PENTEST REPORT

Mobile Penetration Testing

Bina Nusantara University

APPS WE TRIED

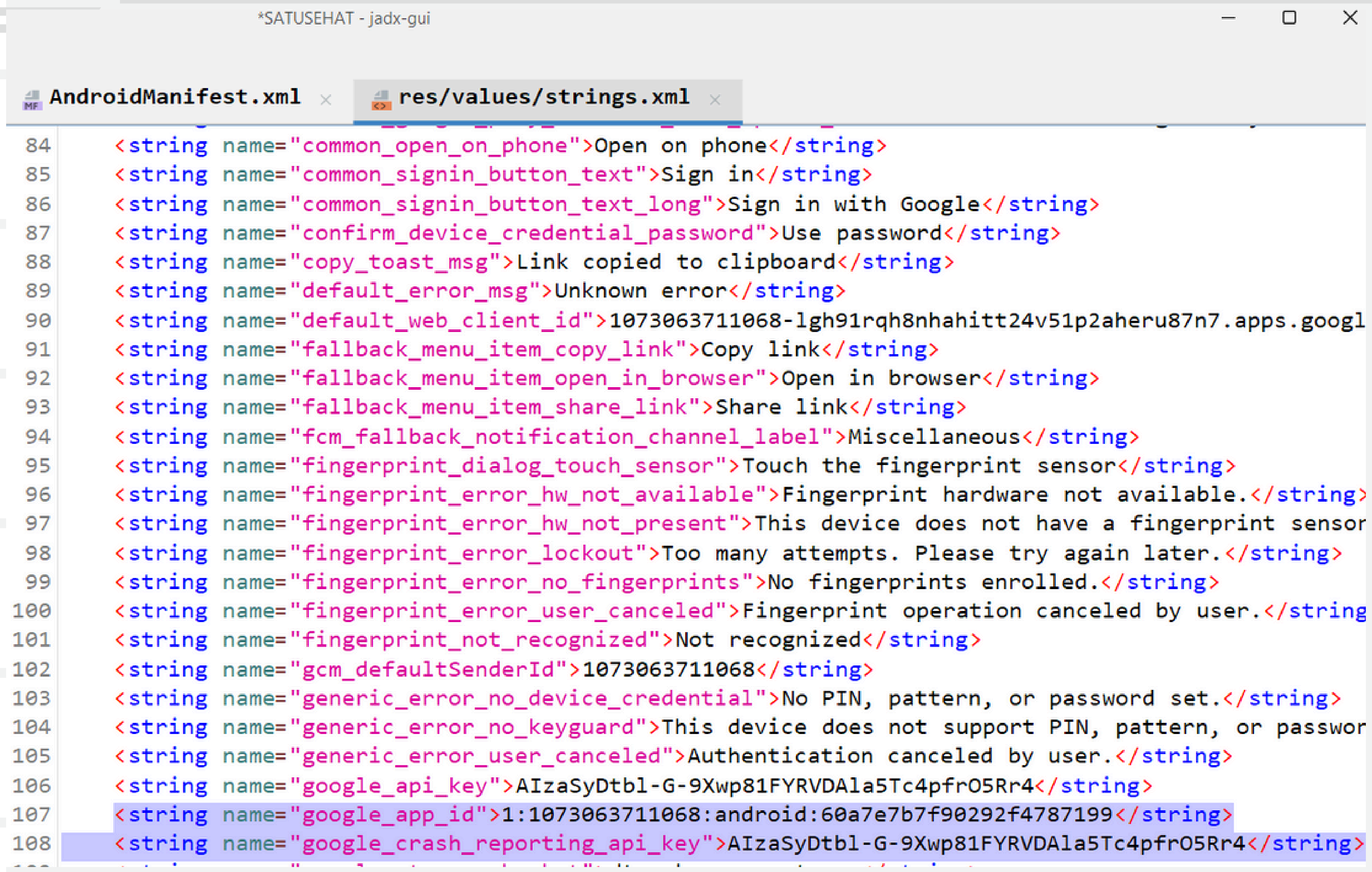
- SATUSEHAT
- IPUSNAS
- JKN Mobile

-> Succeeded in finding something

- NIKE
- SHEIN
- Janji Jawa
- Kopi Kenangan
- WeChat
- Identitas Kependudukan Digital

