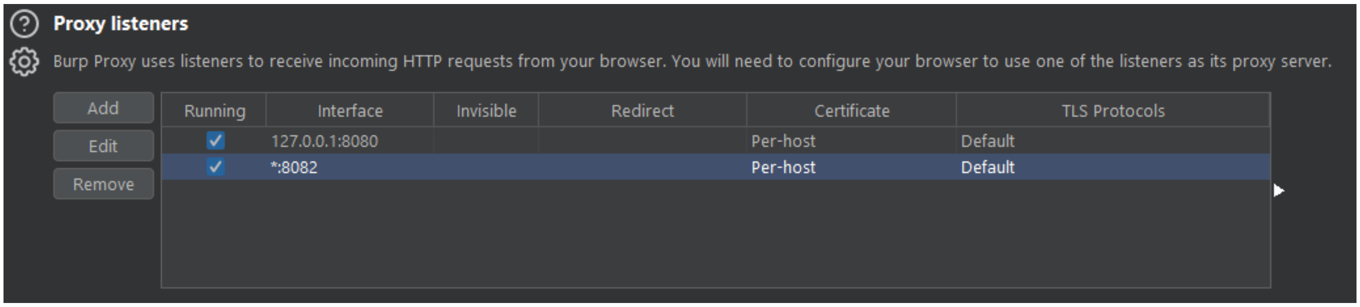
Intercept requests

Set proxy on burpsuite



Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default
☑	*:8082			Per-host	Default

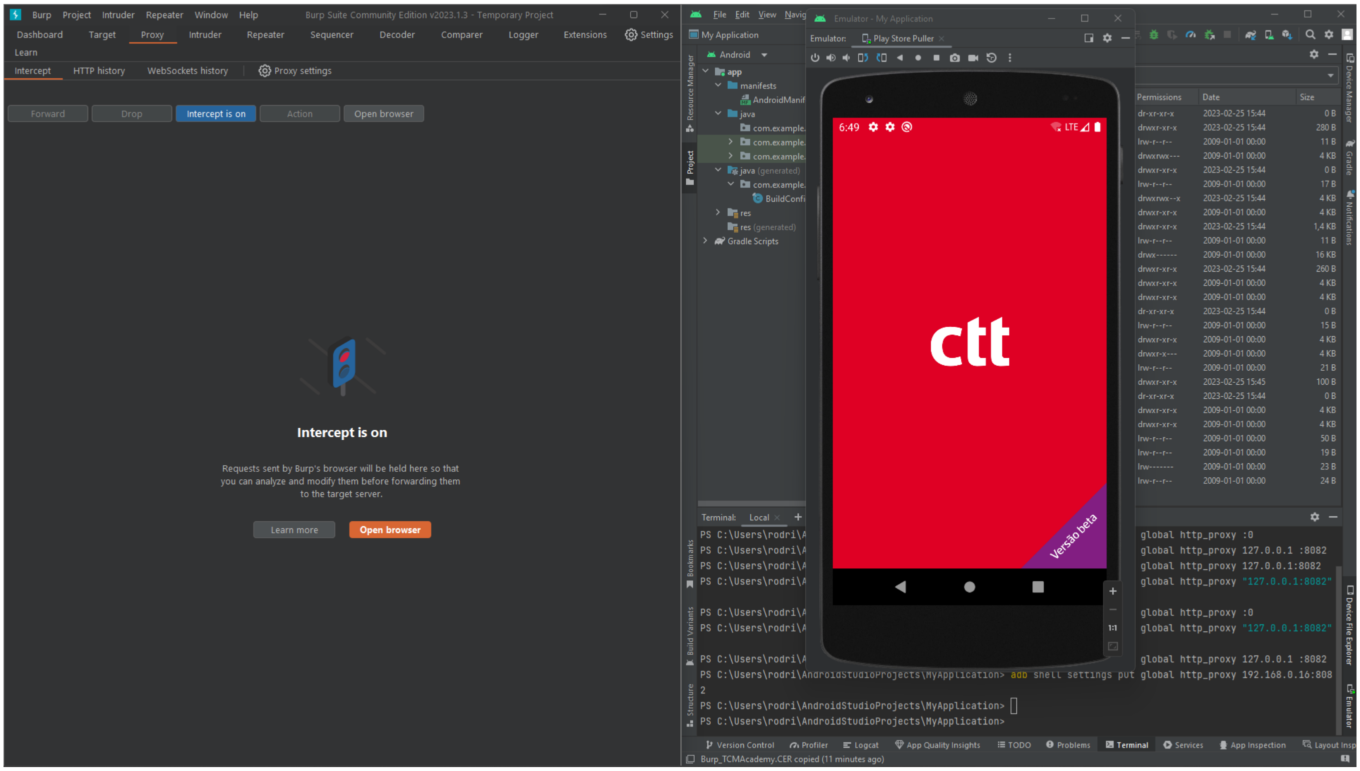
Set proxy on Android VM

```
PS adb shell settings put global http_proxy 192.168.0.16:8082
```

