Jailbreaking iOS 15 to 16

Hi fellows, many of you are looking to jailbreak the iPhone running on 15 or 16 latest up to the date. Here are few simple steps you need to follow for a successful jailbreak. I will try to make it as simple as it can be possible. Feel free to contact me on my Linkedin profile given below.

linkedin.com/in/markhor

Muhammad Shoaib

# Step 1

Download latest release of Palera1n from this link <https://github.com/palera1n/palera1n/releases>.

Download balena etcher latest from this link: <https://github.com/balena-io/etcher/releases>

Palera1n ISO file by the architecture of amd.

**Note**: you will need a flash drive (at least 16b)

Only phone with till **A11** bionic chip is supported for this guide.

# Step 2

After downloading the files mentioned above you need to insert the flash drive into the laptop.

Open the balena etcher select the palera1n iso file

In next step you need to select the flash drive inserted.

Then select the option flash and wait for few seconds to complete the flashing process.

Now your Flash drive is bootable image of Palera1n.

Reboot the laptop and get into boot menu.

Select your Flash drive as your bootable drive.

# Step 3

You have to remove screen passcode from your iPhone.

Once Flash drive is loaded you have to select the switch option to select the type of jailbreak you wanted to perform.

After that, select option from where you can choose between Bind and Fake fs. Use spacebar to select the options.

Next step will be selecting Palera1n > Start

Connect your iPhone with USB cable into your laptop system.

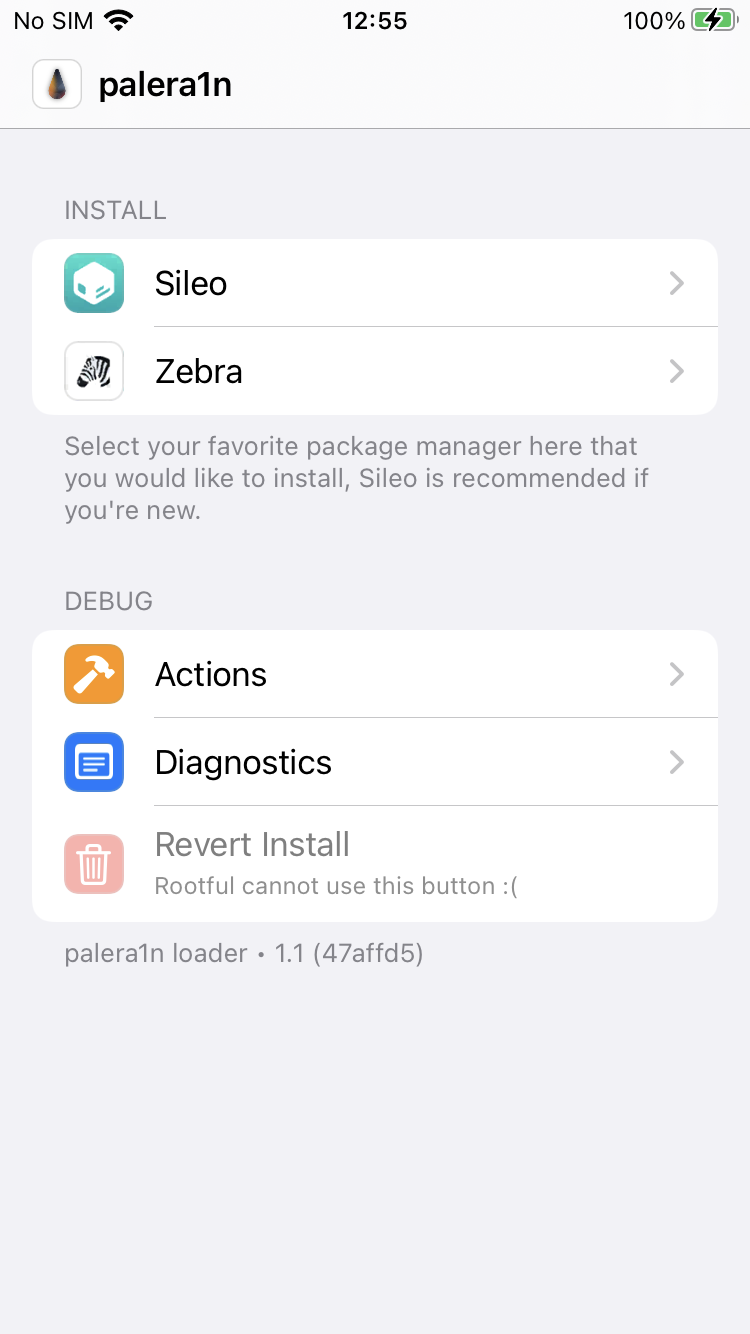
Once detected iPhone will pop up notification. Select Trust option.

After this your phone will boot into the DFU Mode. Its also known as Recovery mode.

You need to follow the instruction mentioned on the screen to put your phone into Recovery mode manually once. Don’t worry if your phone restarts multiple times during this process.

