FRIDA TOOL:

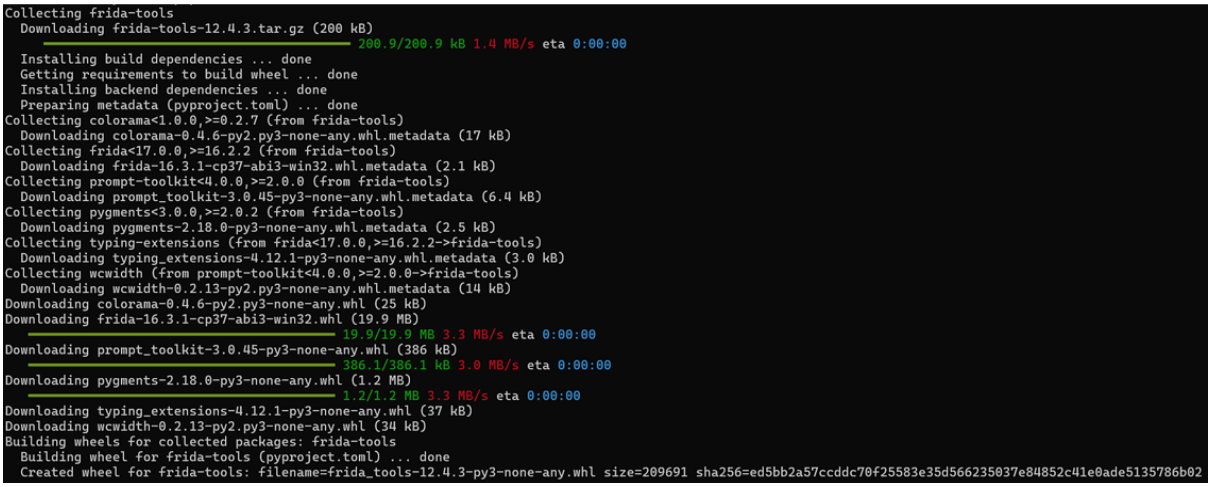
Aakash R
CB.SC.P2CYS23011

Frida is a dynamic instrumentation toolkit designed for developers, reverse engineers, and security researchers. It allows you to inject scripts into running processes to inspect and modify their behaviour on the fly.

Use Cases

- **Security Testing**: Inspect and modify the behavior of applications to find vulnerabilities and test security mechanisms.
- **Reverse Engineering**: Understand how applications work internally by examining and modifying their runtime behavior.
- **Debugging**: Debug applications by injecting scripts to track down bugs and performance issues.
- **Bypassing Restrictions**: Modify app behavior to bypass certain restrictions or implement additional features.

Frida uses an injector to load a shared library into the target process. This library provides a JavaScript runtime environment where user scripts are executed. The scripts can hook into various functions, manipulate memory, and interact with the app in real-time.

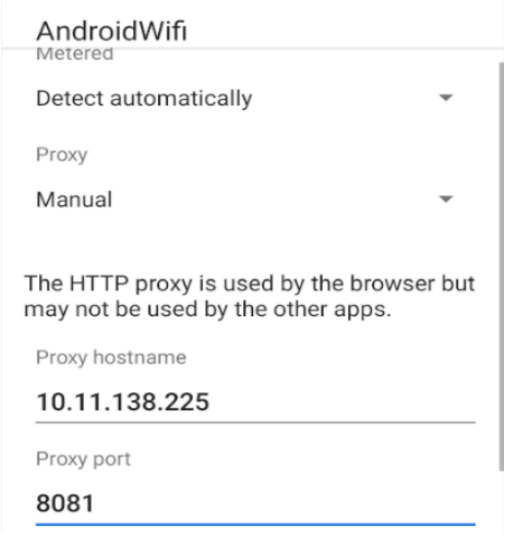


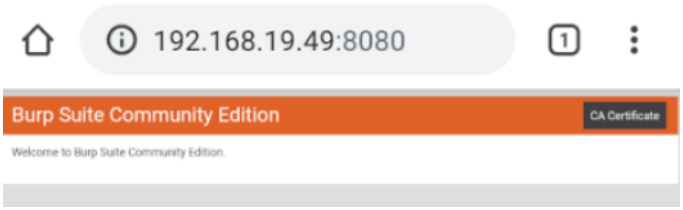
```
D:\Mtech Course\Sem 3\Android Assignments\frida_tools>emulator -list-avds
INFO    | Storing crashdata in: C:\Temps\\AndroidEmulator\emu-crash-34.2.14.db, detection is enabled for process: 10760
Pixel_3_API_19
Pixel_4_XL_API_30

D:\Mtech Course\Sem 3\Android Assignments\frida_tools>emulator -avd

D:\Mtech Course\Sem 3\Android Assignments\frida_tools>emulator -avd Pixel_3_API_19
INFO    | Storing crashdata in: C:\Temps\\AndroidEmulator\emu-crash-34.2.14.db, detection is enabled for process: 11000
INFO    | Android emulator version 34.2.14.0 (build_id 11834374) (CL:N/A)
INFO    | Found systemPath C:\Users\Jay Shah\AppData\Local\Android\Sdk\system-images\android-19\default\x86\
INFO    | Storing crashdata in: C:\Temps\\AndroidEmulator\emu-crash-34.2.14.db, detection is enabled for process: 9936
INFO    | Duplicate loglines will be removed, if you wish to see each individual line launch with the -log-nofilter flag
.
INFO    | IPv4 server found: 192.168.1.1
INFO    | Ignore IPv6 address: 857:1567:b02:0:6051:1567:b02:0
INFO    | Ignore IPv6 address: 857:1567:b02:0:6051:1567:b02:0 (2x)
INFO    | Ignore IPv6 address: 205d:1567:b02:0:6051:1567:b02:0
INFO    | Ignore IPv6 address: 205d:1567:b02:0:6051:1567:b02:0 (2x)
INFO    | Ignore IPv6 address: 4063:1567:b02:0:6051:1567:b02:0
INFO    | Ignore IPv6 address: 4063:1567:b02:0:6051:1567:b02:0 (2x)
```

```
PS D:\Mtech Course\Sem 3\Android Assignments\frida_tools> adb push frida-server /data/local/tmp
frida-server: 1 file pushed, 0 skipped. 23.2 MB/s (56532312 bytes in 2.320s)
PS D:\Mtech Course\Sem 3\Android Assignments\frida_tools> adb shell
```

```
PS D:\Mtech Course\Sem 3\Android Assignments\frida_tools> adb push frida-server /data/local/tmp
frida-server: 1 file pushed, 0 skipped. 23.2 MB/s (56532312 bytes in 2.320s)
PS D:\Mtech Course\Sem 3\Android Assignments\frida_tools> adb shell
root@generic_x86:/ # cd /data/local/tmp
root@generic_x86:/data/local/tmp # ls
frida-server
hmod 777 frida-server                                                    <
root@generic_x86:/data/local/tmp # chmod 777 frida-server
root@generic_x86:/data/local/tmp #
```

With Burp Suite:





Search for CA Certificate