Export Cert

1. Generate cert on Burp
2. Add cert through settings on VM

Result (SSL Pinning is being used)



Intercept is on

Requests sent by Burp's browser will be held here so that you can analyze and modify them before forwarding them to the target server.

Permissions	Date	Size
dr-xr-xr-x	2023-02-25 15:44	0 B
drwxr-xr-x	2023-02-25 15:44	280 B
lrw-r--r--	2009-01-01 00:00	11 B
drwxrwx---	2009-01-01 00:00	4 KB
drwxr-xr-x	2023-02-25 15:44	0 B
lrw-r--r--	2009-01-01 00:00	17 B
drwxrwx--x	2023-02-25 15:44	4 KB
drwxr-xr-x	2009-01-01 00:00	4 KB
drwxr-xr-x	2023-02-25 15:44	1,4 KB
lrw-r--r--	2009-01-01 00:00	11 B
drwx------	2009-01-01 00:00	16 KB
drwxr-xr-x	2023-02-25 15:44	260 B
drwxr-xr-x	2009-01-01 00:00	4 KB
drwxr-xr-x	2009-01-01 00:00	4 KB
dr-xr-xr-x	2023-02-25 15:44	0 B
lrw-r--r--	2009-01-01 00:00	15 B
drwxr-xr-x	2009-01-01 00:00	4 KB
drwxr-x---	2009-01-01 00:00	4 KB
lrw-r--r--	2009-01-01 00:00	21 B
drwxr-xr-x	2023-02-25 15:45	100 B
dr-xr-xr-x	2023-02-25 15:44	0 B
drwxr-xr-x	2009-01-01 00:00	4 KB
drwxr-xr-x	2009-01-01 00:00	4 KB
lrw-r--r--	2009-01-01 00:00	50 B
lrw-r--r--	2009-01-01 00:00	19 B
lrw-------	2009-01-01 00:00	23 B
lrw-r--r--	2009-01-01 00:00	24 B

```
PS C:\Users\rodri\A                                         global http_proxy :0
PS C:\Users\rodri\A                                         global http_proxy 127.0.0.1 :8082
PS C:\Users\rodri\A                                         global http_proxy 127.0.0.1:8082
PS C:\Users\rodri\A                                         global http_proxy "127.0.0.1:8082"

PS C:\Users\rodri\A                                         global http_proxy :0
PS C:\Users\rodri\A                                         global http_proxy "127.0.0.1:8082"

PS C:\Users\rodri\A                                         global http_proxy 127.0.0.1 :8082
PS C:\Users\rodri\AndroidStudioProjects\MyApplication> adb shell settings put global http_proxy 192.168.0.16:808
2
PS C:\Users\rodri\AndroidStudioProjects\MyApplication>
PS C:\Users\rodri\AndroidStudioProjects\MyApplication>
```

Burp_TCMAcademy.CER copied (11 minutes ago)

