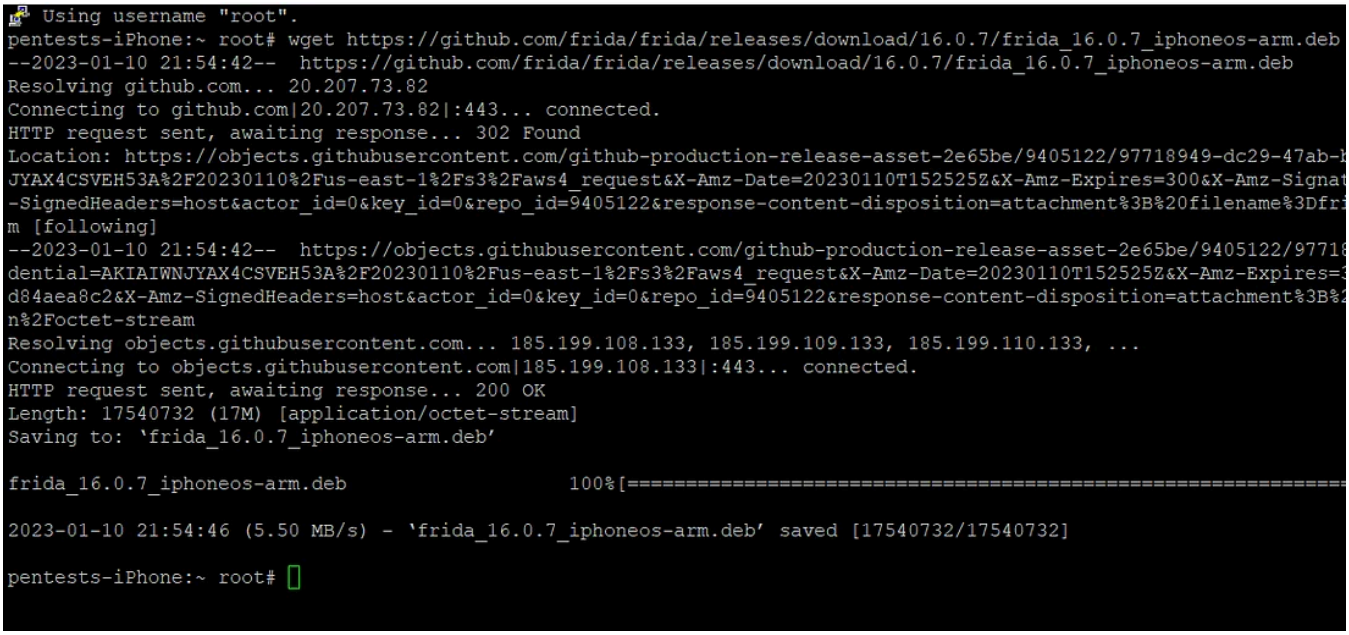
2: Direct method:

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

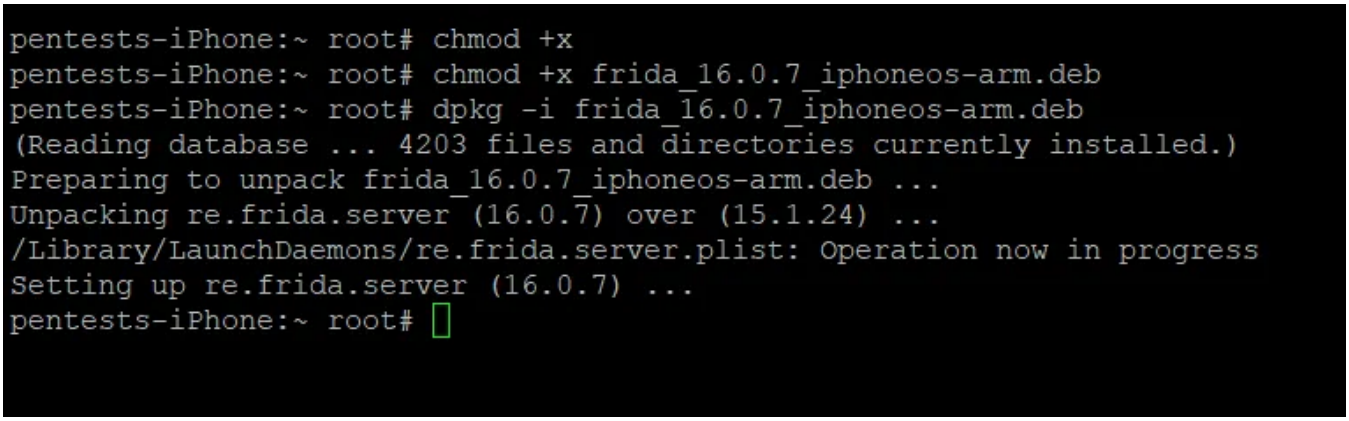
Step 1: Find the Tweak's deb file from its source.

