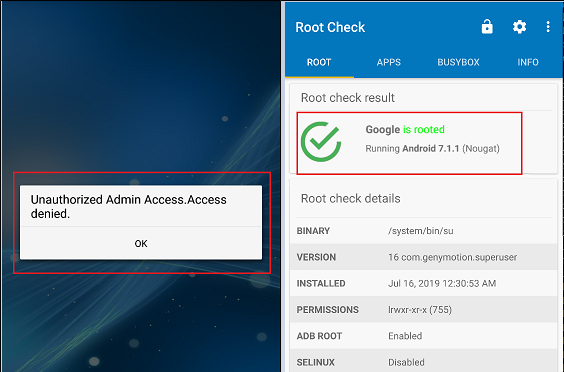
**Root detection bypass using Frida**

First try to install and use app on rooted device. If Root detection is implemented then App will not accessible on rooted device.



Follow below steps to bypassing Root detection using Frida.

1. Install Frida and Frida tools

pip install Frida

pip install frida-tools



2. Download adb platform tools if not installed on your computer.

3. Download Frida injection script(root\_bypass.js) for root bypass.

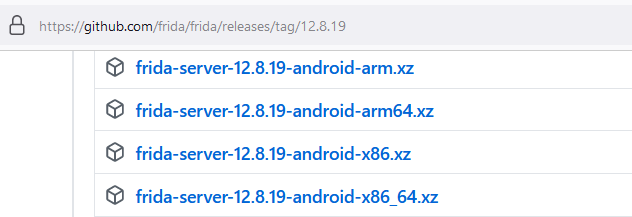
<https://gist.github.com/pich4ya/0b2a8592d3c8d5df9c34b8d185d2ea35>

4. Connect your device using below adb command

adb connect <ip of device:port>

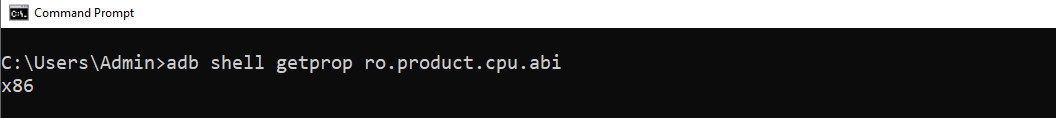
5.Download Frida’s server for supported android device’s arch version form below link

<https://github.com/frida/frida/releases/>



6. To find out arch version of device use below command

adb shell getprop ro.product.cpu.abi



7. Push frida-server into device using below command

adb push <path of frida-server folder><space></data/local/tmp>



8. Give permissions to frida-server using below command

adb shell chmod 777 /data/local/tmp/frida-server



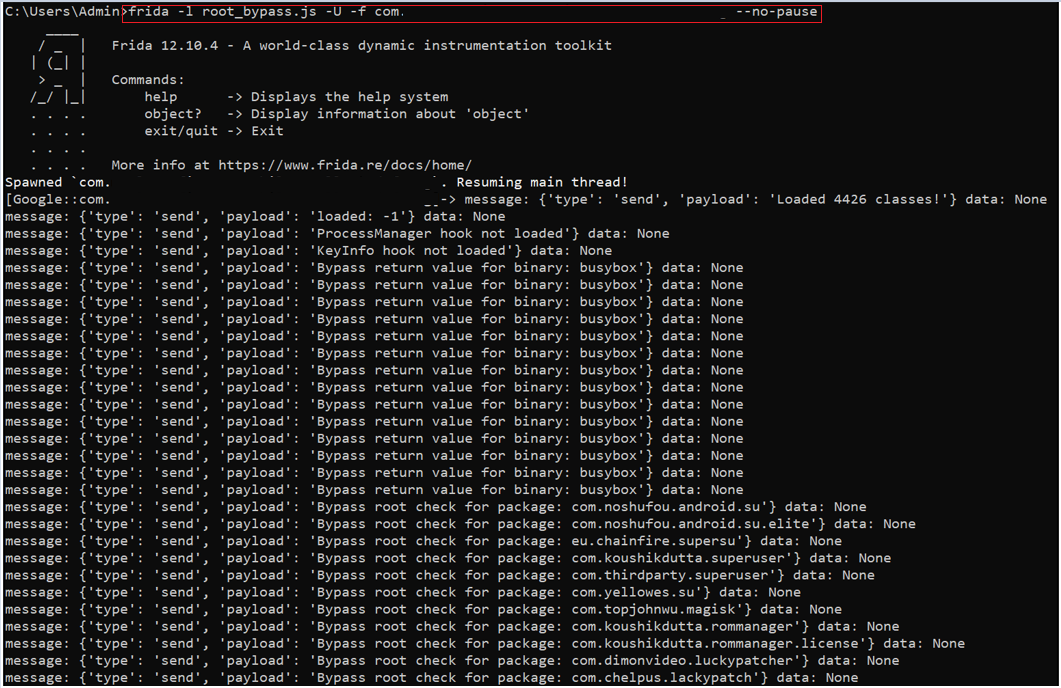
9. Check and start frida server in device using below command

adb shell /data/local/tmp/frida-server &



10. Hook target application with **root\_bypass.js** script by using below command

frida -l <path\_to\_root\_bypass.js\_onyourpcr> -U -f <application\_package\_name> --no-pause



11. Following screenshot shows that we are able to bypass root detection and now are app is accessible on rooted device

