Day 4

Exploitation Analyst

Hacking the SSL Network protocol:

Android SSL Pinning Bypass

YouTube video: (https://youtu.be/_7J5HrwIr0k?si=uMctNDHpYltf43EZ)

Objective: To bypass the Android SSL pinning.

Tools required:

1. Frida (https://github.com/frida)
2. Frida Codeshare scripts (https://codeshare.frida.re/@akabe1/frida-multiple-unpinning/)
3. Android device (say Android studio)
4. Adb platform tools (https://developer.android.com/tools/releases/platform-tools)

Steps:

First confirm that Frida is recognising the android device:

```
ohit@Rohits-MacBook-Pro platform-tools % adb devices
ist of devices attached
mulator-5554   device

ohit@Rohits-MacBook-Pro platform-tools %
```

Now, we will do the SSH on the emulator as shown below: This will give the file structure as well

```
rohit@Rohits-MacBook-Pro platform-tools % adb shell
emu64x:/ # ls
acct       bugreports  data          etc             lost+found  odm_dlkm     product                sys          vendor
adb_keys   cache       data_mirror   init            metadata    oem          sdcard                 system       vendor_dlkm
apex       config      debug_ramdisk init.environ.rc mnt         postinstall  second_stage_resources system_dlkm
bin        d           dev           linkerconfig    odm         proc         storage                system_ext
emu64x:/ #
```

In another tab we are pushing the Frida server in the emulator:

```
rohit@Rohits-MacBook-Pro platform-tools % adb push frida-server-x86 /data/local/tmp/frida-new-server
frida-server-x86: 1 file pushed, 0 skipped. 103.1 MB/s (53604060 bytes in 0.496s)
rohit@Rohits-MacBook-Pro platform-tools %
```

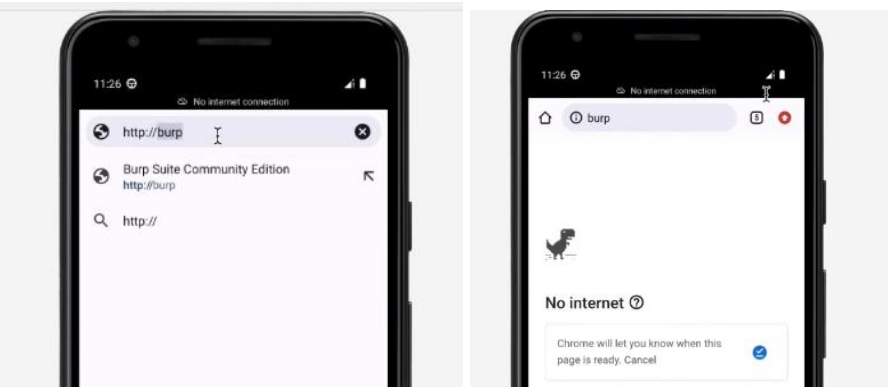
Now, verify that it is actually passed there or not: Yes it is there

```
emu64x:/ # cd /data/local/tmp
emu64x:/data/local/tmp # ls
frida-new-server  frida-server  re.frida.server
```

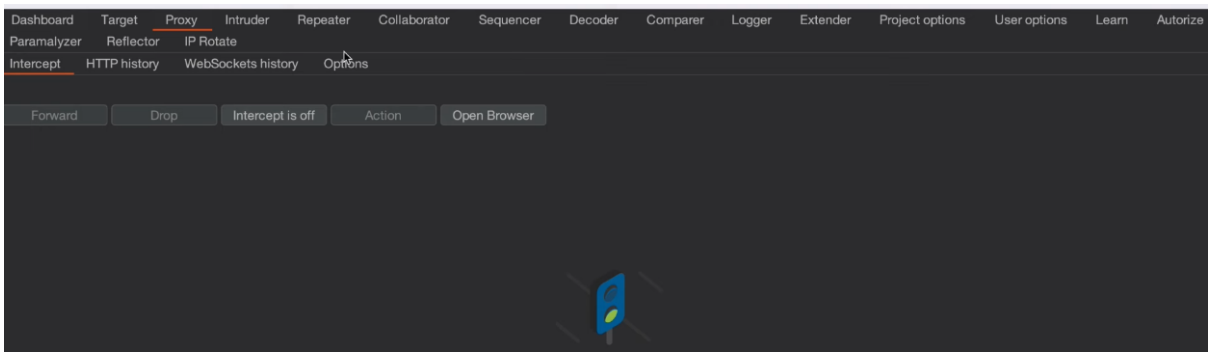
Now, give executable permission for this file to run and then execute the server file as well:

```
emu64x:/data/local/tmp # chmod +x frida
frida-new-server   frida-server
emu64x:/data/local/tmp # chmod +x frida-server
emu64x:/data/local/tmp # ./frid
frida-new-server   frida-server
emu64x:/data/local/tmp # ./frida-server
```