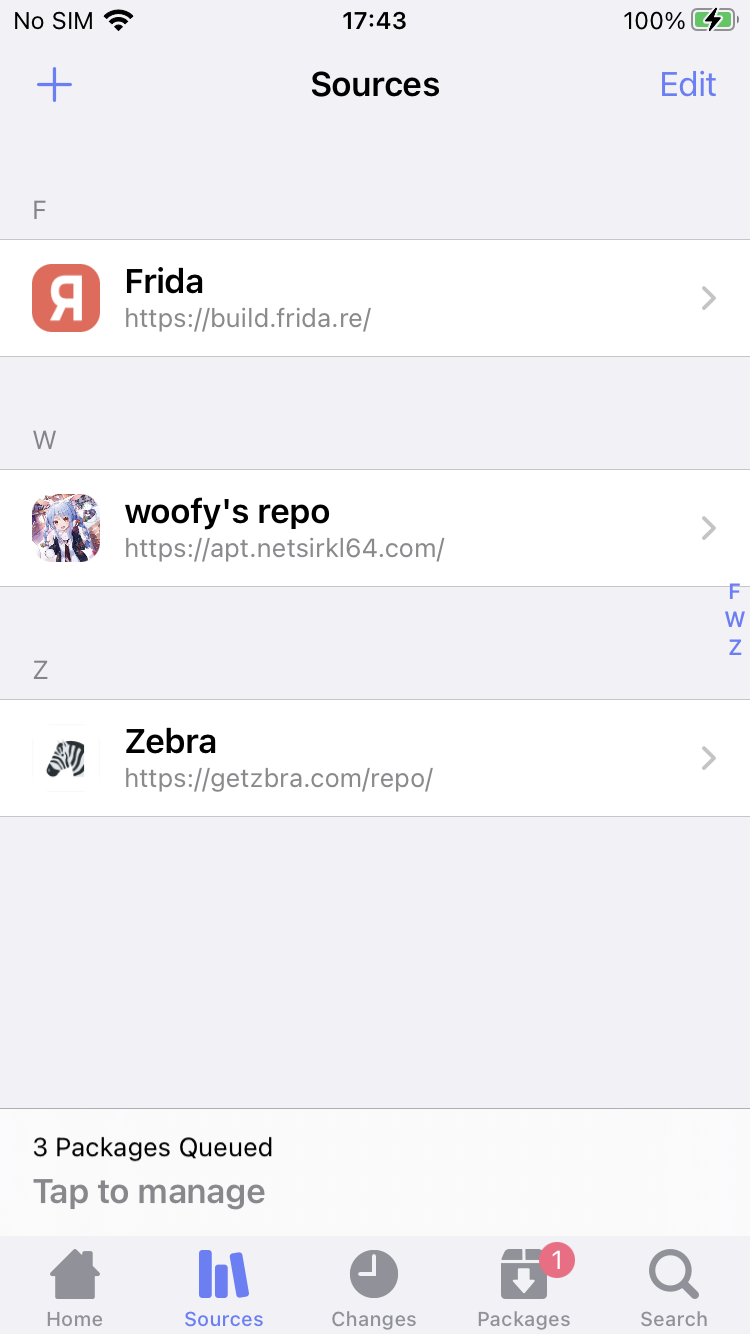
Once the process is completed your phone will boot into normal mode automatically.

You have to wait for 1o seconds to Palera1n app to appear on the home screen.



