**Day 4**

**Exploitation Analyst**

**Hacking the SSL Network protocol:**

**Android SSL Pinning Bypass**

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

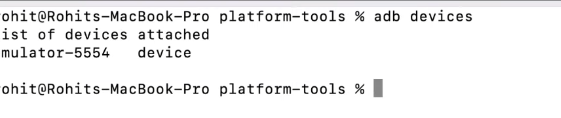
Objective: To bypass the Android SSL pinning.

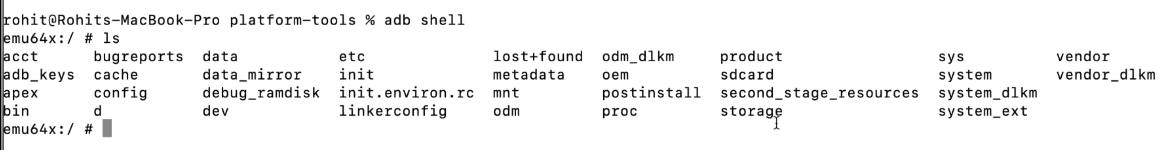
Tools required:

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>)

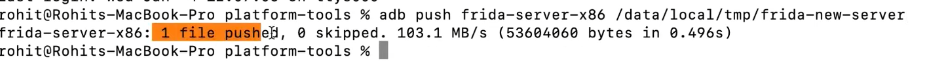
Steps:

First confirm that Frida is recognising the android device:



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


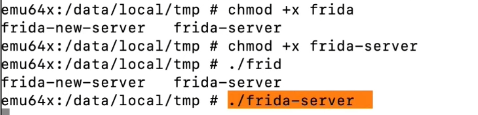
In another tab we are pushing the Frida server in the emulator:



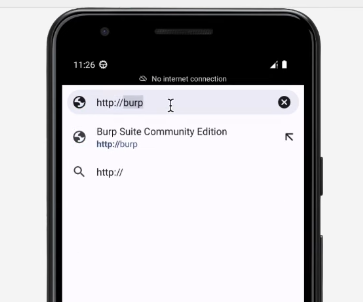
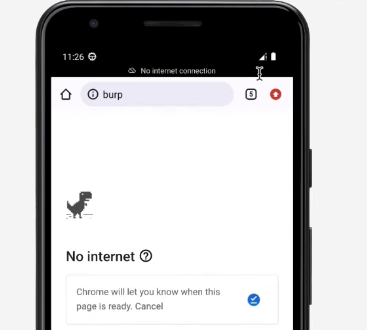
Now, verify that it is actually passed there or not: Yes it is there



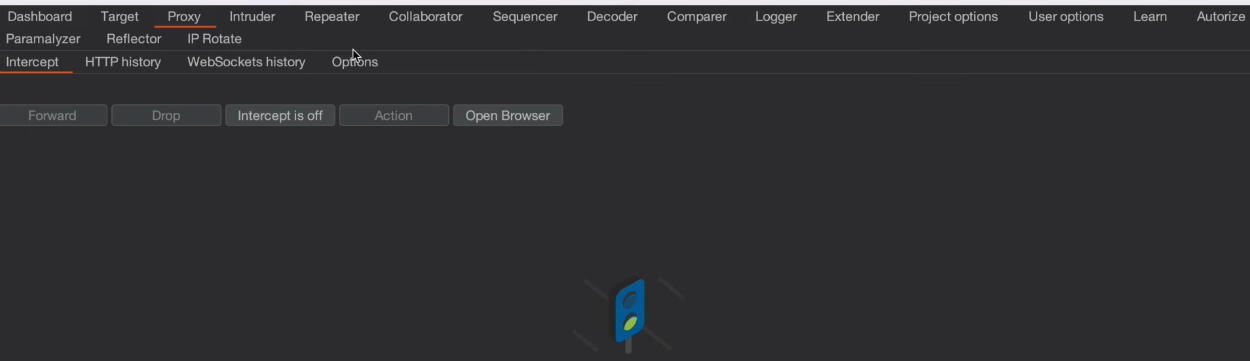
Now, give executable permission for this file to run and then execute the server file as well:



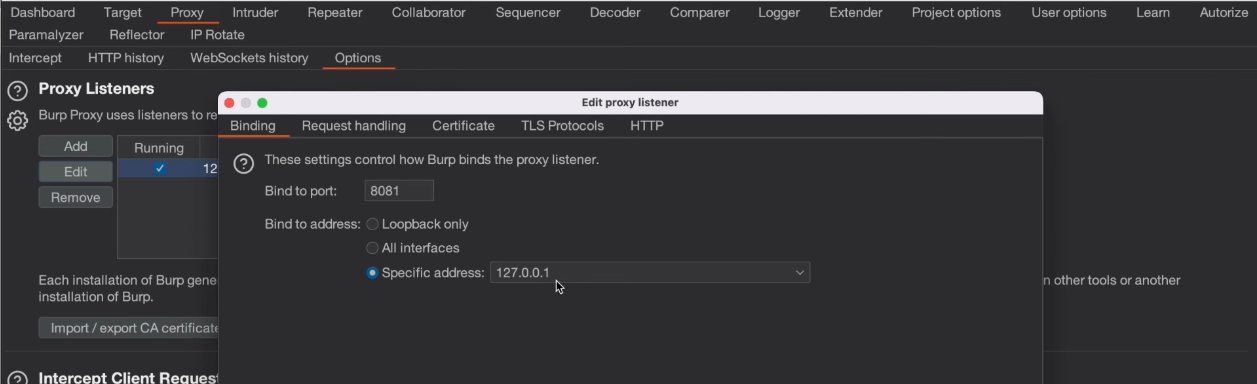
Now, keep it running and then go to the android device and confirm if the device is connected to the burp proxy or not: here it is not connected at this moment.

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

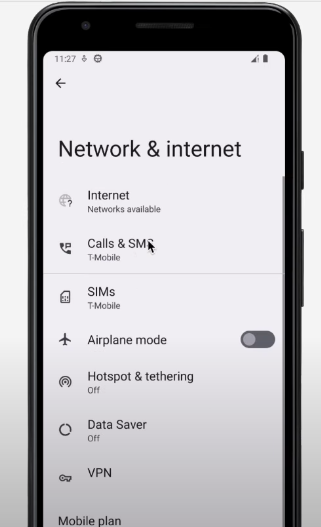


Go to the proxy setting option:

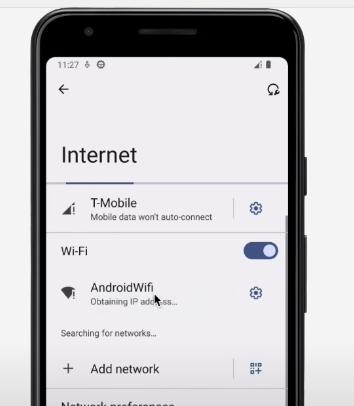


Click on the drop down menu at the specific address button, and then select the machine(your host) IP address.

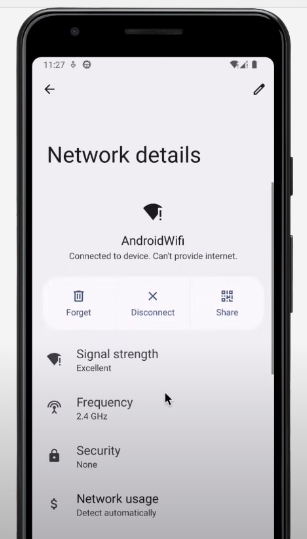
Now, go the settings in the android device: Click on the Network and Internet



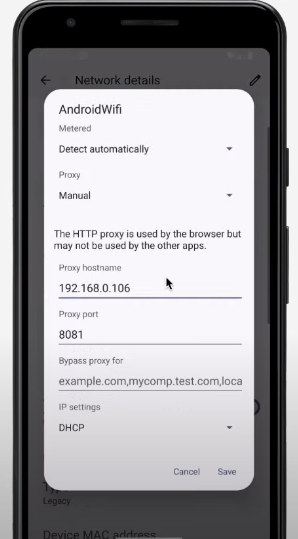
Then click on the ‘Internet’: Wifi will be available



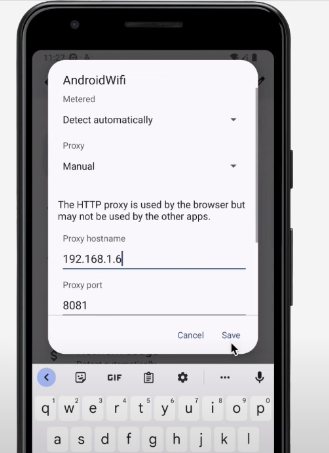
We will then change the setting of the wifi:



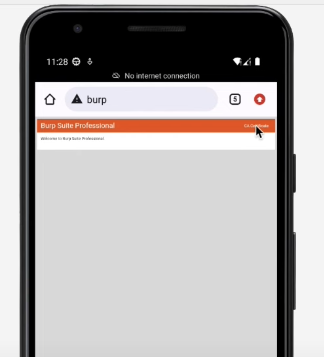
Click on the pen icon shown above: Following screen will appear



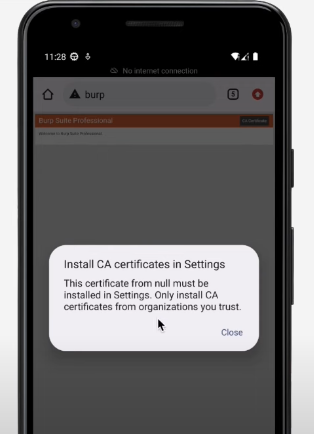
We will now change the settings as shown below: host name will be same as the one we did in the burpsuite, and also change the port number if required as per the burpsuite.



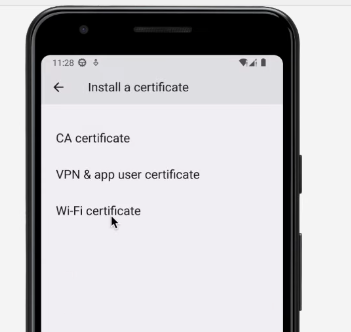
Then verify that the device is successfully connected to the burpsuite: Yes it is connected.



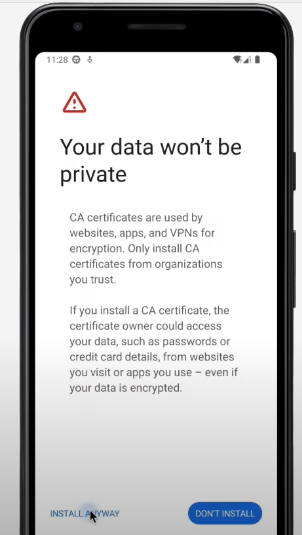
Now, click on the certificate at the top right corner and then, download the certificate:

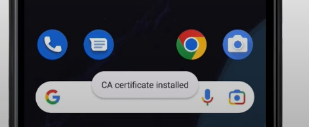


Now, go to the mobile again and go to the settings in the mobile, and look for the CA certificate option:

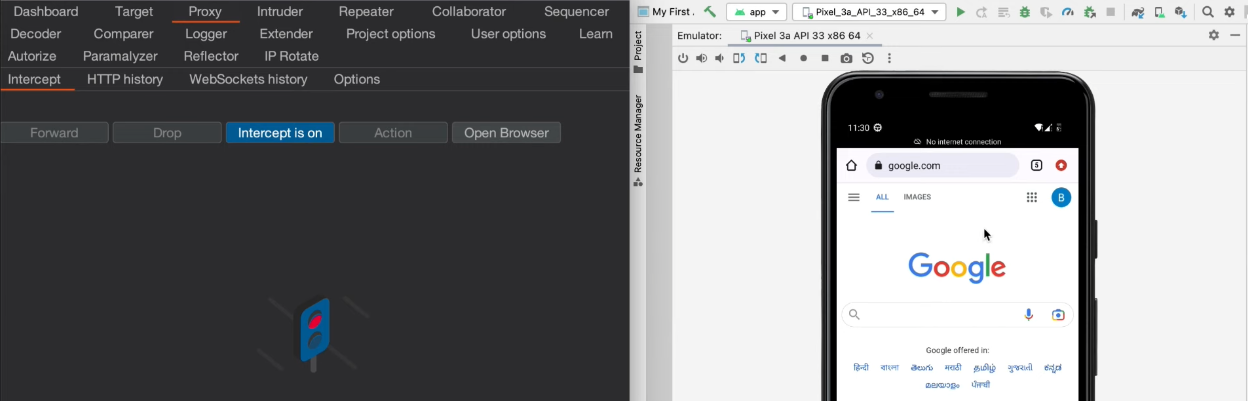


Click on the CA certificate: Then click on “Install anyway” option.