Patching the SSL certificate with the help of Frida and Objection

Install of frida with the help of python and PIP

```
PS C:\Users\rodri> pip3 install frida
Collecting frida
  Downloading frida-16.0.10-cp37-abi3-win_amd64.whl (30.7 MB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 30.7/30.7 MB 23.4 MB/s eta 0:00:00
Collecting typing-extensions
  Downloading typing_extensions-4.5.0-py3-none-any.whl (27 kB)
Installing collected packages: typing-extensions, frida
Successfully installed frida-16.0.10 typing-extensions-4.5.0

[notice] A new release of pip available: 22.3.1 -> 23.0.1
[notice] To update, run:
C:\Users\rodri\AppData\Local\Microsoft\WindowsApps\PythonSoftwareFoundation.Python.
3.10_qbz5n2kfra8p0\python.exe -m pip install --upgrade pip
PS C:\Users\rodri>
```

Install of objection with the help of python and PIP

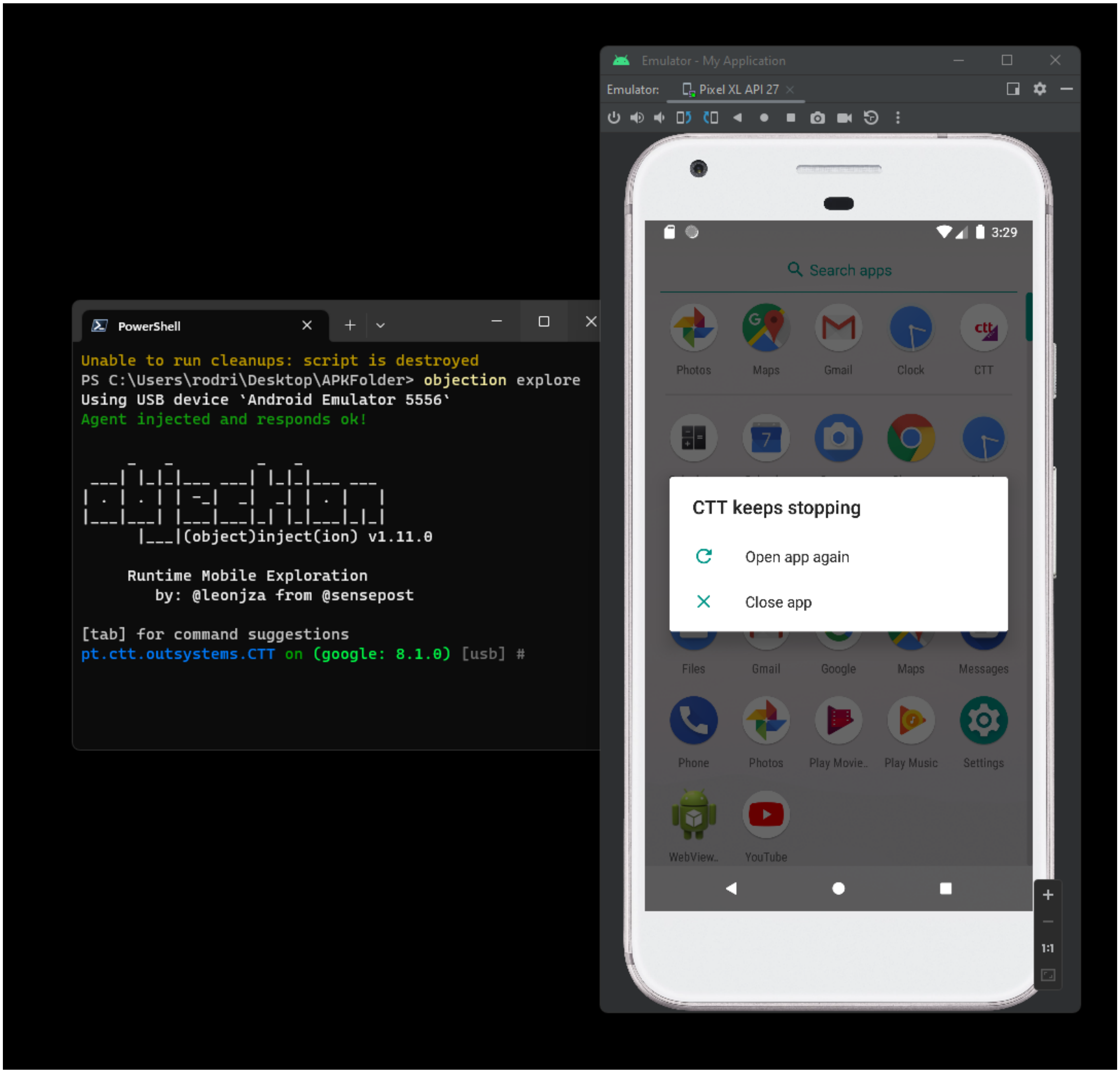
```
PS C:\Users\rodri> pip3 install objection
Collecting objection
  Downloading objection-1.11.0.tar.gz (327 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 327.2/327.2 kB 3.4 MB/s eta 0:00:00
<SNIP>
PS C:\Users\rodri>
```