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

Step 3: Download the deb file using wget



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



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:

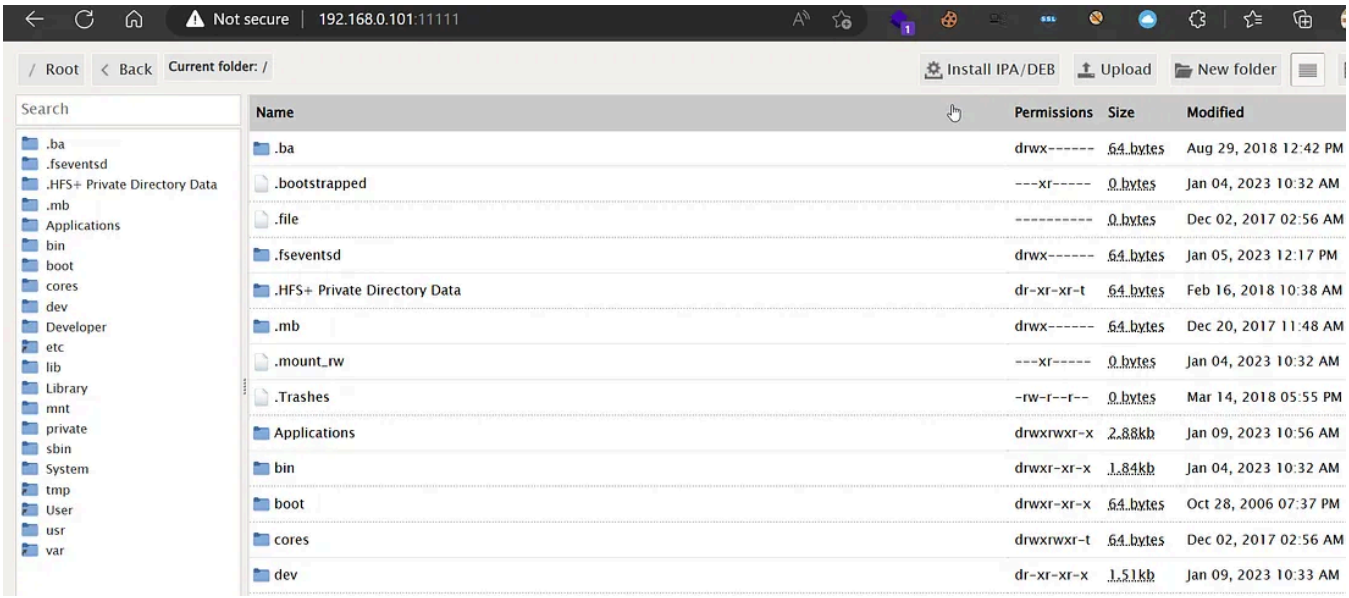
Tweaks are basically third party applications which can be used to outrun some sort of fences set up in the target iOS applications. A lot of tweaks are available but here I am listing out the necessary ones.

