BYPASS SSL PINNING MENGGUNAKAN FRIDA

EASTY TO LEARN

AMINUDIN

REQUIREMENTS

Rooted Devices/Emultaor

disini saya menggunakan genymotion,
bisa kalian download di https://www.genymotion.com/fun-zone/

Python & Frida Packages

kalian bisa download python disini, https://www.python.org/.
Dan install frida packages dengan command dibawah

```
python -m pip install Frida
python -m pip install objection
python -m pip install frida-tools


or


pip install Frida
pip install objection
pip install frida-tools
```

Platform Tools (adb)

bisa kalian cari di google untuk linknya.

Injection Script

nanti akan saya share script injectionnya

LANGKAH LANGKAH

1. check device konek dengan 'adb devices'
2. check arch dari devices/emulator android kalian dengan command 'adb shell getprop ro.product.cpu.abi'
3. download frida server dari https://github.com/frida/frida/releases/ sesuai dengan arch nya misal 86/64
4. install aplikasi target pada devices/emulator
5. setelah download frida server silahkan extract lalu push frida servernya ke devices/emulator kalian dengan cara 'adb push *./frida-server-12.4.7-android-x86 /data/local/tmp'*
6. lalu kasih permission ke frida server agar bisa di exec dengan command 'adb shell "chmod 777 /data/local/tmp/frida-server-12.4.7-android-x86"'
7. Generate proxy CA Certificate dari genymotion, lalu push ke android devices dengan nama 'cert-der.crt', dengan command adb push namacert.der /data/local/tmp/cert-der.crt
8. lalu push frida script injectionnya ke devices dengan command adb push ./fridascript.js /data/local/tmp
9. lalu jalankan frida server pada devices android dengan command adb shell /data/local/tmp/*frida-server-12.4.7-android-x86 &*
10. kalau sudah sekarang kita cari nama package target aplikasi yang mau kita bypass dengan command frida-ps -U
11. lalu kita jalankan command berikut ini frida -U -f com.package-target -l D:\frida\fridascript.js --no-paus
12. kalau sudah berhasil kita check dan coba untuk sniffing lagi