-> Failed to find anything relevant

STATIC ANALYSIS FINDINGS



*SATUSEHAT - jadx-gui

AndroidManifest.xml | res/values/strings.xml

```
    <string name="common_open_on_phone">Open on phone</string>
    <string name="common_signin_button_text">Sign in</string>
    <string name="common_signin_button_text_long">Sign in with Google</string>
    <string name="confirm_device_credential_password">Use password</string>
    <string name="copy_toast_msg">Link copied to clipboard</string>
    <string name="default_error_msg">Unknown error</string>
    <string name="default_web_client_id">1073063711068-lgh91rqh8nhahitt24v51p2aheru87n7.apps.googl
    <string name="fallback_menu_item_copy_link">Copy link</string>
    <string name="fallback_menu_item_open_in_browser">Open in browser</string>
    <string name="fallback_menu_item_share_link">Share link</string>
    <string name="fcm_fallback_notification_channel_label">Miscellaneous</string>
    <string name="fingerprint_dialog_touch_sensor">Touch the fingerprint sensor</string>
    <string name="fingerprint_error_hw_not_available">Fingerprint hardware not available.</string>
    <string name="fingerprint_error_hw_not_present">This device does not have a fingerprint sensor
    <string name="fingerprint_error_lockout">Too many attempts. Please try again later.</string>
    <string name="fingerprint_error_no_fingerprints">No fingerprints enrolled.</string>
    <string name="fingerprint_error_user_canceled">Fingerprint operation canceled by user.</string
    <string name="fingerprint_not_recognized">Not recognized</string>
    <string name="gcm_defaultSenderId">1073063711068</string>
    <string name="generic_error_no_device_credential">No PIN, pattern, or password set.</string>
    <string name="generic_error_no_keyguard">This device does not support PIN, pattern, or passwor
    <string name="generic_error_user_canceled">Authentication canceled by user.</string>
    <string name="google_api_key">AIzaSyDtbl-G-9Xwp81FYRVDAla5Tc4pfrO5Rr4</string>
    <string name="google_app_id">1:1073063711068:android:60a7e7b7f90292f4787199</string>
    <string name="google_crash_reporting_api_key">AIzaSyDtbl-G-9Xwp81FYRVDAla5Tc4pfrO5Rr4</string>
```

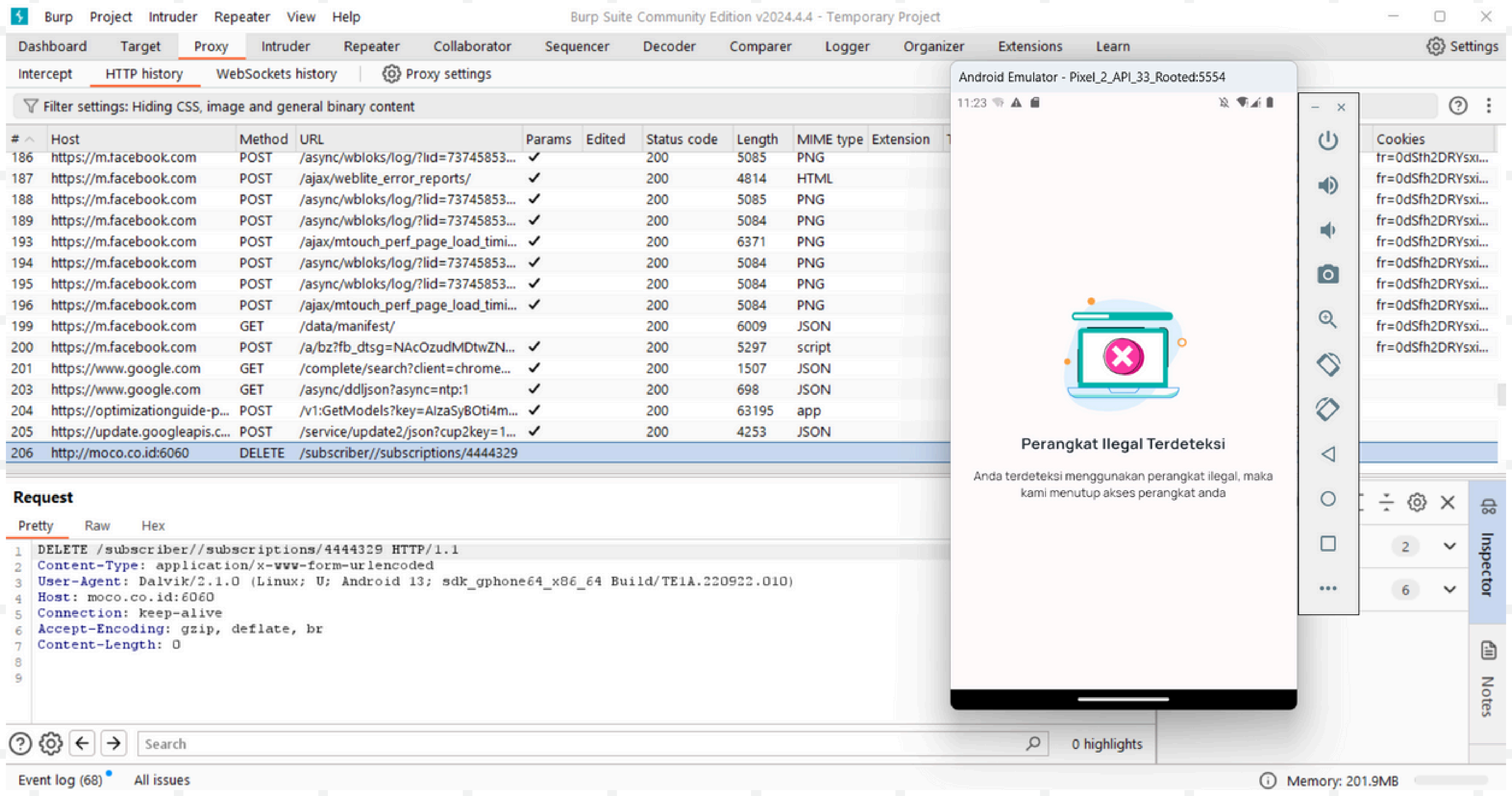
Hardcoded API keys can be extracted and abused by attackers. This can lead to unauthorized access to Google services, potentially resulting in data breaches, quota exhaustion, or financial costs due to misuse.