Patch the apk with the Frida gadget with the help of objection

```
PS C:\Users\rodri\Desktop\APKFolder> objection patchapk --source .\ctt_pulled.apk
No architecture specified. Determining it using `adb`...
Detected target device architecture as: x86
Using latest Github gadget version: 16.0.10
Patcher will be using Gadget version: 16.0.10
Detected apktool version as: 2.7.0
Running apktool empty-framework-dir...
Press any key to continue . . .
Unpacking .\ctt_pulled.apk
App already has android.permission.INTERNET
Setting extractNativeLibs to true...
Target class not specified, searching for launchable activity instead...
Reading smali from:
```

```
C:\Users\rodri\AppData\Local\Temp\tmpitsu385x.apktemp\smali\pt/ctt/outsystems/CTT/M
ainActivity.smali
Injecting loadLibrary call at line: 6
Attempting to fix the constructors .locals count
Current locals value is 0, updating to 1:
Writing patched smali back to:
C:\Users\rodri\AppData\Local\Temp\tmpitsu385x.apktemp\smali\pt/ctt/outsystems/CTT/M
ainActivity.smali
Creating library path:
C:\Users\rodri\AppData\Local\Temp\tmpitsu385x.apktemp\lib\x86
Copying Frida gadget to libs path...
Rebuilding the APK with the frida-gadget loaded...
Built new APK with injected loadLibrary and frida-gadget
Performing zipalign
Zipalign completed
Signing new APK.
Signed the new APK
Copying final apk from
C:\Users\rodri\AppData\Local\Temp\tmpitsu385x.apktemp.aligned.objection.apk to
.\ctt_pulled.objection.apk in current directory...
Cleaning up temp files...
PS C:\Users\rodri\Desktop\APKFolder>
```

Patch result



```
Unable to run cleanups: script is destroyed
PS C:\Users\rodri\Desktop\APKFolder> objection explore
Using USB device `Android Emulator 5556`
Agent injected and responds ok!

     _   _         _   _
 ___| |_|_|___ ___| |_|_|___ ___
| . | . | | -_|  _|  _| | . |   |
|___|___| |___|___|_| |_|___|_|_|
      |___|(object)inject(ion) v1.11.0

     Runtime Mobile Exploration
        by: @leonjza from @sensepost

[tab] for command suggestions
pt.ctt.outsystems.CTT on (google: 8.1.0) [usb] #
```