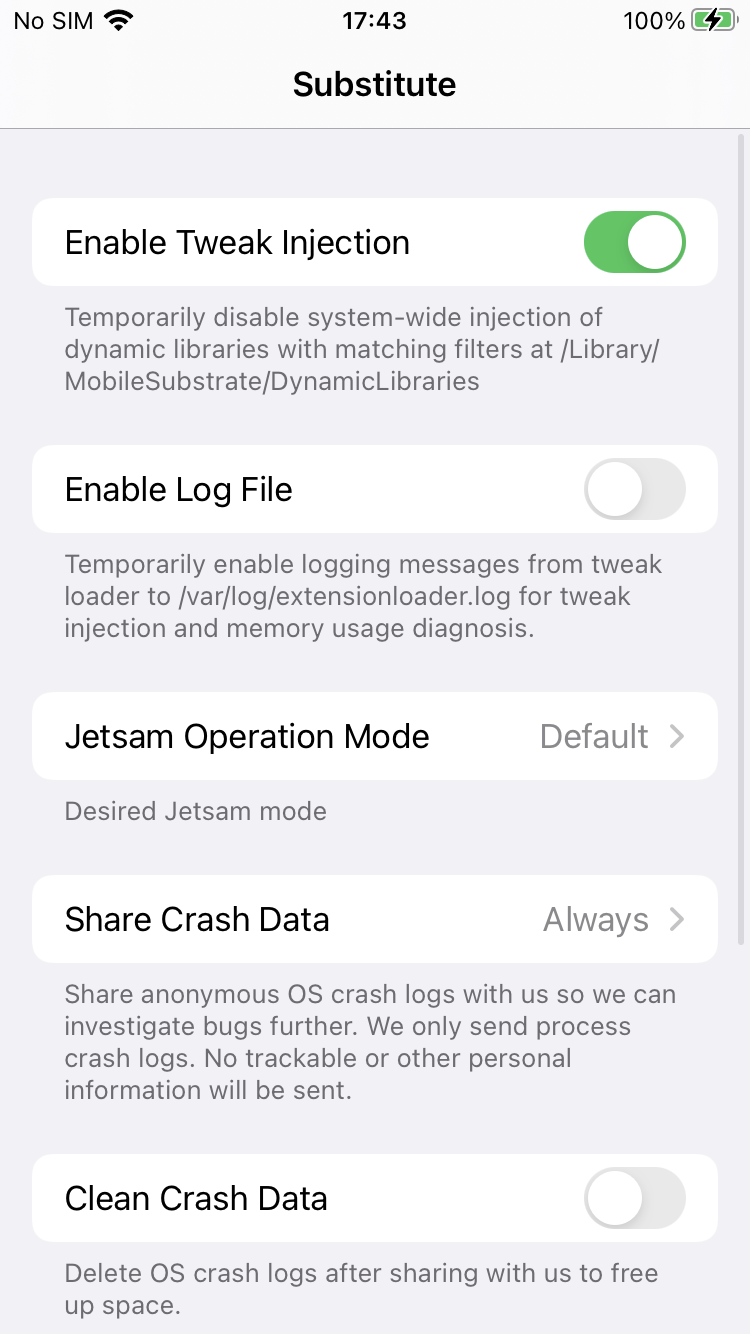
Figure

Open the Palera1n app and select Sileo or zebra as per your choice to install.



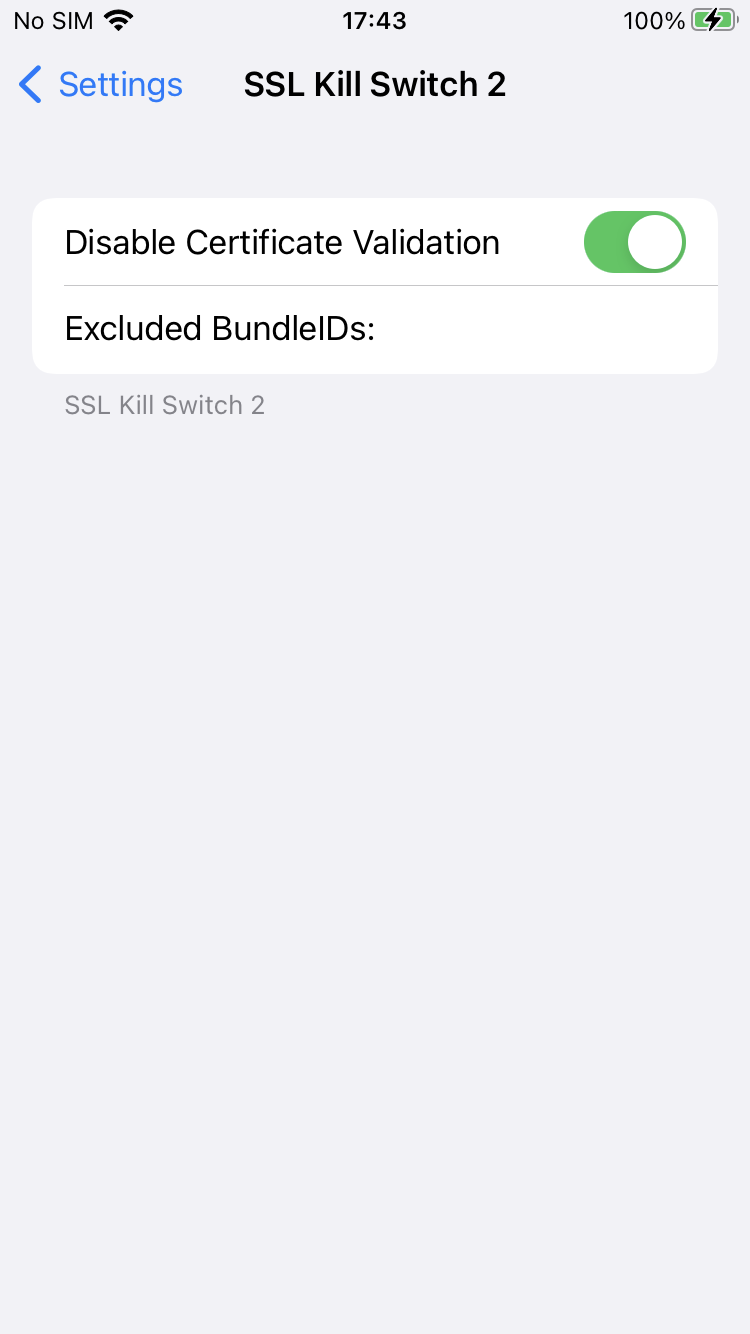
Figure

Once install you need to update the sileo or zebra.



Figure

I have installed the SSL Kill Switch 2 for successful SSL Bypass



Figure

Now your iPhone is jailbroken. Happy Hacking!

For SSL Kill Switch I will be writing another guide and on How to fetch IPA from iDevice. Stay tuned!!