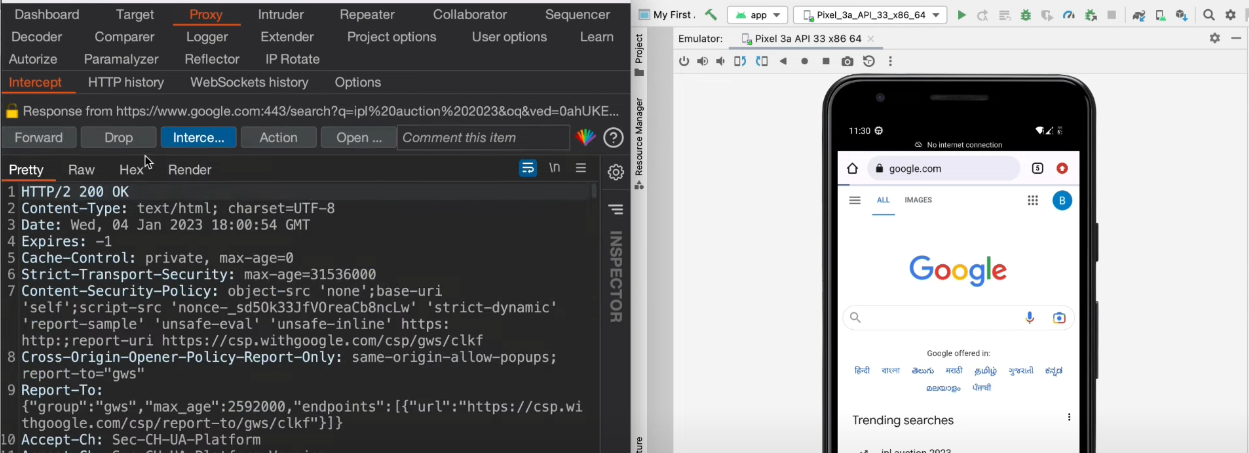


Select the certificate and it automatically get installed:  


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

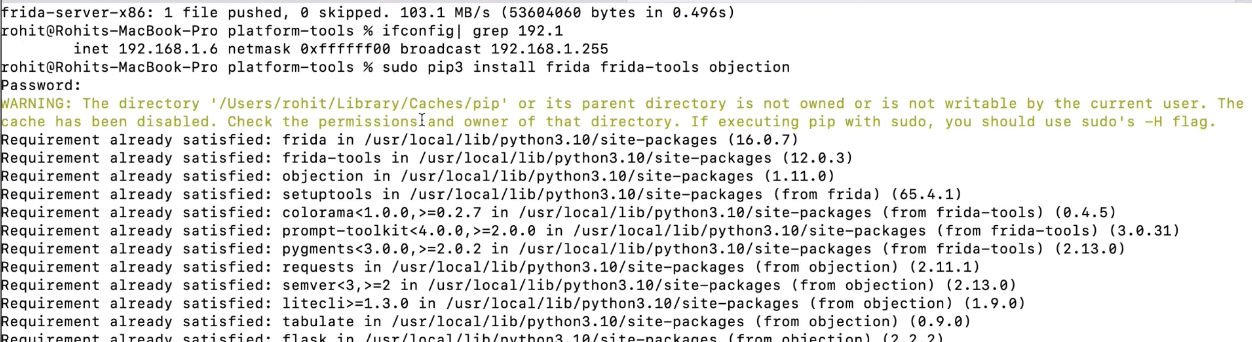


The moment I clicked on something in the browser, we will see in the burpsuite as well:

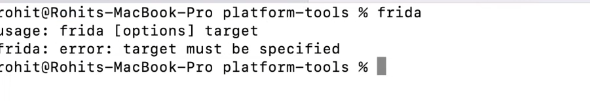


Now, clealry we are able to capture the website, but can we do the apps? Yes, follow the next steps:

For that we will install the tools:



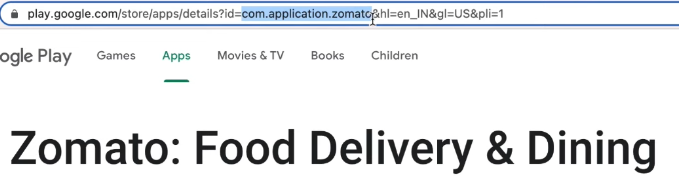
Confirm if it is succeessfully installed or not:



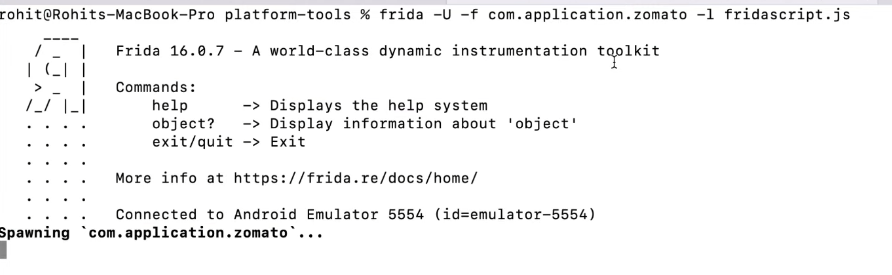
Now, create the fridascript.js file and paste the code from the following like: <https://codeshare.frida.re/@akabe1/frida-multiple-unpinning/>



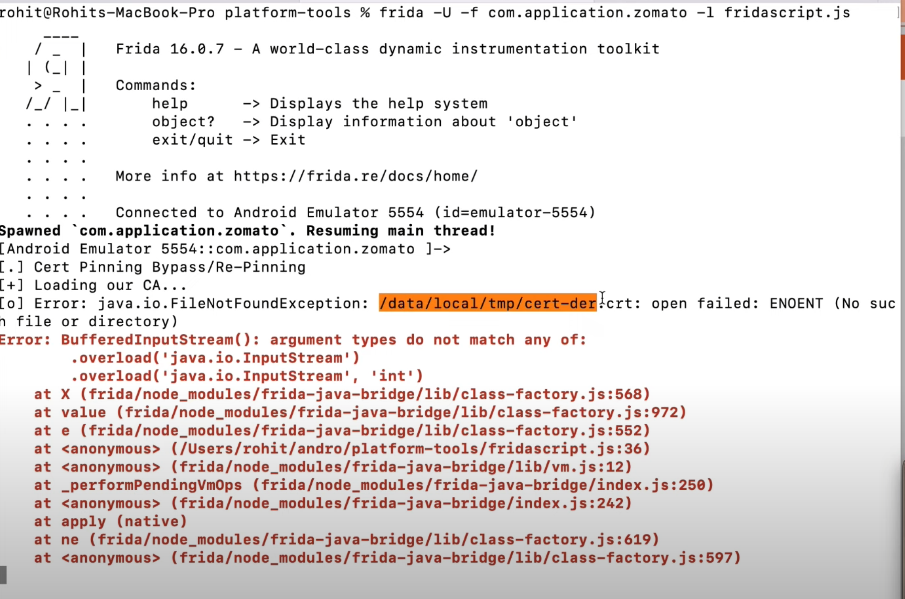
Now, we need the package name of the app, which we need to hop and perform: Go to the website and copy it.



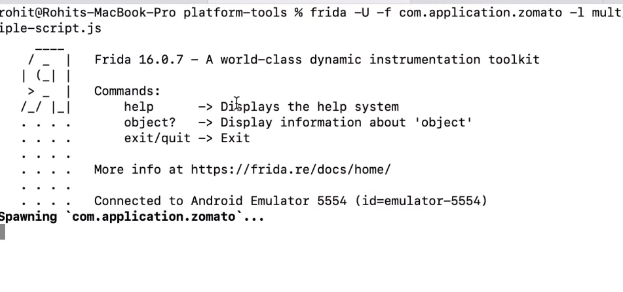
Now, we will run the command in the terminal as: not we shall have to mention the package name.



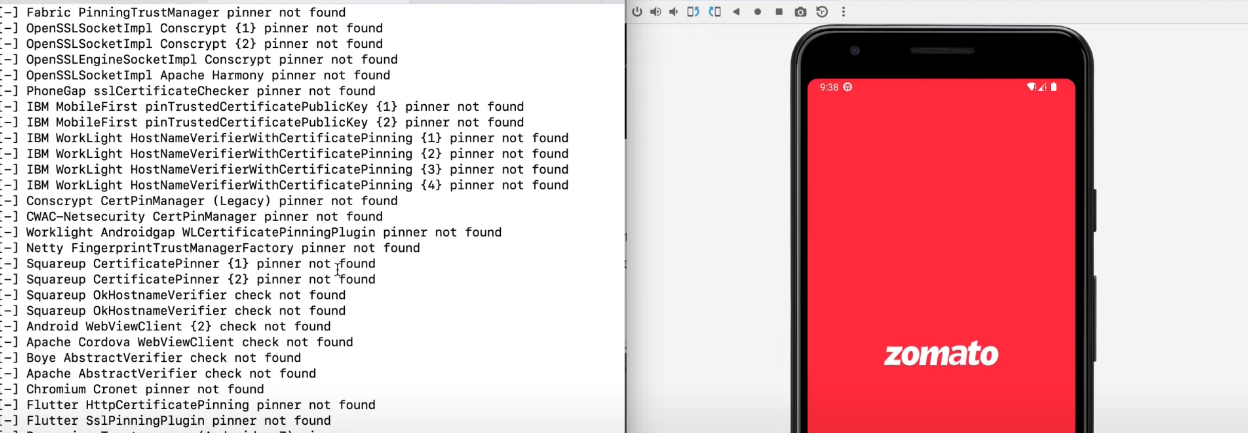
After a moment: an error occurred. Fix this error by copy pasting the certificate.