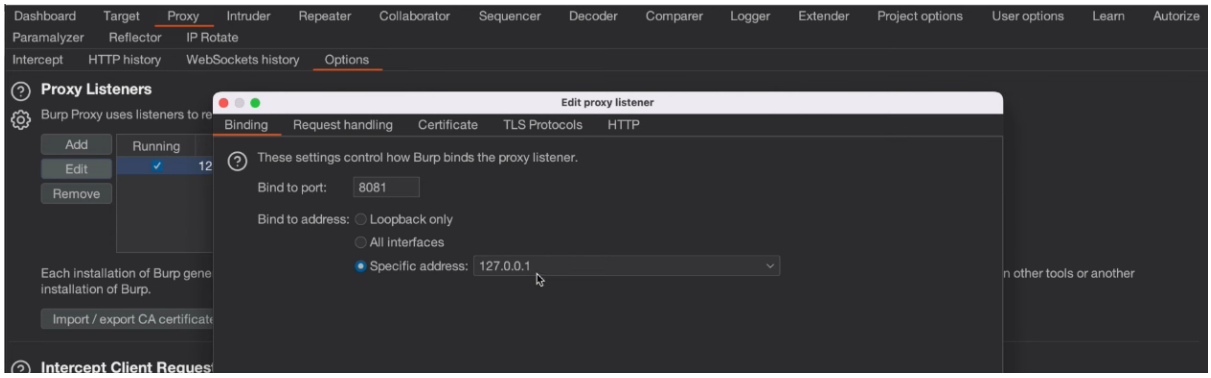
Now, keep it running and then go to the android device and confirm if the device is connected to the burp proxy or not: here it is not connected at this moment.



So, now we will configure it: Open burpsuite in the laptop

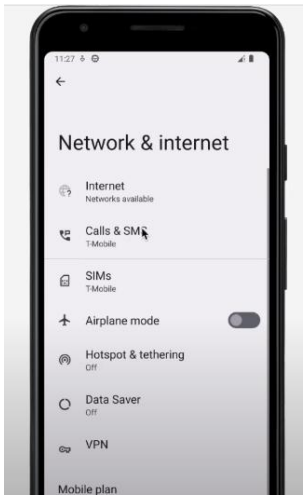


Go to the proxy setting option:

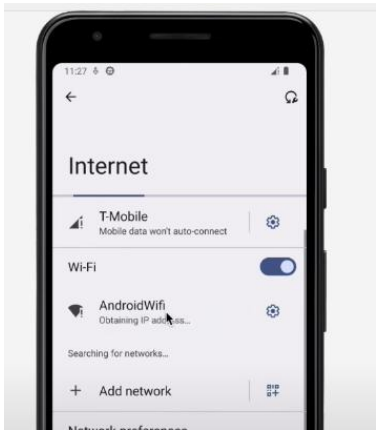


Click on the drop down menu at the specific address button, and then select the machine(your host) IP address.