A: **Filza:**

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

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

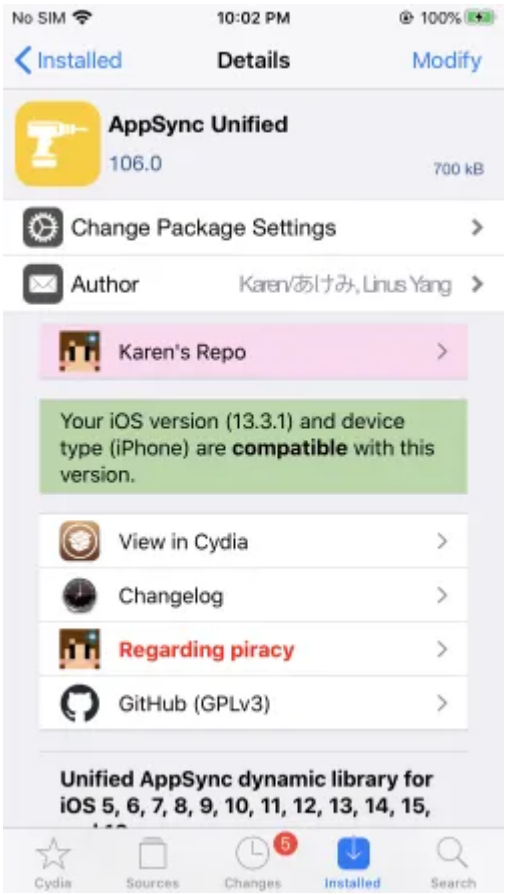
Filza also provides WebDav server so we can access the application on our other local machines.



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/

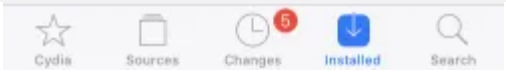
This one can be used to install/Backup IPA files directly to our jailbroken iOS device.

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.

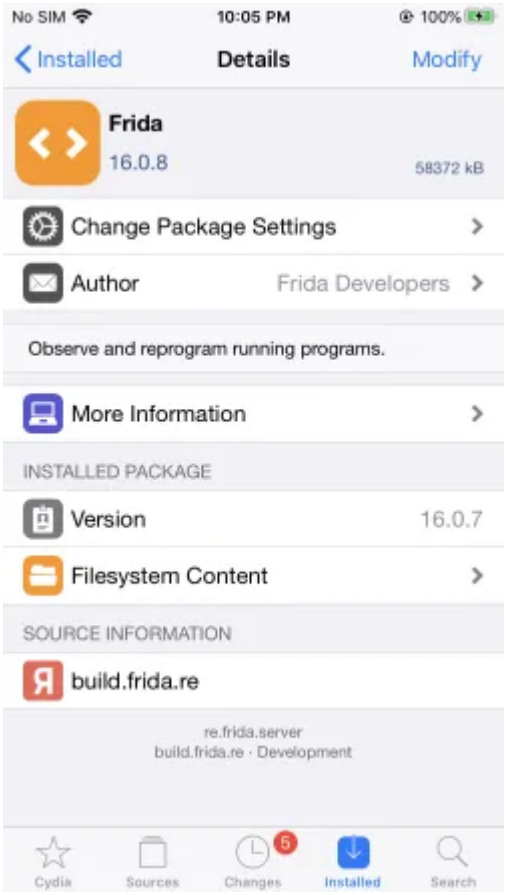
Root credential: — root: alpine



E: Frida

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

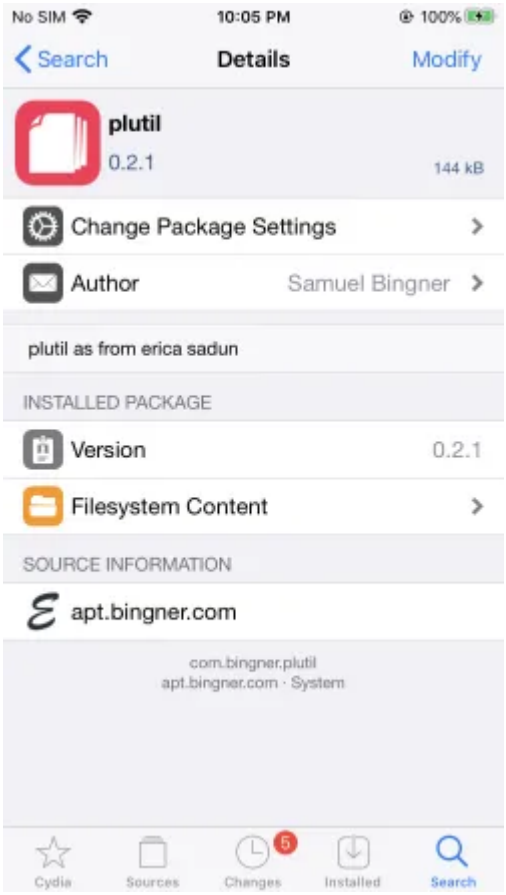
To work with frida tools, a frida server must be installed on our iOS device.