CTT keeps stopping

Open app again

Close app

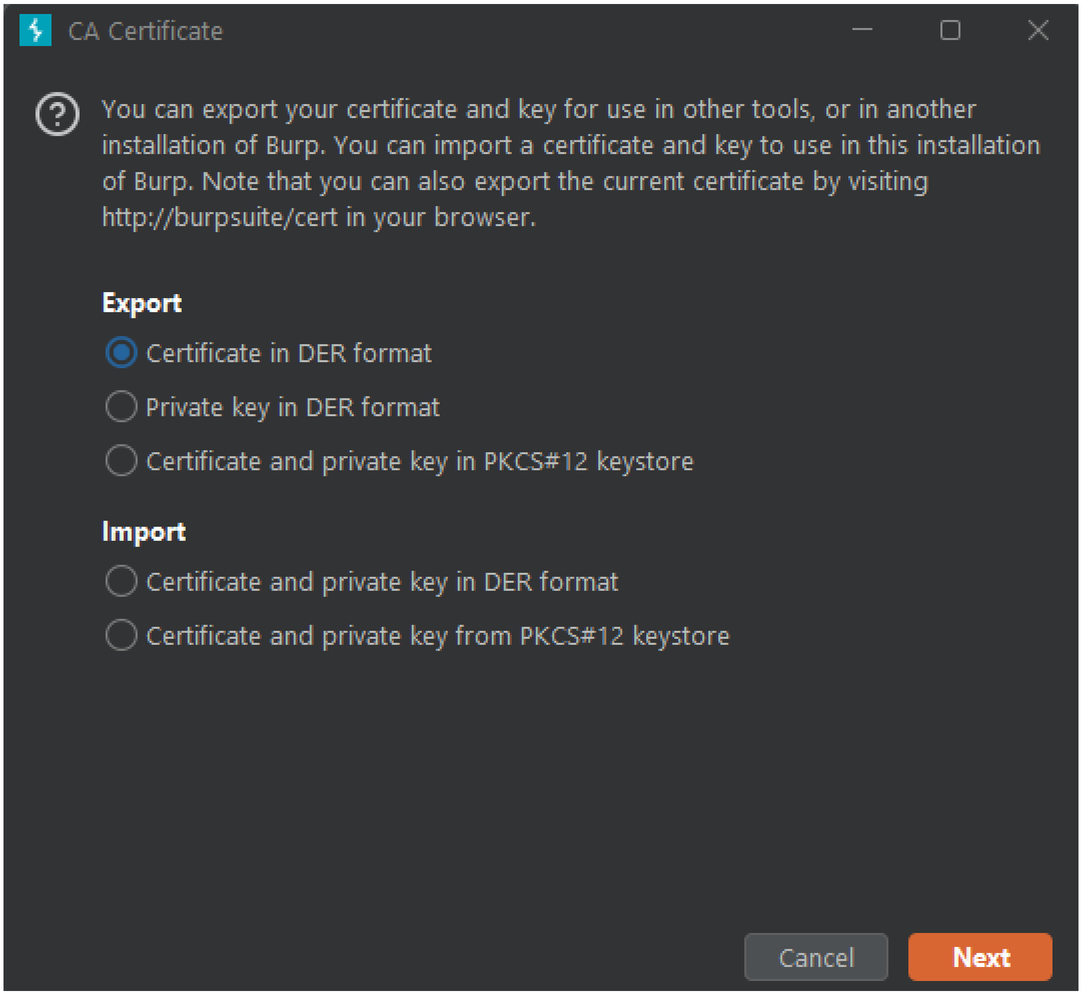
Manual patching the SSL certificate with the help of Frida

Setup BurpSuite as MITM

I used the following blogpost

Copy ssl cert to data directory

1. Export the Burp Suite cert



You can export your certificate and key for use in other tools, or in another installation of Burp. You can import a certificate and key to use in this installation of Burp. Note that you can also export the current certificate by visiting http://burpsuite/cert in your browser.