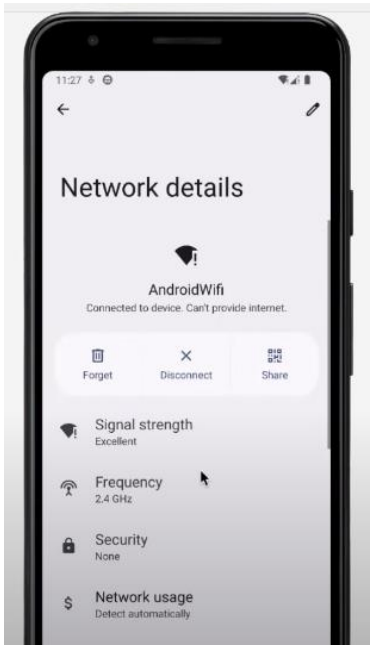
Now, go the settings in the android device: Click on the Network and Internet



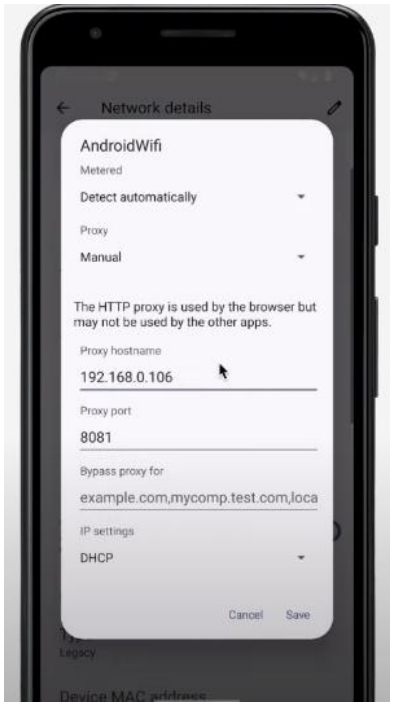
Then click on the ‘Internet’: Wifi will be available



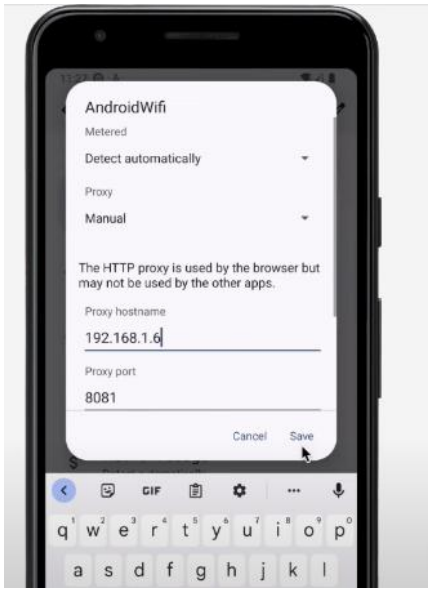
We will then change the setting of the wifi:



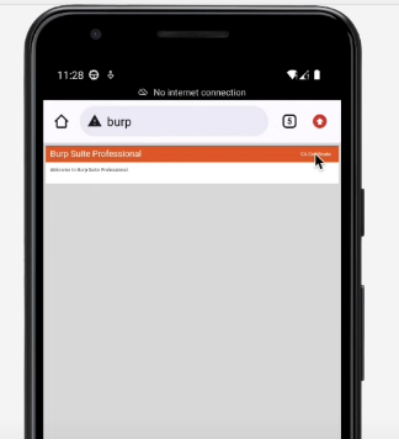
Click on the pen icon shown above: Following screen will appear



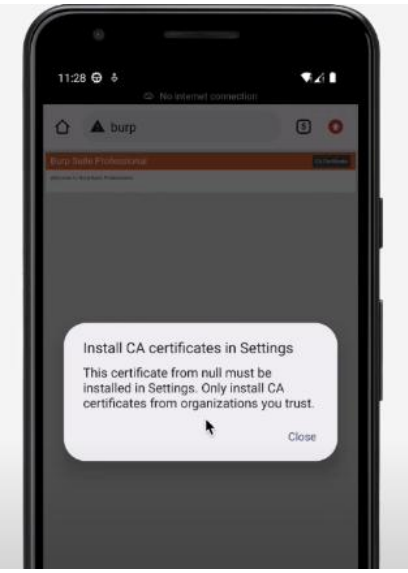
We will now change the settings as shown below: host name will be same as the one we did in the burpsuite, and also change the port number if required as per the burpsuite.