MSTG-CRYPTO-1 : API KEY & APP ID (Low-High)

SATUSEHAT

No Root Check

ROADBLOCK


Burp Suite Community Edition v2024.4.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Android Emulator - Pixel_2_API_33_Rooted:5554

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Cookies
186	https://m.facebook.com	POST	/async/wbloks/log/?lid=73745853...	✓		200	5085	PNG		fr=0dSfh2DRYsxi...
187	https://m.facebook.com	POST	/ajax/weblite_error_reports/	✓		200	4814	HTML		fr=0dSfh2DRYsxi...
188	https://m.facebook.com	POST	/async/wbloks/log/?lid=73745853...	✓		200	5085	PNG		fr=0dSfh2DRYsxi...
189	https://m.facebook.com	POST	/async/wbloks/log/?lid=73745853...	✓		200	5084	PNG		fr=0dSfh2DRYsxi...
193	https://m.facebook.com	POST	/ajax/mtouch_perf_page_load_timi...	✓		200	6371	PNG		fr=0dSfh2DRYsxi...
194	https://m.facebook.com	POST	/async/wbloks/log/?lid=73745853...	✓		200	5084	PNG		fr=0dSfh2DRYsxi...
195	https://m.facebook.com	POST	/async/wbloks/log/?lid=73745853...	✓		200	5084	PNG		fr=0dSfh2DRYsxi...
196	https://m.facebook.com	POST	/ajax/mtouch_perf_page_load_timi...	✓		200	5084	PNG		fr=0dSfh2DRYsxi...
199	https://m.facebook.com	GET	/data/manifest/			200	6009	JSON		fr=0dSfh2DRYsxi...
200	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcOzudMDtwZN...	✓		200	5297	script		fr=0dSfh2DRYsxi...
201	https://www.google.com	GET	/complete/search?client=chrome...	✓		200	1507	JSON		
203	https://www.google.com	GET	/async/ddljson?async=ntp:1	✓		200	698	JSON		
204	https://optimizationguide-p...	POST	/v1:GetModels?key=AIzaSyBOti4m...	✓		200	63195	app		
205	https://update.googleapis.c...	POST	/service/update2/json?cup2key=1...	✓		200	4253	JSON		
206	http://moco.co.id:6060	DELETE	/subscriber//subscriptions/4444329							

Request

Pretty Raw Hex

```
DELETE /subscriber//subscriptions/4444329 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 13; sdk_gphone64_x86_64 Build/TE1A.220922.010)
Host: moco.co.id:6060
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
Content-Length: 0
```

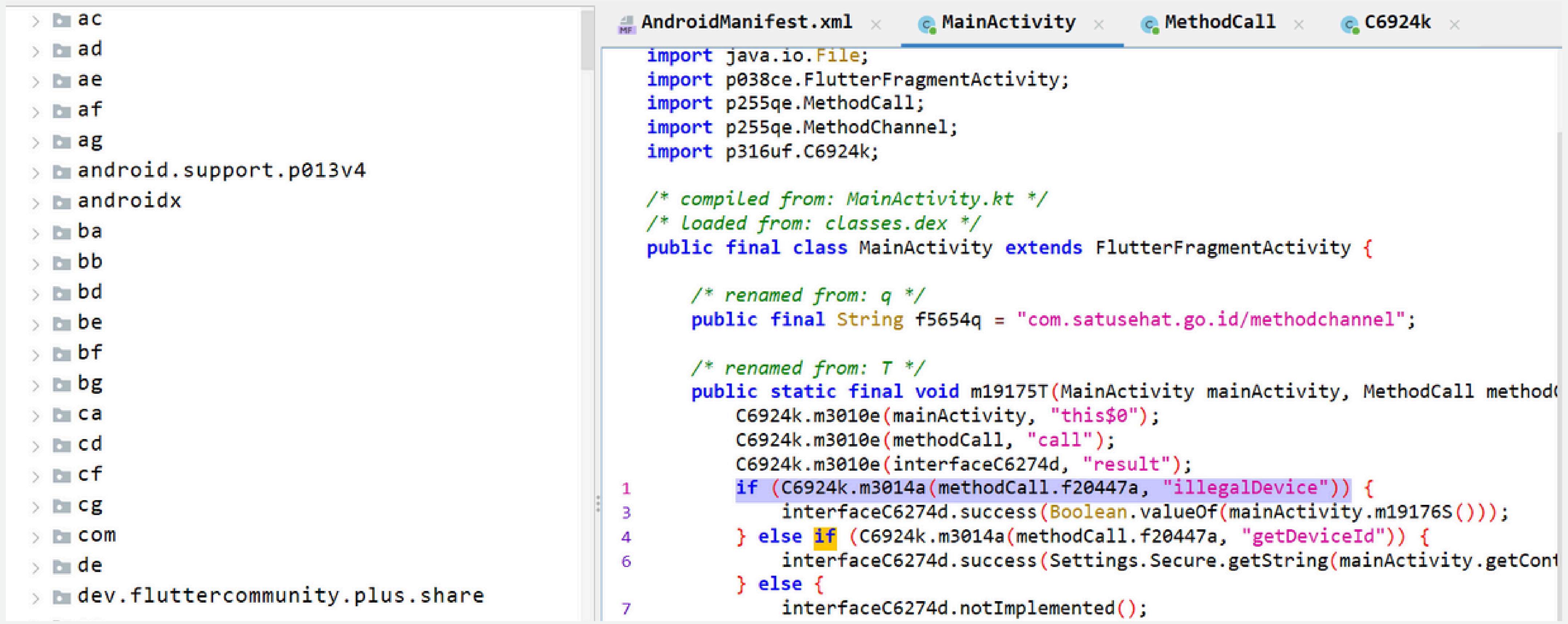
Perangkat Ilegal Terdeteksi

Anda terdeteksi menggunakan perangkat ilegal, maka kami menutup akses perangkat anda