Export

● Certificate in DER format

○ Private key in DER format

○ Certificate and private key in PKCS#12 keystore

Import

○ Certificate and private key in DER format

○ Certificate and private key from PKCS#12 keystore

2. Copy the certificate to the device

```
PS > mv .\burp .\burp.PEM
PS > adb push .\burp.PEM /sdcard/
.\burp.PEM: 1 file pushed, 0 skipped. 2.9 MB/s (939 bytes in 0.000s)
PS >
```

Unpin the certificate with the help of frida

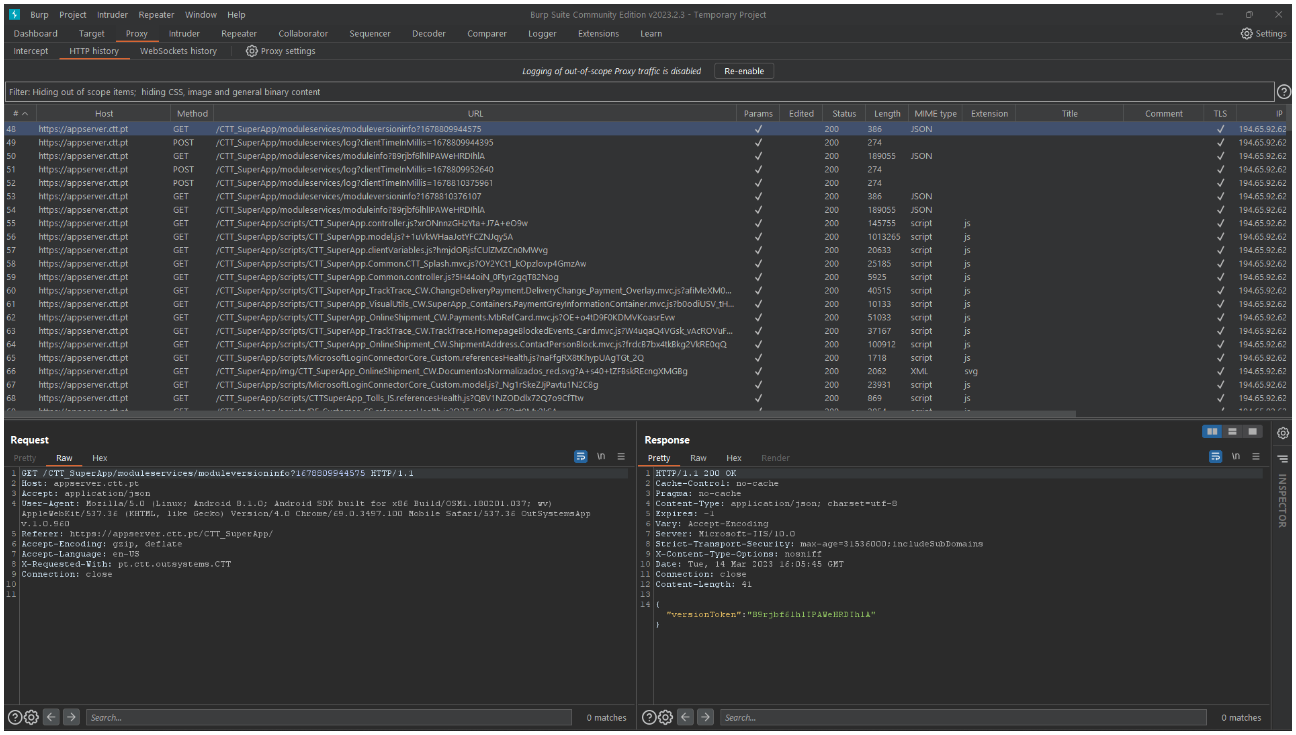
1. Run the frida-server on the target

```
PS > tar -xvf .\frida-server-16.0.10-android-x86.xz
PS > mv .\frida-server-16.0.10-android-x86 .\frida-server
PS > adb root
PS > adb push .\frida-server /data/local/tmp/
.\frida-server: 1 file pushed, 0 skipped. 86.1 MB/s (53608156 bytes in 0.594s)
PS > adb shell "chmod 755 /data/local/tmp/frida-server"
PS > adb shell "/data/local/tmp/frida-server &"
```