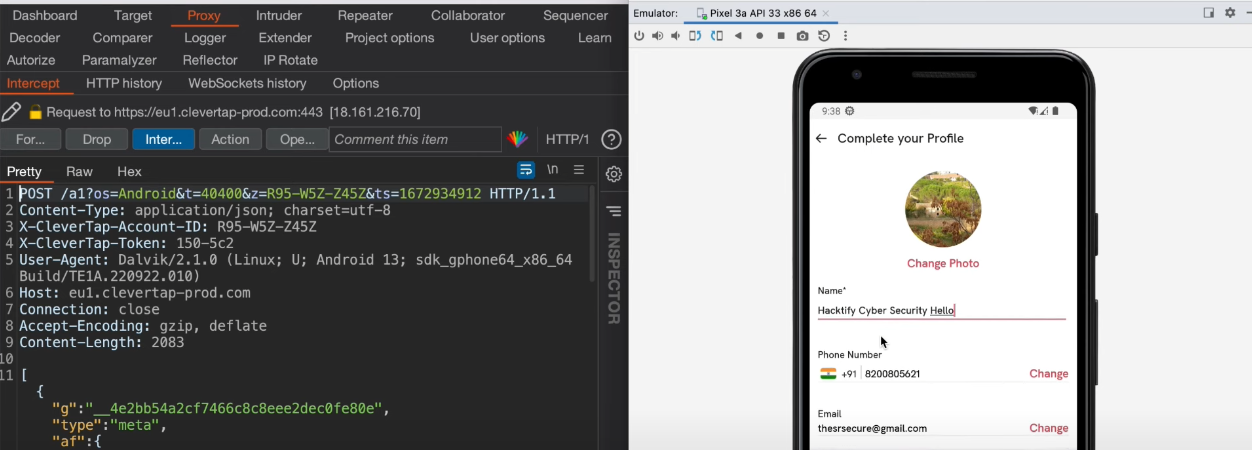
Once, it is fixed, we will use the same command:



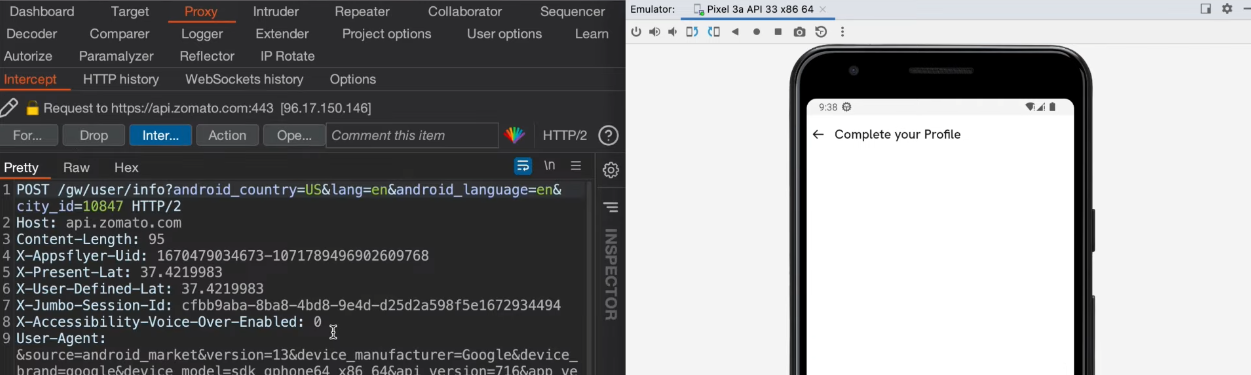
This time it is done:



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.



--The End--