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

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

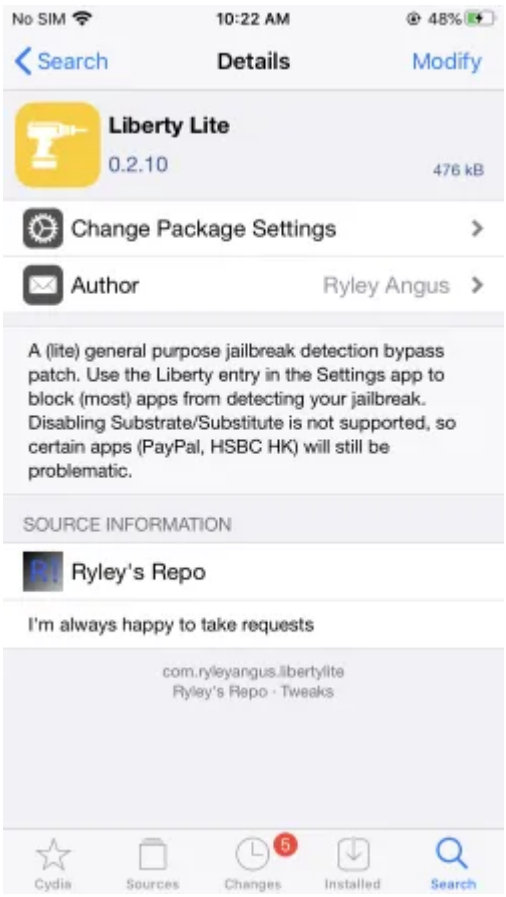
```
pentests-iPhone:~ root# fsmon
FSE_XATTR_MODIFIED      38      "logd"  /private/var/db/diagnostics/Persist/000000000000026f.tracev3
FSE_XATTR_MODIFIED      38      "logd"  /private/var/db/diagnostics/Special/0000000000000131.tracev3
FSE_XATTR_MODIFIED      38      "logd"  /private/var/db/diagnostics/Persist/000000000000026f.tracev3
FSE_XATTR_MODIFIED      38      "logd"  /private/var/db/diagnostics/Persist/000000000000026f.tracev3
FSE_XATTR_MODIFIED      38      "logd"  /private/var/db/diagnostics/Signpost/0000000000000025.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.2ZlLT6
FSE_DELETE      6126    "Cydia" /private/var/tmp/clearsigned.message.2ZlLT6
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.pli
FSE_CHOWN       100     "cfprefsd"      /private/var/mobile/Library/Preferences/com.apple.sharingd.pli
FSE_CHOWN       100     "cfprefsd"      /private/var/mobile/Library/Preferences/com.apple.sharingd.pli
FSE_XATTR_MODIFIED      38      "logd"  /private/var/db/diagnostics/Persist/000000000000026f.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
```

Tweaks for Bypassing Jailbreak detection:

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

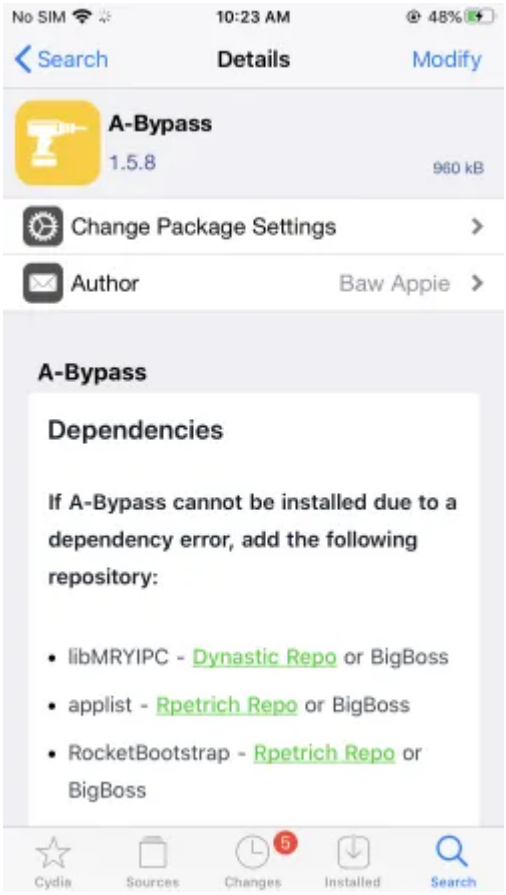
A: Liberty Lite

Repo: https://ryleyangus.com/repo/



B: A-Bypass

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

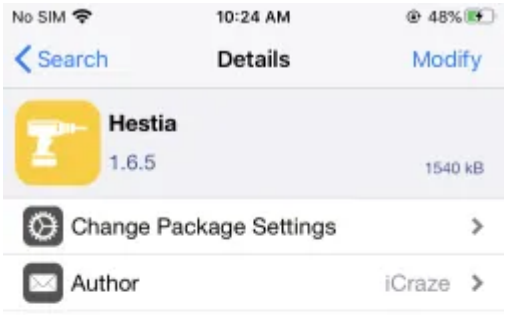


C: HideJB

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

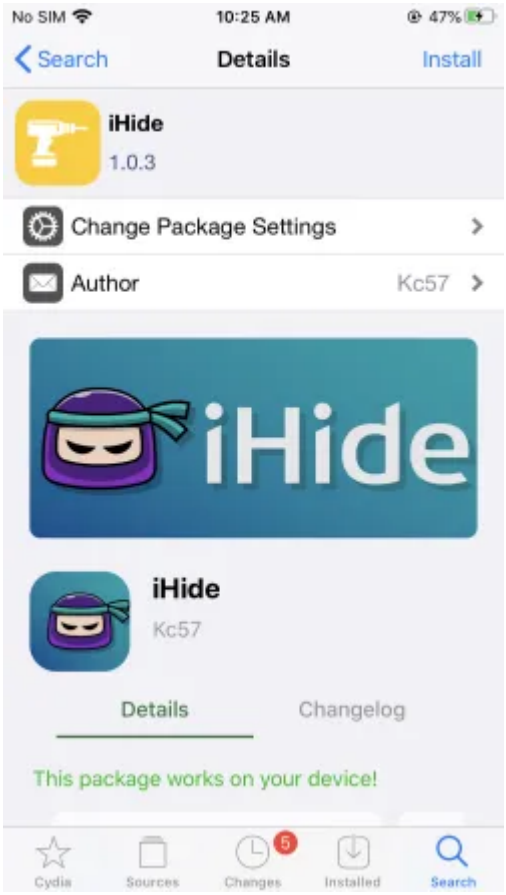
D: Hestia

Repo: https://havoc.app/



E: iHide

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



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

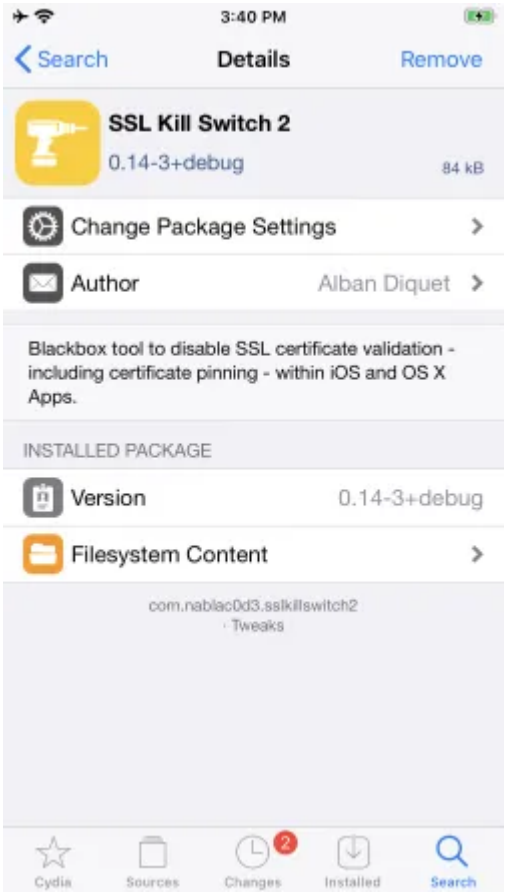
Frida CodeShare

Tweaks for Bypassing SSL Pinning Bypass:

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

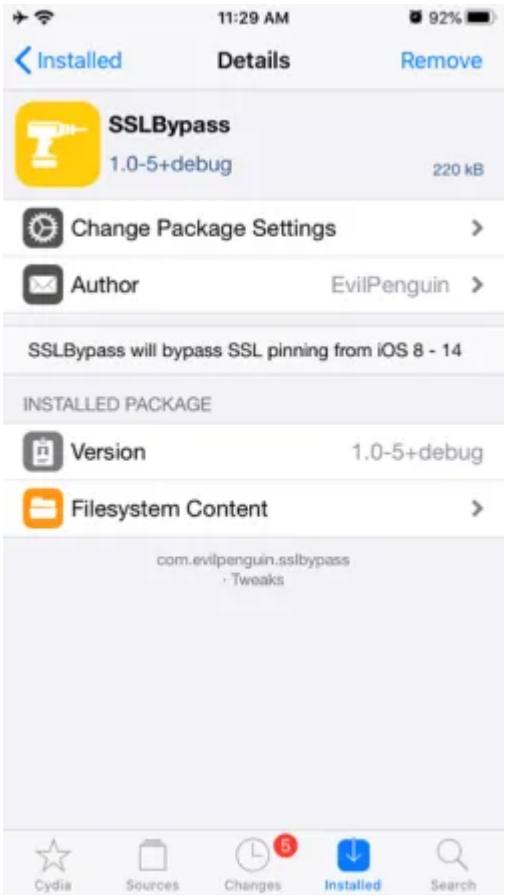
A: **SSL Kill Switch**

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



B: SSLBypass

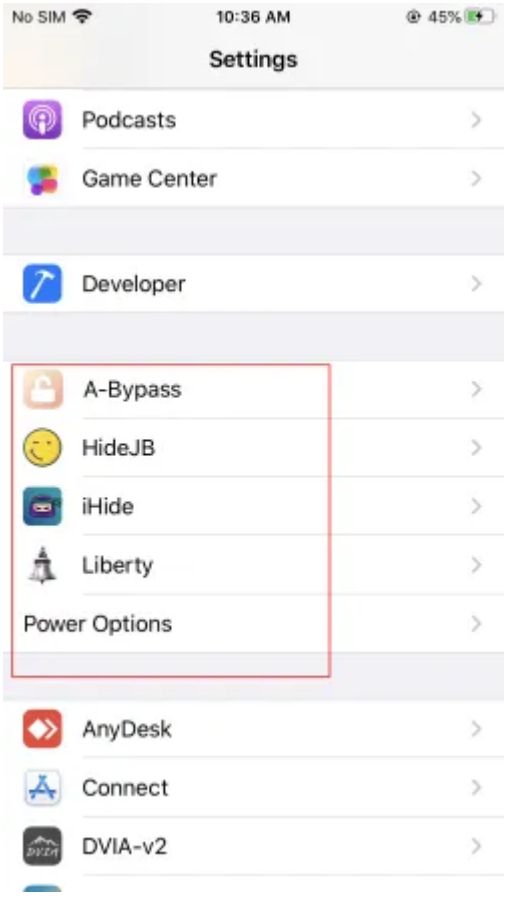
Repo: SSLBypass/packages at main · evilpenguin/SSLBypass · GitHub



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 :)