Setting Burpsuit Proxy detects the device as Illegal

SATUSEHAT

POSSIBLE WAYS



```
ac
ad
ae
af
ag
android.support.p013v4
androidx
ba
bb
bd
be
bf
bg
ca
cd
cf
cg
com
de
dev.fluttercommunity.plus.share
```

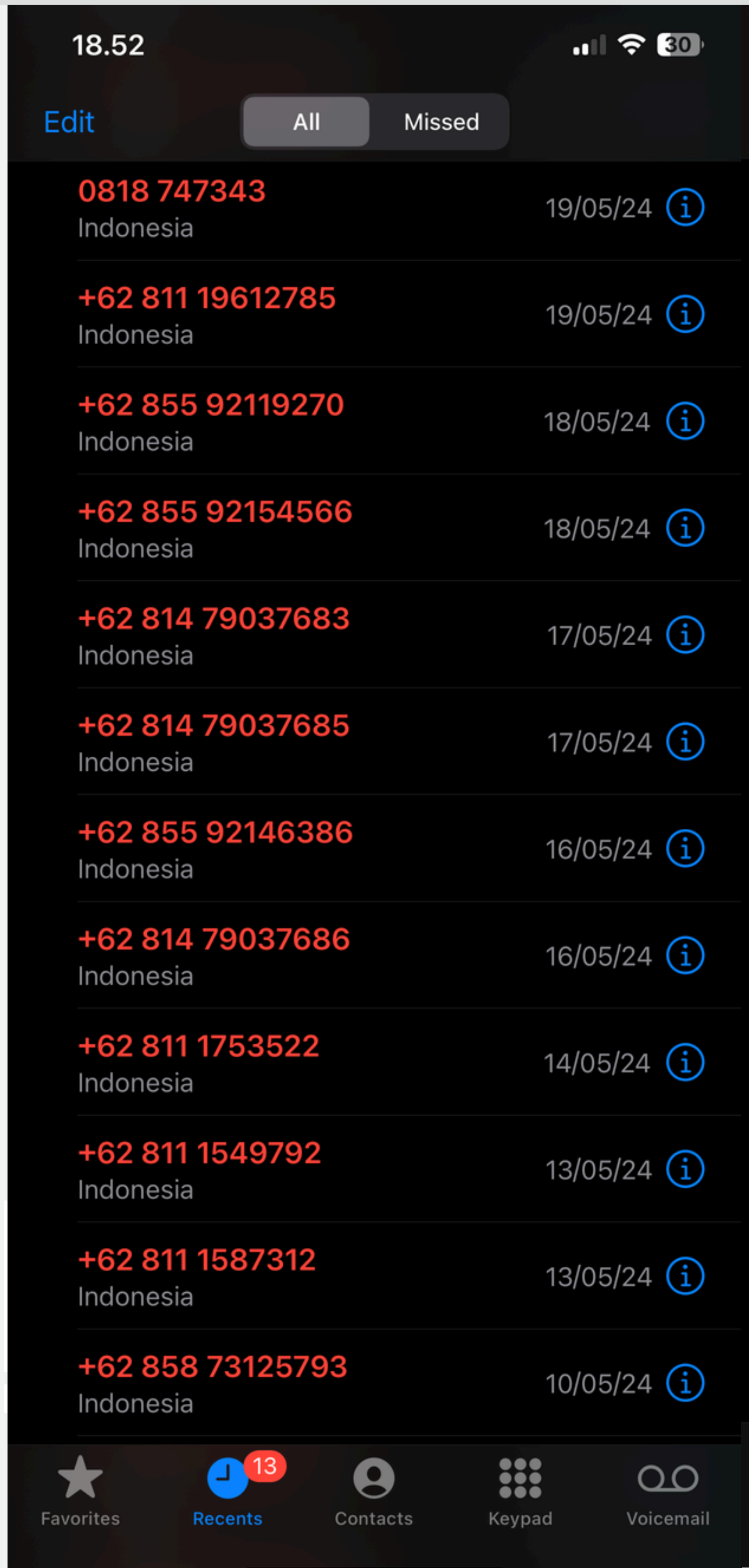
AndroidManifest.xml × MainActivity × MethodCall × C6924k ×

```java
import java.io.File;
import p038ce.FlutterFragmentActivity;
import p255qe.MethodCall;
import p255qe.MethodChannel;
import p316uf.C6924k;

/* compiled from: MainActivity.kt */
/* loaded from: classes.dex */
public final class MainActivity extends FlutterFragmentActivity {

    /* renamed from: q */
    public final String f5654q = "com.satusehat.go.id/methodchannel";

    /* renamed from: T */
    public static final void m19175T(MainActivity mainActivity, MethodCall method
        C6924k.m3010e(mainActivity, "this$0");
        C6924k.m3010e(methodCall, "call");
        C6924k.m3010e(interfaceC6274d, "result");
        if (C6924k.m3014a(methodCall.f20447a, "illegalDevice")) {
            interfaceC6274d.success(Boolean.valueOf(mainActivity.m19176S()));
        } else if (C6924k.m3014a(methodCall.f20447a, "getDeviceId")) {
            interfaceC6274d.success(Settings.Secure.getString(mainActivity.getCont
        } else {
            interfaceC6274d.notImplemented();
```