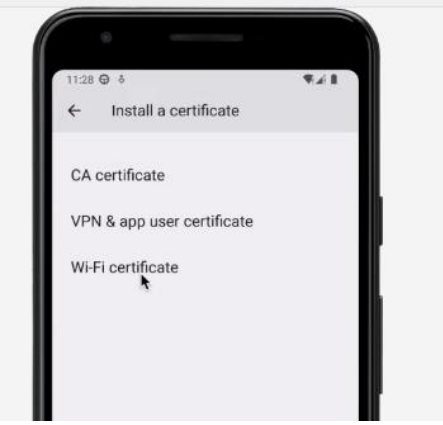
Then verify that the device is successfully connected to the burpsuite: Yes it is connected.



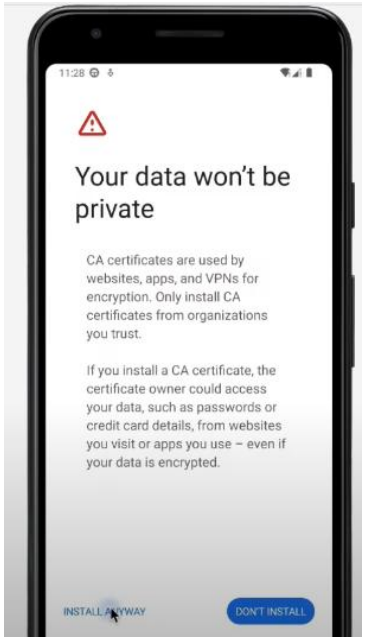
Now, click on the certificate at the top right corner and then, download the certificate:



Now, go to the mobile again and go to the settings in the mobile, and look for the CA certificate option:

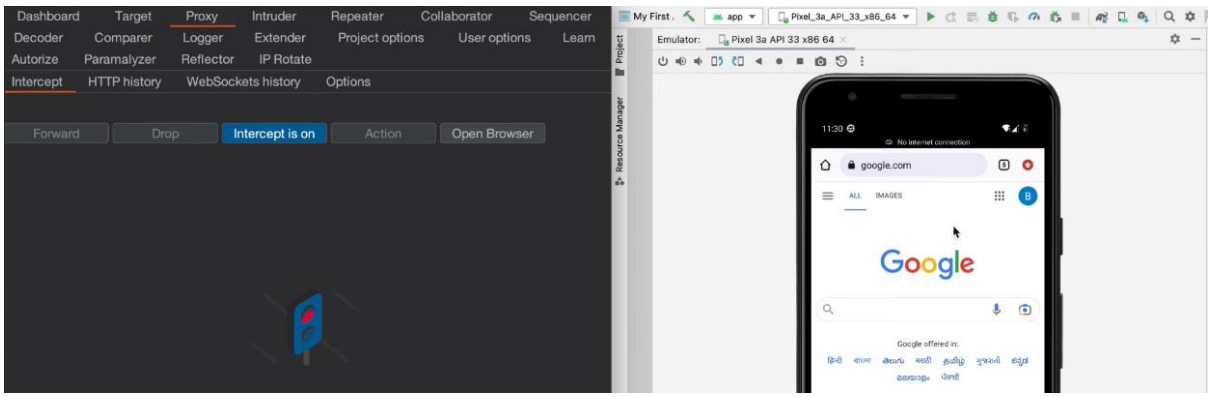


Click on the CA certificate: Then click on “Install anyway” option.