IOS Pentest Hacking Mobile

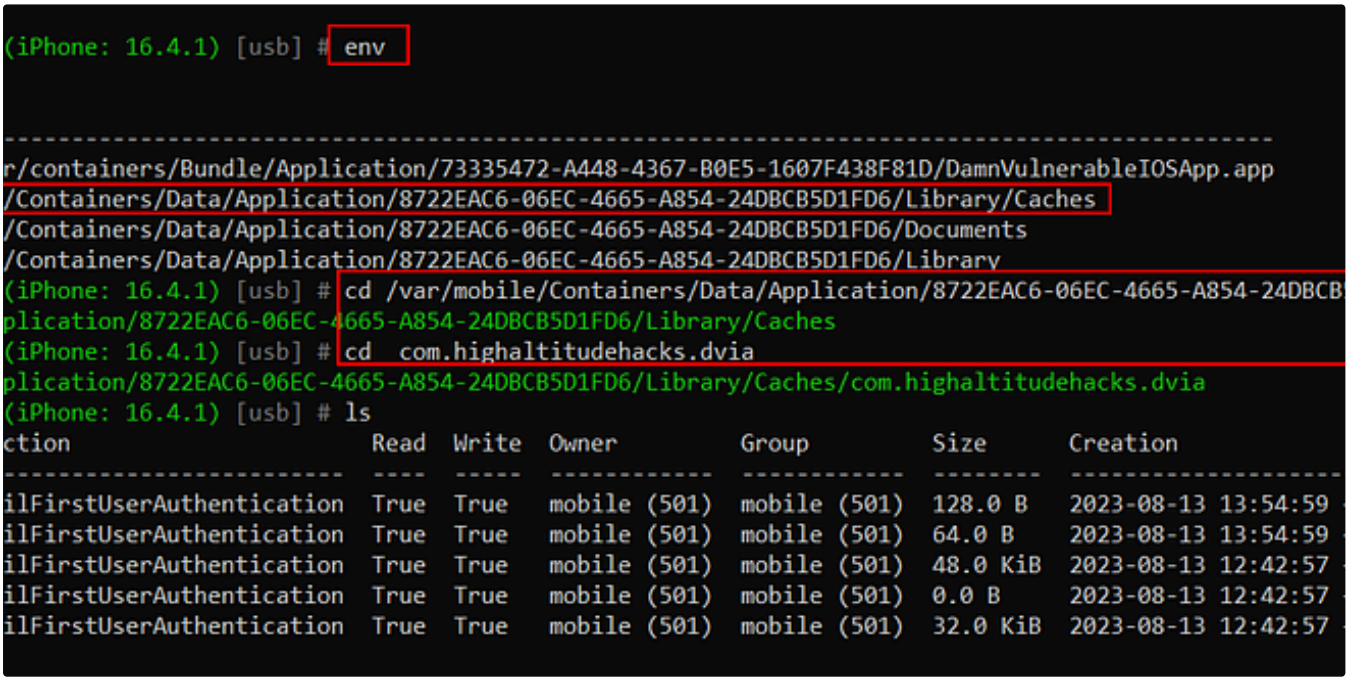
Following

Written by Kishor balan

418 Followers

Security Analyst || eWPTXv2 || eJPT

More from Kishor balan



Kishor balan

iOS Pentesting Series Part 2- Into The Battlefield..