2.

```
PS > adb push .\frida_multiple_unpinning.js /data/local/tmp
PS > adb shell pm list packages | findstr ctt
package:pt.ctt.outsystems.CTT
PS > frida -U -l frida_multiple_unpinning.js -f pt.ctt.outsystems.CTT
     ____
    / _  |   Frida 16.0.10 - 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 `pt.ctt.outsystems.CTT`. Resuming main thread!
[Android Emulator 5554::pt.ctt.outsystems.CTT ]->
======
[#] Android Bypass for various Certificate Pinning methods [#]
======
[-] OkHTTPv3 {2} pinner not found
[-] Trustkit {1} pinner not found
[-] Trustkit {2} pinner not found
[-] Trustkit {3} pinner not found
[-] Appcelerator PinningTrustManager pinner not found
[-] Fabric PinningTrustManager pinner not found
[-] OpenSSLSocketImpl Conscrypt {1} pinner not found
[-] OpenSSLSocketImpl Conscrypt {2} pinner not found
[-] OpenSSLEngineSocketImpl Conscrypt pinner not found
[-] OpenSSLSocketImpl Apache Harmony pinner not found
[-] PhoneGap sslCertificateChecker pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {1} pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {1} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {3} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {4} pinner not found
[-] Conscrypt CertPinManager (Legacy) pinner not found
[-] CWAC-Netsecurity CertPinManager pinner not found
[-] Worklight Androidgap WLCertificatePinningPlugin pinner not found
[-] Netty FingerprintTrustManagerFactory pinner not found
[-] Squareup CertificatePinner {1} pinner not found
[-] Squareup CertificatePinner {2} pinner not found
[-] Squareup OkHostnameVerifier check not found
[-] Squareup OkHostnameVerifier check not found
[-] Android WebViewClient {2} check not found
[-] Apache Cordova WebViewClient check not found
[-] Boye AbstractVerifier check not found
[-] Apache AbstractVerifier check not found
[-] Chromium Cronet pinner not found
[-] Flutter HttpCertificatePinning pinner not found
[-] Flutter SslPinningPlugin pinner not found
[+] Bypassing Trustmanager (Android < 7) pinner
[+] Bypassing Trustmanager (Android < 7) pinner
[+] Bypassing Trustmanager (Android < 7) pinner
[+] Bypassing Android WebViewClient check {4}
[+] Bypassing Trustmanager (Android < 7) pinner
[+] Bypassing TrustManagerImpl (Android > 7) checkTrustedRecursive check:
appserver.ctt.pt
[+] Bypassing OkHTTPv3 {4}: appserver.ctt.pt
[+] Bypassing OkHTTPv3 {4}: appserver.ctt.pt
[+] Bypassing OkHTTPv3 {4}: appserver.ctt.pt
[+] Bypassing OkHTTPv3 {4}: appserver.ctt.pt
[+] Bypassing OkHTTPv3 {4}: appserver.ctt.pt
[+] Bypassing OkHTTPv3 {4}: appserver.ctt.pt
```