Deleting/Modifying the “Illegal Device” Function but this results to the App not functioning completely

SATUSEHAT

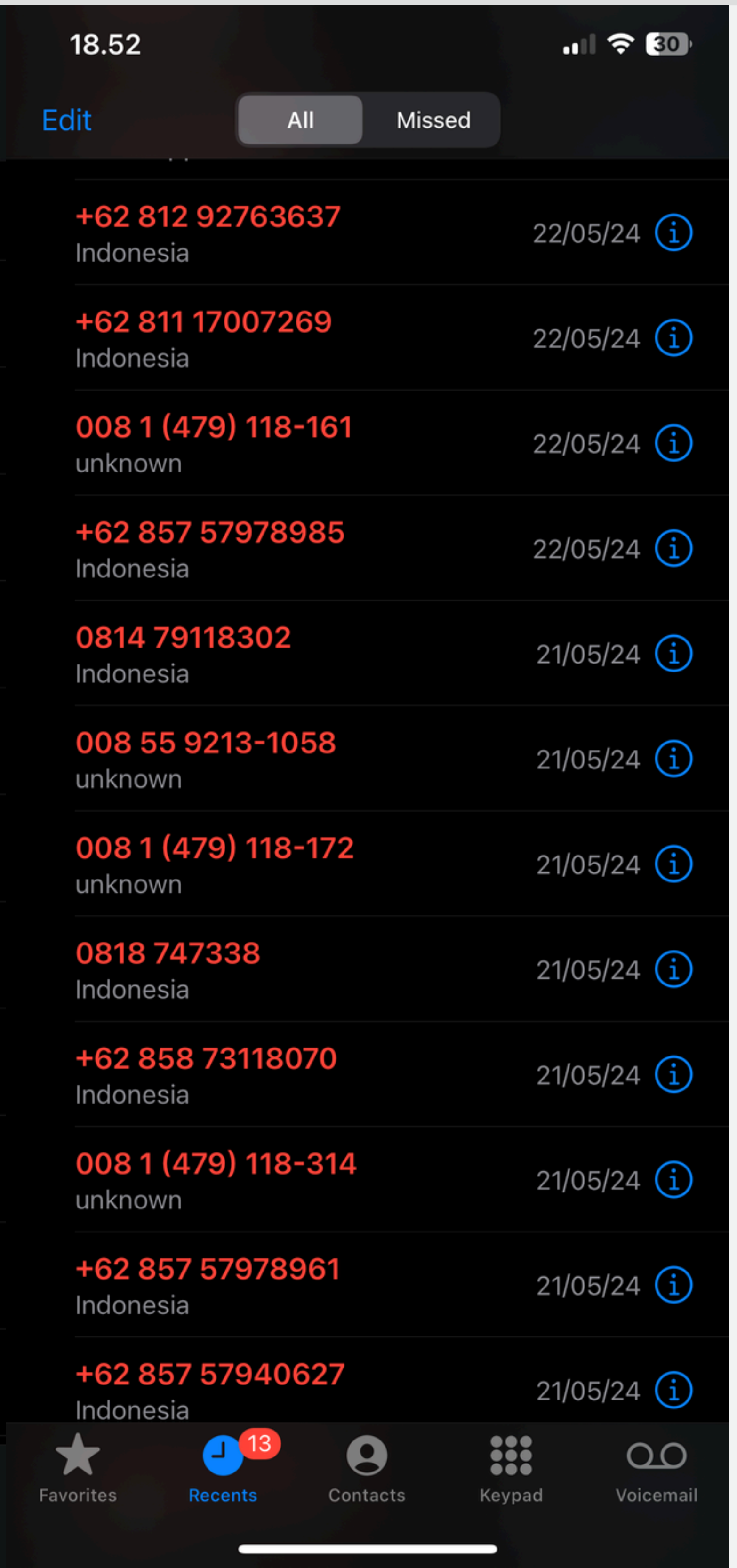
WEIRD STUFF THAT HAPPENED



18.52

Edit | All | Missed

0818 747343 — Indonesia — 19/05/24
+62 811 19612785 — Indonesia — 19/05/24
+62 855 92119270 — Indonesia — 18/05/24
+62 855 92154566 — Indonesia — 18/05/24
+62 814 79037683 — Indonesia — 17/05/24
+62 814 79037685 — Indonesia — 17/05/24
+62 855 92146386 — Indonesia — 16/05/24
+62 814 79037686 — Indonesia — 16/05/24
+62 811 1753522 — Indonesia — 14/05/24
+62 811 1549792 — Indonesia — 13/05/24
+62 811 1587312 — Indonesia — 13/05/24
+62 858 73125793 — Indonesia — 10/05/24