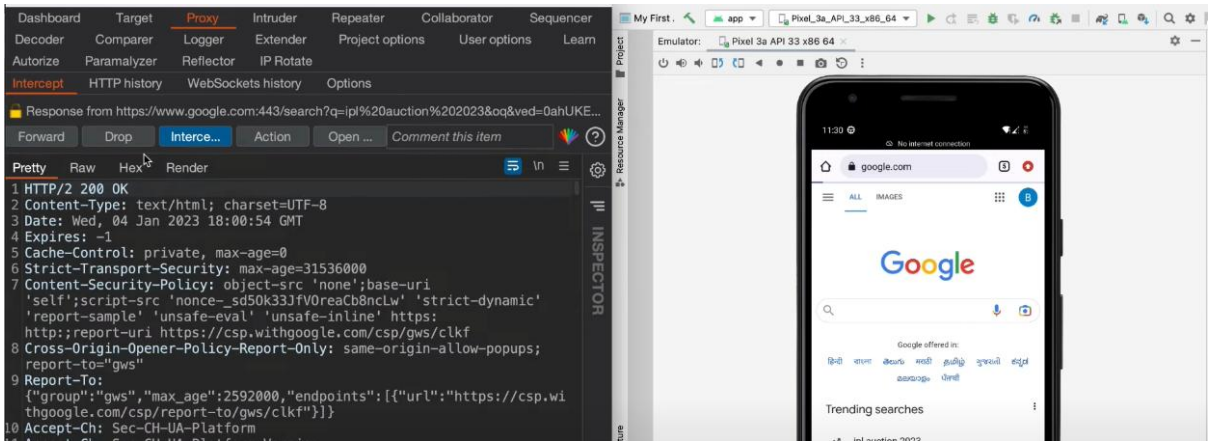


Select the certificate and it automatically get installed:

Now, we will open burpsuite and the android emulator too: First open the google, then make intercept on.



The moment I clicked on something in the browser, we will see in the burpsuite as well:



Now, clealry we are able to capture the website, but can we do the apps? Yes, follow the next steps:

For that we will install the tools:

```
frida-server-x86: 1 file pushed, 0 skipped. 103.1 MB/s (53604060 bytes in 0.496s)
rohit@Rohits-MacBook-Pro platform-tools % ifconfig| grep 192.1
        inet 192.168.1.6 netmask 0xffffff00 broadcast 192.168.1.255
rohit@Rohits-MacBook-Pro platform-tools % sudo pip3 install frida frida-tools objection
Password:
WARNING: The directory '/Users/rohit/Library/Caches/pip' or its parent directory is not owned or is not writable by the current user. The cache has been disabled. Check the permissions and owner of that directory. If executing pip with sudo, you should use sudo's -H flag.
Requirement already satisfied: frida in /usr/local/lib/python3.10/site-packages (16.0.7)
Requirement already satisfied: frida-tools in /usr/local/lib/python3.10/site-packages (12.0.3)
Requirement already satisfied: objection in /usr/local/lib/python3.10/site-packages (1.11.0)
Requirement already satisfied: setuptools in /usr/local/lib/python3.10/site-packages (from frida) (65.4.1)
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in /usr/local/lib/python3.10/site-packages (from frida-tools) (0.4.5)
Requirement already satisfied: prompt-toolkit<4.0.0,>=2.0.0 in /usr/local/lib/python3.10/site-packages (from frida-tools) (3.0.31)
Requirement already satisfied: pygments<3.0.0,>=2.0.2 in /usr/local/lib/python3.10/site-packages (from frida-tools) (2.13.0)
Requirement already satisfied: requests in /usr/local/lib/python3.10/site-packages (from objection) (2.11.1)
Requirement already satisfied: semver<3,>=2 in /usr/local/lib/python3.10/site-packages (from objection) (2.13.0)
Requirement already satisfied: litecli>=1.3.0 in /usr/local/lib/python3.10/site-packages (from objection) (1.9.0)
Requirement already satisfied: tabulate in /usr/local/lib/python3.10/site-packages (from objection) (0.9.0)
Requirement already satisfied: flask in /usr/local/lib/python3.10/site-packages (from objection) (2.2.2)
```

Confirm if it is succeessfully installed or not:

```
rohit@Rohits-MacBook-Pro platform-tools % frida
usage: frida [options] target
frida: error: target must be specified
rohit@Rohits-MacBook-Pro platform-tools %
```

Now, create the fridascript.js file and paste the code from the following like: https://codeshare.frida.re/@akabe1/frida-multiple-unpinning/

```
rohit@Rohits-MacBook-Pro platform-tools % nano fridascript.js
rohit@Rohits-MacBook-Pro platform-tools %
```

Now, we need the package name of the app, which we need to hop and perform: Go to the website and copy it.

Zomato: Food Delivery & Dining

Now, we will run the command in the terminal as: not we shall have to mention the package name.

```
rohit@Rohits-MacBook-Pro platform-tools % frida -U -f com.application.zomato -l fridascript.js
     ____
    / _  |   Frida 16.0.7 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)
Spawning `com.application.zomato`...
```

After a moment: an error occurred. Fix this error by copy pasting the certificate.