3. Intercept request



Logging of out-of-scope Proxy traffic is disabled

Filter: Hiding out of scope items; hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
48	https://appserver.ctt.pt	GET	/CTT_SuperApp/moduleservices/moduleversioninfo?1678809944575	✓		200	386	JSON				✓	194.65.92.62
49	https://appserver.ctt.pt	POST	/CTT_SuperApp/moduleservices/log?clientTimeInMillis=1678809944395	✓		200	274					✓	194.65.92.62
50	https://appserver.ctt.pt	GET	/CTT_SuperApp/moduleservices/moduleinfo?B9rjbf6lhlIPAWeHRDIhlA	✓		200	189055	JSON				✓	194.65.92.62
51	https://appserver.ctt.pt	POST	/CTT_SuperApp/moduleservices/log?clientTimeInMillis=1678809952640	✓		200	274					✓	194.65.92.62
52	https://appserver.ctt.pt	POST	/CTT_SuperApp/moduleservices/log?clientTimeInMillis=1678810375961	✓		200	274					✓	194.65.92.62
53	https://appserver.ctt.pt	GET	/CTT_SuperApp/moduleservices/moduleversioninfo?1678810376107	✓		200	386	JSON				✓	194.65.92.62
54	https://appserver.ctt.pt	GET	/CTT_SuperApp/moduleservices/moduleinfo?B9rjbf6lhlIPAWeHRDIhlA	✓		200	189055	JSON				✓	194.65.92.62
55	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp.controller.js?xrONnnzGHzYta+J7A+eO9w	✓		200	145755	script	js			✓	194.65.92.62
56	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp.model.js?+1uVkWHaaJotYFCZNJqy5A	✓		200	1013265	script	js			✓	194.65.92.62
57	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp.clientVariables.js?hmjdORjsfCUlZMZCn0MWvg	✓		200	20633	script	js			✓	194.65.92.62
58	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp.Common.CTT_Splash.mvc.js?OY2YCt1_kOpzlovp4GmzAw	✓		200	25185	script	js			✓	194.65.92.62
59	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp.Common.controller.js?5H44oiN_0Ftyr2gqT82Nog	✓		200	5925	script	js			✓	194.65.92.62
60	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp_TrackTrace_CW.ChangeDeliveryPayment.DeliveryChange_Payment_Overlay.mvc.js?afiMeXM0...	✓		200	40515	script	js			✓	194.65.92.62
61	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp_VisualUtils_CW.SuperApp_Containers.PaymentGreyInformationContainer.mvc.js?b0odiUSV_tH...	✓		200	10133	script	js			✓	194.65.92.62
62	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp_OnlineShipment_CW.Payments.MbRefCard.mvc.js?OE+o4tD9F0KDMVKoasrEvw	✓		200	51033	script	js			✓	194.65.92.62
63	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp_TrackTrace_CW.TrackTrace.HomepageBlockedEvents_Card.mvc.js?W4uqaQ4VGsk_vAcROVuF...	✓		200	37167	script	js			✓	194.65.92.62
64	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTT_SuperApp_OnlineShipment_CW.ShipmentAddress.ContactPersonBlock.mvc.js?frdcB7bx4tkBkg2VkRE0qQ	✓		200	100912	script	js			✓	194.65.92.62
65	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/MicrosoftLoginConnectorCore_Custom.referencesHealth.js?naFfgRX8tKhypUAgTGt_2Q	✓		200	1718	script	js			✓	194.65.92.62
66	https://appserver.ctt.pt	GET	/CTT_SuperApp/img/CTT_SuperApp_OnlineShipment_CW.DocumentosNormalizados_red.svg?A+s40+tZFBskREcngXMGBg	✓		200	2062	XML	svg			✓	194.65.92.62
67	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/MicrosoftLoginConnectorCore_Custom.model.js?_Ng1rSkeZJjPavtu1N2C8g	✓		200	23931	script	js			✓	194.65.92.62
68	https://appserver.ctt.pt	GET	/CTT_SuperApp/scripts/CTTSuperApp_Tolls_IS.referencesHealth.js?QBV1NZODdlx72Q7o9CfTtw	✓		200	869	script	js			✓	194.65.92.62

Request

```
GET /CTT_SuperApp/moduleservices/moduleversioninfo?1678809944575 HTTP/1.1
Host: appserver.ctt.pt
Accept: application/json
User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; Android SDK built for x86 Build/OSM1.180201.037; wv)
AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/69.0.3497.100 Mobile Safari/537.36 OutSystemsApp
v.1.0.960
Referer: https://appserver.ctt.pt/CTT_SuperApp/
Accept-Encoding: gzip, deflate
Accept-Language: en-US
X-Requested-With: pt.ctt.outsystems.CTT
Connection: close


```

Response

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=31536000;includeSubDomains
X-Content-Type-Options: nosniff
Date: Tue, 14 Mar 2023 16:05:45 GMT
Connection: close
Content-Length: 41

{
  "versionToken":"B9rjbf6lhlIPAWeHRDIhlA"
}
```