18.52

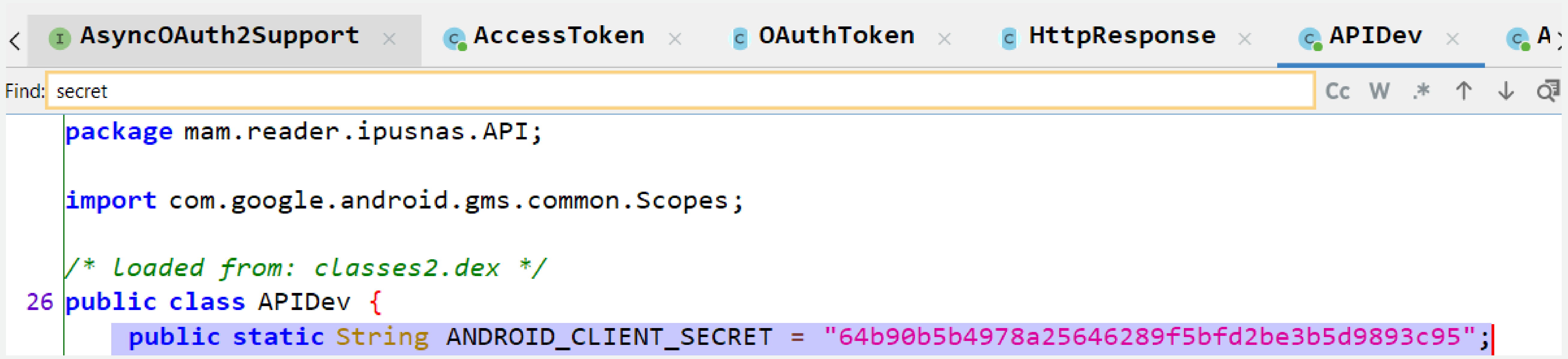
Edit | All | Missed

+62 812 92763637 — Indonesia — 22/05/24
+62 811 17007269 — Indonesia — 22/05/24
008 1 (479) 118-161 — unknown — 22/05/24
+62 857 57978985 — Indonesia — 22/05/24
0814 79118302 — Indonesia — 21/05/24
008 55 9213-1058 — unknown — 21/05/24
008 1 (479) 118-172 — unknown — 21/05/24
0818 747338 — Indonesia — 21/05/24
+62 858 73118070 — Indonesia — 21/05/24
008 1 (479) 118-314 — unknown — 21/05/24
+62 857 57978961 — Indonesia — 21/05/24
+62 857 57940627 — Indonesia — 21/05/24

Random unknown calls after signing up

SATUSEHAT

STATIC ANALYSIS FINDINGS



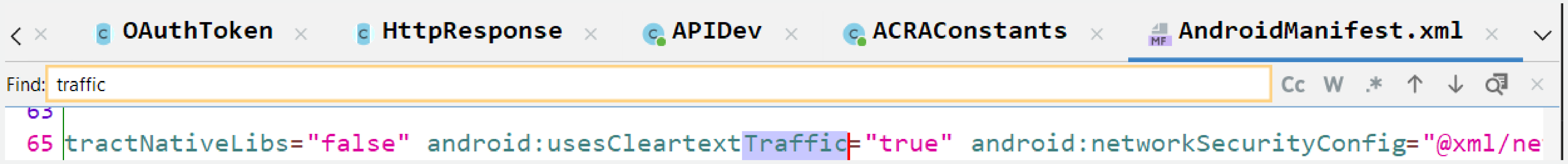
```
package mam.reader.ipusnas.API;

import com.google.android.gms.common.Scopes;

/* loaded from: classes2.dex */
public class APIDev {
    public static String ANDROID_CLIENT_SECRET = "64b90b5b4978a25646289f5bfd2be3b5d9893c95";
```

MSTG-CRYPTO-1 : HardCoded Secret Key (Low-High)

A hardcoded secret key can be extracted from the application binary, allowing attackers to gain unauthorized access to APIs or services. This could lead to significant data breaches or unauthorized actions within the system.