Hola Peeps,

6 min read · Aug 14, 2023

44 2

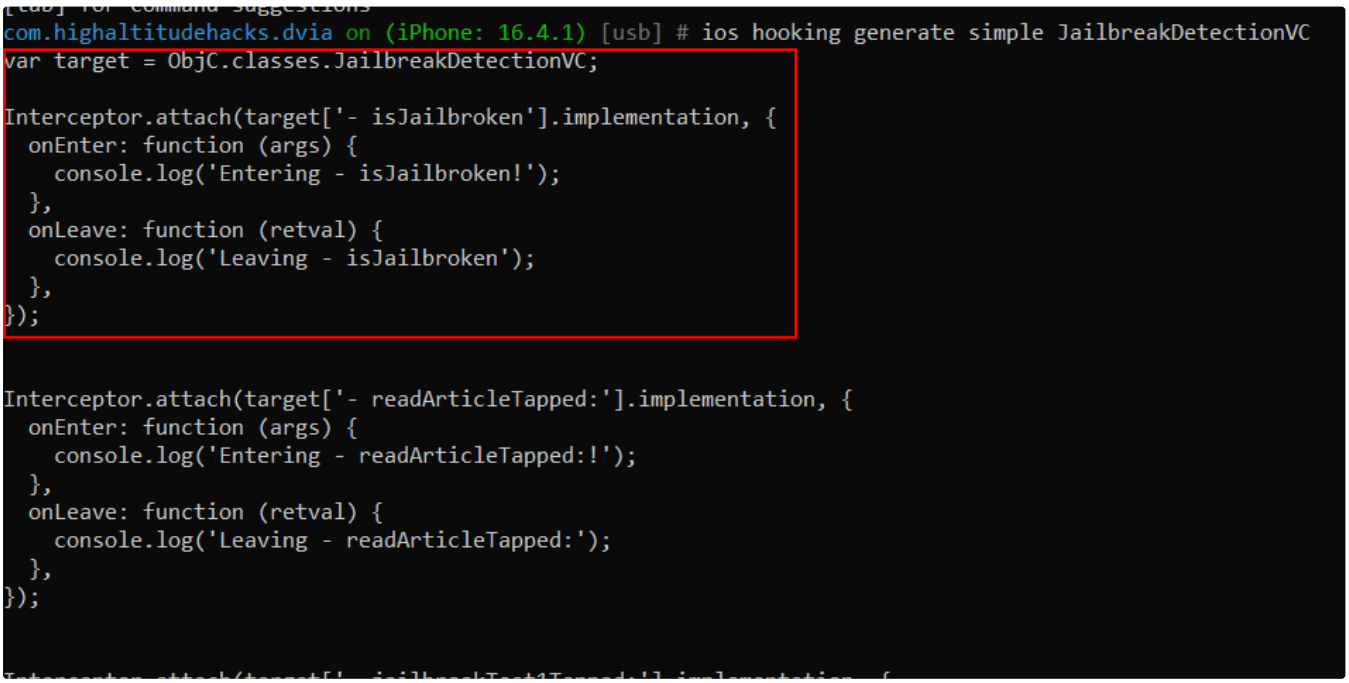
Kishor balan

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

Hola H3ckers,

6 min read · Nov 27, 2022

243 2



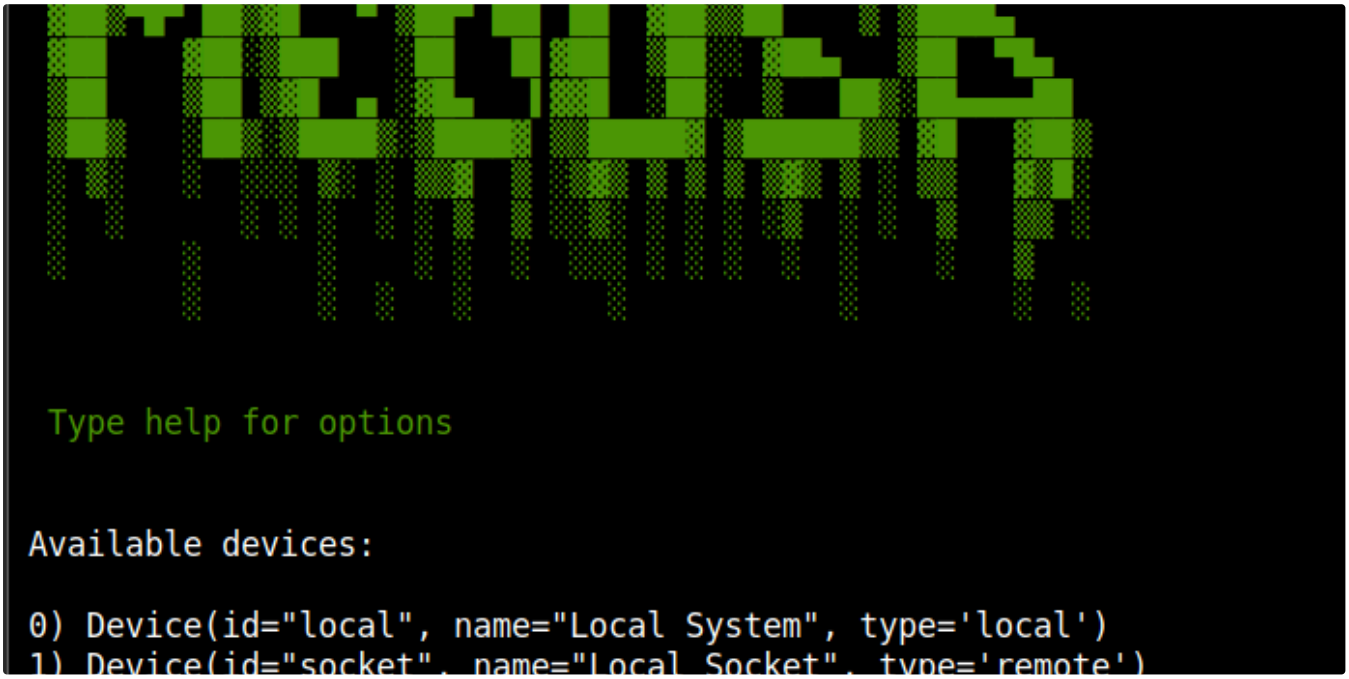
Kishor balan

iOS Pentesting Series Part 3- The Ceasefire

Hola mates,

7 min read · Aug 19, 2023

22



Kishor balan

My fav 7 methods for Bypassing Android Root detection

Hola H3ck3rs,

6 min read · Oct 16, 2022

185 2

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 :-

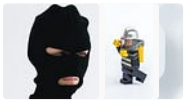
1 min read · Feb 1, 2024

2

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

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