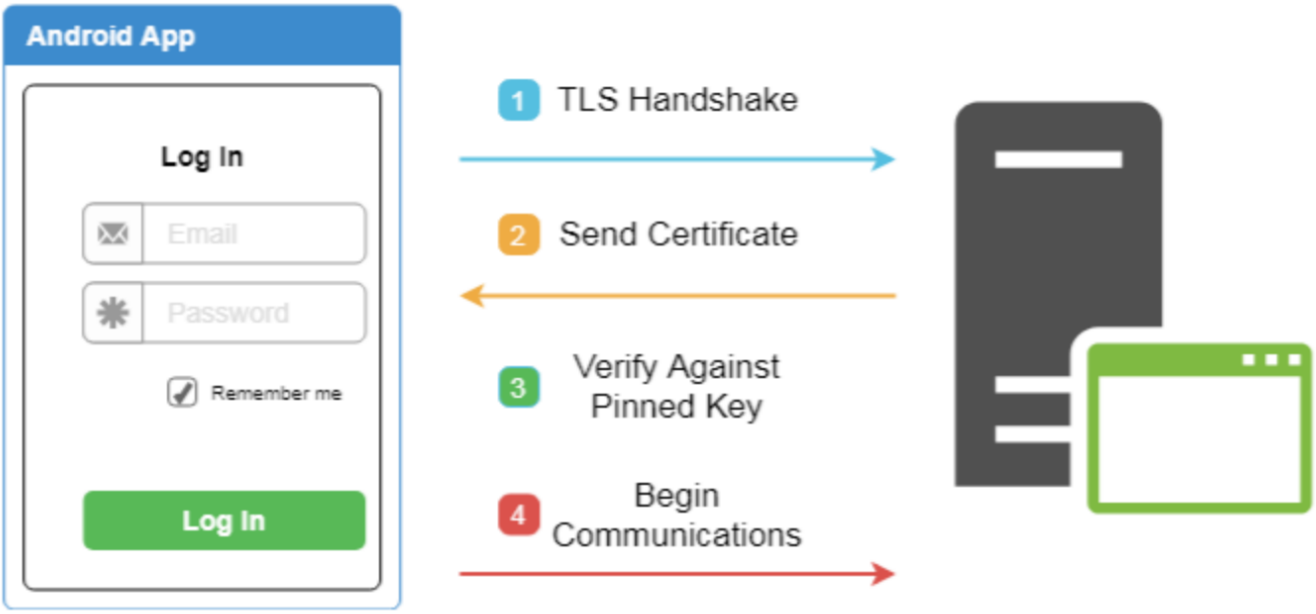
Mobile Application Pentesting-Part6

Piyush Patil
May 17 · 3 min read ★



Bypassing Certificate Pinning

SSL Pinning is a technique that we use in the client side to avoid man-in-the-middle attack by validating the server certificates again even after SSL handshaking. The developers embed (or pin) a list of trustful certificates to the client application during development, and use them to compare against the server certificates during runtime.

Decompile the apk

Find the methods responsible for validating the trustness of the cert

Patch the method by simply removing the code lines

> *Method 2: Using XPosed Framework*

Xposed is a framework that allows users to easily apply add-ons (called Modules) to the ROM. Rather than flashing a new ROM to get a specific feature, you can use Xposed to add individual features to whatever ROM you're using, or even just the stock ROM.

Installation:-

Download the app from https://www.xda-developers.com/xposed-framework-hub/

Run it and find an application named SSL pinning bypass(SSLunpinning), install it

> *Method 3: Using Objection*

Objection is a runtime mobile exploration toolkit, powered by Frida. It was built with the aim of helping assess mobile applications and their security posture without the need for a jailbroken or rooted mobile device.

then,

objection patchapk -s com.xyz.android.apk

This will create a new apk which is hooked

Push the apk file or install the application by

$ adb push <local file path> <remote file path>

or

$ adb install (path to apk)

Now run,

objection -g (new apk file name) explore -q

Where,

-g stands for "Name of the Frida Gadget/Process to connect to"

explore stands for "objection exploration REPL"

thus if the file is successfully injected

run "android sslpinning disable"

. . .

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

In our case(Nexus Android), we used frida-server-12.4.0-android-arm.xz.