IPUSNAS

STATIC ANALYSIS FINDINGS



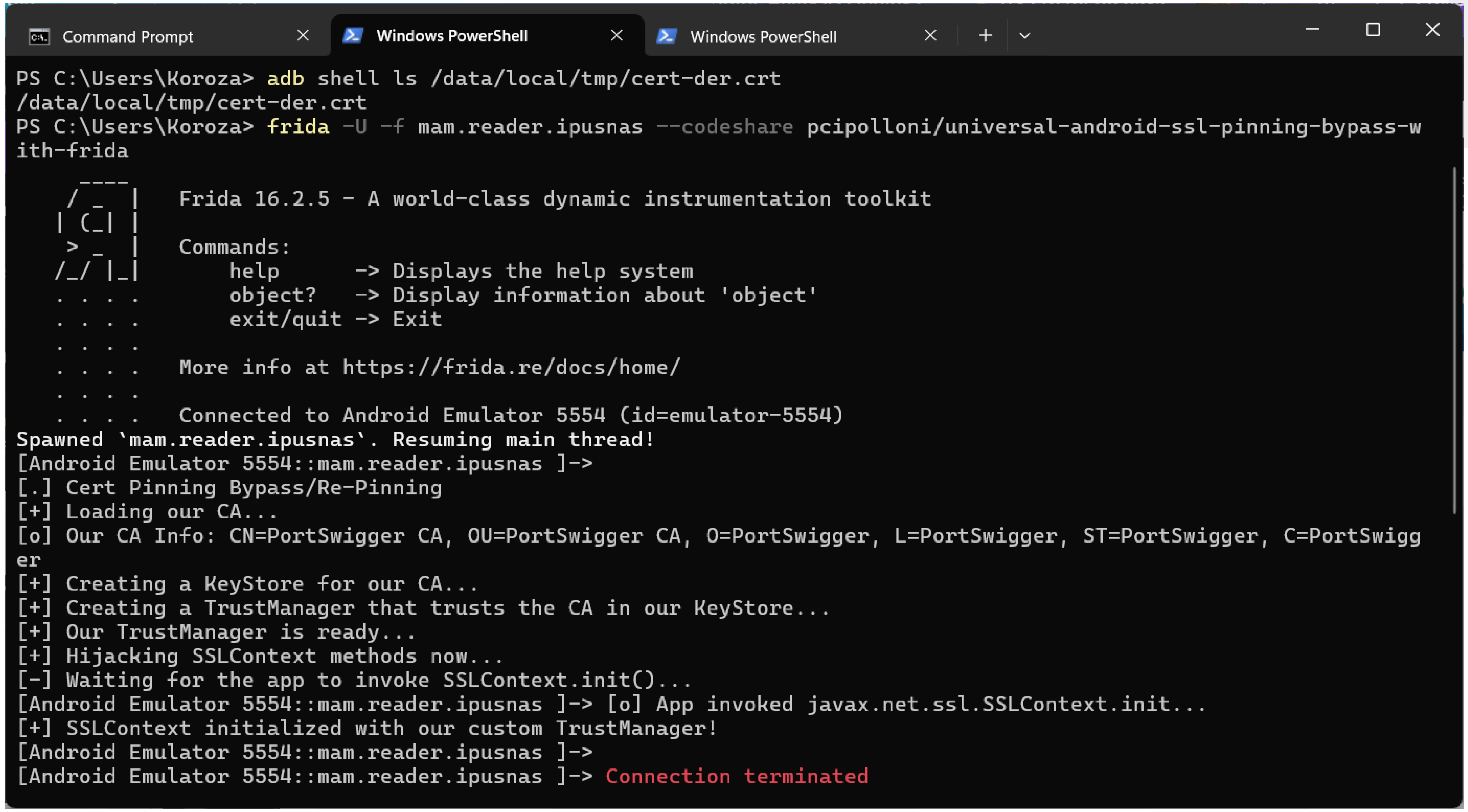
```
tractNativeLibs="false"  android:usesCleartextTraffic="true"  android:networkSecurityConfig="@xml/ne
```

MSTG-NETWORK-1 : Clear Text Traffic HTTP (Low-Medium)

Using clear text traffic means data can be intercepted in transit, leading to potential data leakage or man-in-the-middle attacks. However, the severity depends on the type of data transmitted.