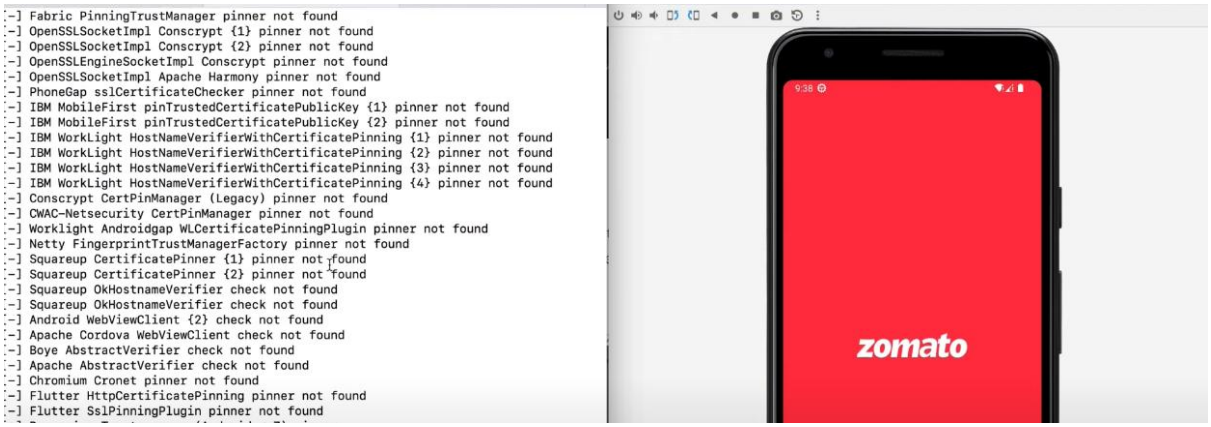
```
rohit@Rohits-MacBook-Pro platform-tools % frida -U -f com.application.zomato -l fridascript.js
     ____
    / _  |   Frida 16.0.7 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.application.zomato`. Resuming main thread!
[Android Emulator 5554::com.application.zomato ]->
[.] Cert Pinning Bypass/Re-Pinning
[+] Loading our CA...
[o] Error: java.io.FileNotFoundException: /data/local/tmp/cert-der.crt: open failed: ENOENT (No suc
h file or directory)
Error: BufferedInputStream(): argument types do not match any of:
        .overload('java.io.InputStream')
        .overload('java.io.InputStream', 'int')
    at X (frida/node_modules/frida-java-bridge/lib/class-factory.js:568)
    at value (frida/node_modules/frida-java-bridge/lib/class-factory.js:972)
    at e (frida/node_modules/frida-java-bridge/lib/class-factory.js:552)
    at <anonymous> (/Users/rohit/andro/platform-tools/fridascript.js:36)
    at <anonymous> (frida/node_modules/frida-java-bridge/lib/vm.js:12)
    at _performPendingVmOps (frida/node_modules/frida-java-bridge/index.js:250)
    at <anonymous> (frida/node_modules/frida-java-bridge/index.js:242)
    at apply (native)
    at ne (frida/node_modules/frida-java-bridge/lib/class-factory.js:619)
    at <anonymous> (frida/node_modules/frida-java-bridge/lib/class-factory.js:597)
```

Once, it is fixed, we will use the same command:

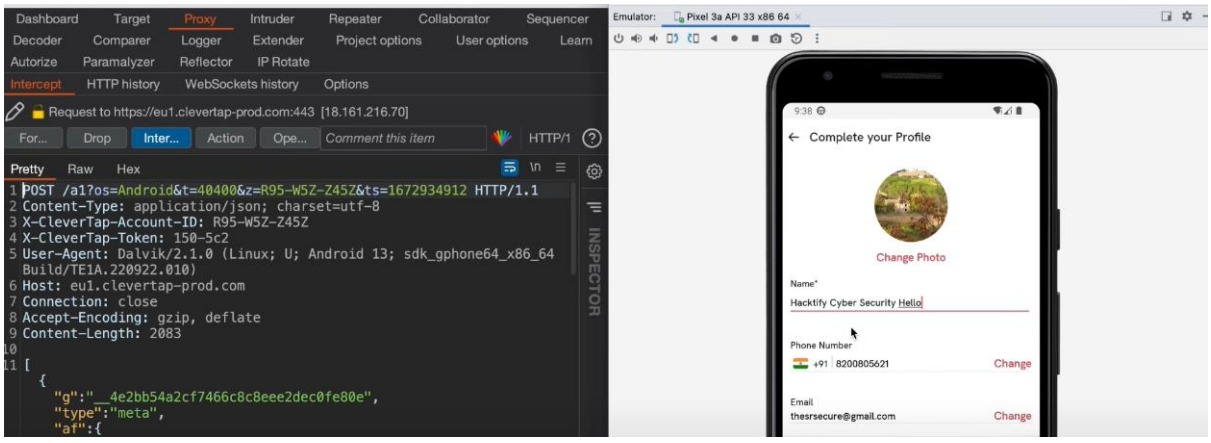
```
rohit@Rohits-MacBook-Pro platform-tools % frida -U -f com.application.zomato -l mult
iple-script.js

     ____
    / _  |   Frida 16.0.7 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)
Spawning `com.application.zomato`...
```

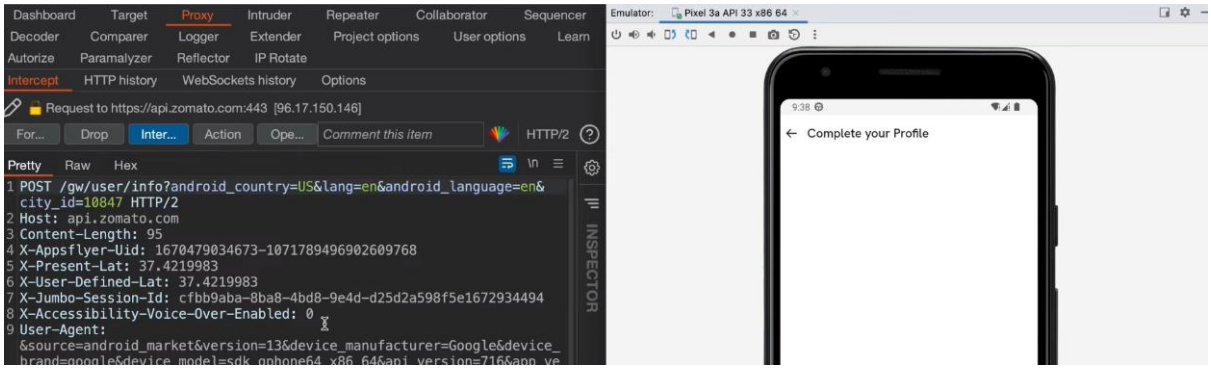
This time it is done:



Now, we will go to the burpsuite:



Now, we will make it off and then on, and then make a change in the profile: yes are able to capture and see the request as well.


Dashboard
Target
Proxy
Intruder
Repeater
Collaborator
Sequencer
Decoder
Comparer
Logger
Extender
Project options
User options
Learn
Autorize
Paramalyzer
Reflector
IP Rotate
Intercept
HTTP history
WebSockets history
Options
Request to https://api.zomato.com:443 [96.17.150.146]
For...
Drop
Inter...
Action
Ope...
Comment this item
HTTP/2
Pretty
Raw
Hex
1 POST /gw/user/info?android_country=US&lang=en&android_language=en&
city_id=10847 HTTP/2
2 Host: api.zomato.com
3 Content-Length: 95
4 X-Appsflyer-Uid: 1670479034673-1071789496902609768
5 X-Present-Lat: 37.4219983
6 X-User-Defined-Lat: 37.4219983
7 X-Jumbo-Session-Id: cfbb9aba-8ba8-4bd8-9e4d-d25d2a598f5e1672934494
8 X-Accessibility-Voice-Over-Enabled: 0
9 User-Agent:
&source=android_market&version=13&device_manufacturer=Google&device_
INSPECTOR
Emulator:
Pixel 3a API 33 x86 64
9:38
Complete your Profile

--The End--