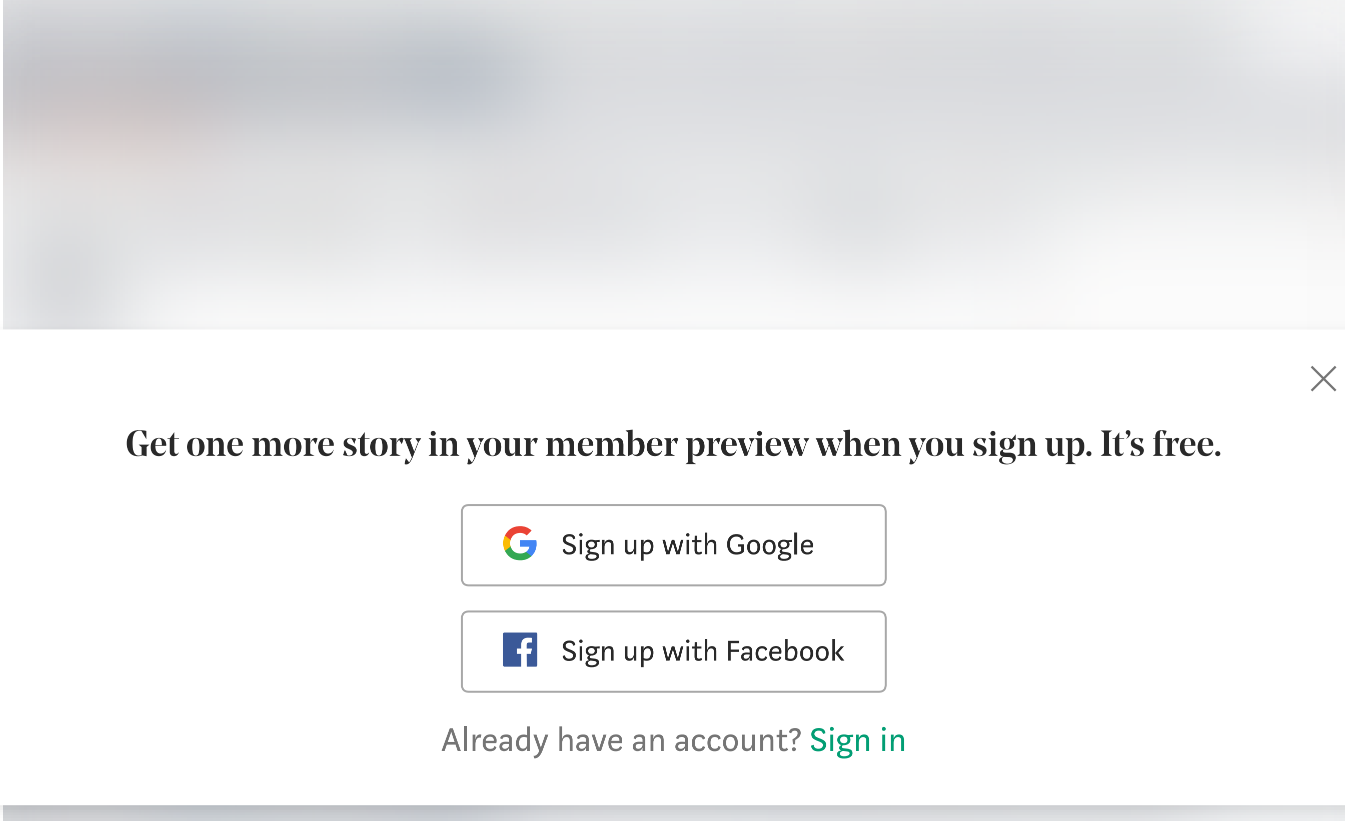
you decompress it and rename decompress file as frida-server

Open terminal and type following commands:-

```
adb push frida-server /data/local/tmp/

adb shell “chmod 755 /data/local/tmp/frida-server”

adb shell

su

cd /data/local/tmp/

./frida-server
```

Keep the frida-server running on this terminal

Go to burp suite and generate burp certificate



Select certificate in DER format

Then you need to rename the certificate generate by burp to burpca-cert-der.crt

mv cacert.der burpca-cert-der.crt

Open new terminal

wget https://techblog.mediaservice.net/wp-content/uploads/2017/07/frida-android-repinning_sa-1.js

Pushing the rogue certificate to the device:-

> *adb push burpca-cert-der.crt /data/local/tmp/cert-der.crt —*

```
$ frida-ps -Uai
```

Android Cybersecurity Security Bug Bounty Penetration Testing

3 claps

WRITTEN BY

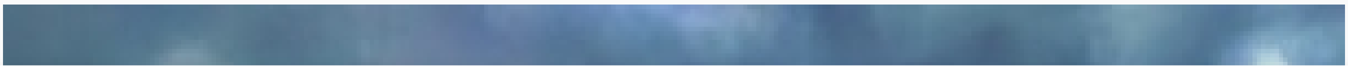
Piyush Patil

Reverse Engineering, Penetration Testing(Web, Mobile, IoT, Network, Infra)

Follow

More From Medium

Top on Medium



How to Predict the End of a Relationship

Colleen Murphy in Mindful Muse
Nov 22 · 5 min read ★

2.4K

Top on Medium

Apparently I Was Nothing But A Woo-Girl

Michelle Ann in Fearless She Wrote

Nov 13 · 4 min read ★

4.98K