IPUSNAS

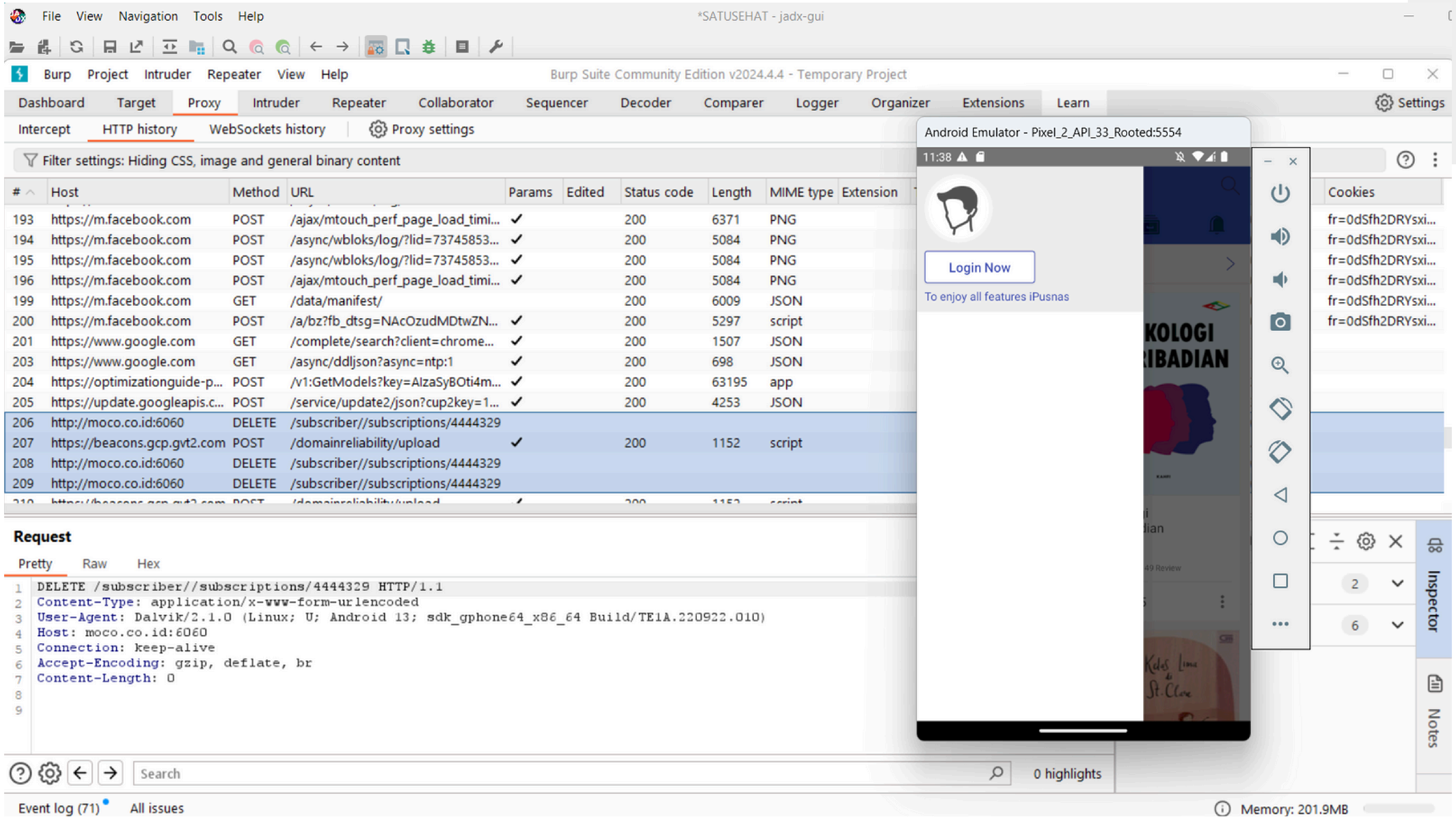
What We Have Done



```
PS C:\Users\Koroza> adb shell ls /data/local/tmp/cert-der.crt
/data/local/tmp/cert-der.crt
PS C:\Users\Koroza> frida -U -f mam.reader.ipusnas --codeshare pcipolloni/universal-android-ssl-pinning-bypass-w
ith-frida
     ____
    / _  |   Frida 16.2.5 - 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 `mam.reader.ipusnas`. Resuming main thread!
[Android Emulator 5554::mam.reader.ipusnas ]->
[.] Cert Pinning Bypass/Re-Pinning
[+] Loading our CA...
[o] Our CA Info: CN=PortSwigger CA, OU=PortSwigger CA, O=PortSwigger, L=PortSwigger, ST=PortSwigger, C=PortSwigg
er
[+] Creating a KeyStore for our CA...
[+] Creating a TrustManager that trusts the CA in our KeyStore...
[+] Our TrustManager is ready...
[+] Hijacking SSLContext methods now...
[-] Waiting for the app to invoke SSLContext.init()...
[Android Emulator 5554::mam.reader.ipusnas ]-> [o] App invoked javax.net.ssl.SSLContext.init...
[+] SSLContext initialized with our custom TrustManager!
[Android Emulator 5554::mam.reader.ipusnas ]->
[Android Emulator 5554::mam.reader.ipusnas ]-> Connection terminated
```

Trying out SSL pinning bypass using Frida

What We Have Done


File View Navigation Tools Help
*SATUSEHAT - jadx-gui
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2024.4.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Android Emulator - Pixel_2_API_33_Rooted:5554
11:38
Login Now
To enjoy all features iPusnas
KOLOGI
IBADIAN
Inspector
Notes
Event log (71) All issues
Memory: 201.9MB
0 highlights
Search

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Cookies
193	https://m.facebook.com	POST	/ajax/mtouch_perf_page_load_timi...	✓		200	6371	PNG		fr=0dSfh2DRYsxi...
194	https://m.facebook.com	POST	/async/wbloks/log/?lid=73745853...	✓		200	5084	PNG		fr=0dSfh2DRYsxi...
195	https://m.facebook.com	POST	/async/wbloks/log/?lid=73745853...	✓		200	5084	PNG		fr=0dSfh2DRYsxi...
196	https://m.facebook.com	POST	/ajax/mtouch_perf_page_load_timi...	✓		200	5084	PNG		fr=0dSfh2DRYsxi...
199	https://m.facebook.com	GET	/data/manifest/			200	6009	JSON		fr=0dSfh2DRYsxi...
200	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcOzudMDtwZN...	✓		200	5297	script		fr=0dSfh2DRYsxi...
201	https://www.google.com	GET	/complete/search?client=chrome...	✓		200	1507	JSON		
203	https://www.google.com	GET	/async/ddljson?async=ntp:1	✓		200	698	JSON		
204	https://optimizationguide-p...	POST	/v1:GetModels?key=AIzaSyBOti4m...	✓		200	63195	app		
205	https://update.googleapis.c...	POST	/service/update2/json?cup2key=1...	✓		200	4253	JSON		
206	http://moco.co.id:6060	DELETE	/subscriber//subscriptions/4444329							
207	https://beacons.gcp.gvt2.com	POST	/domainreliability/upload	✓		200	1152	script		
208	http://moco.co.id:6060	DELETE	/subscriber//subscriptions/4444329							
209	http://moco.co.id:6060	DELETE	/subscriber//subscriptions/4444329							

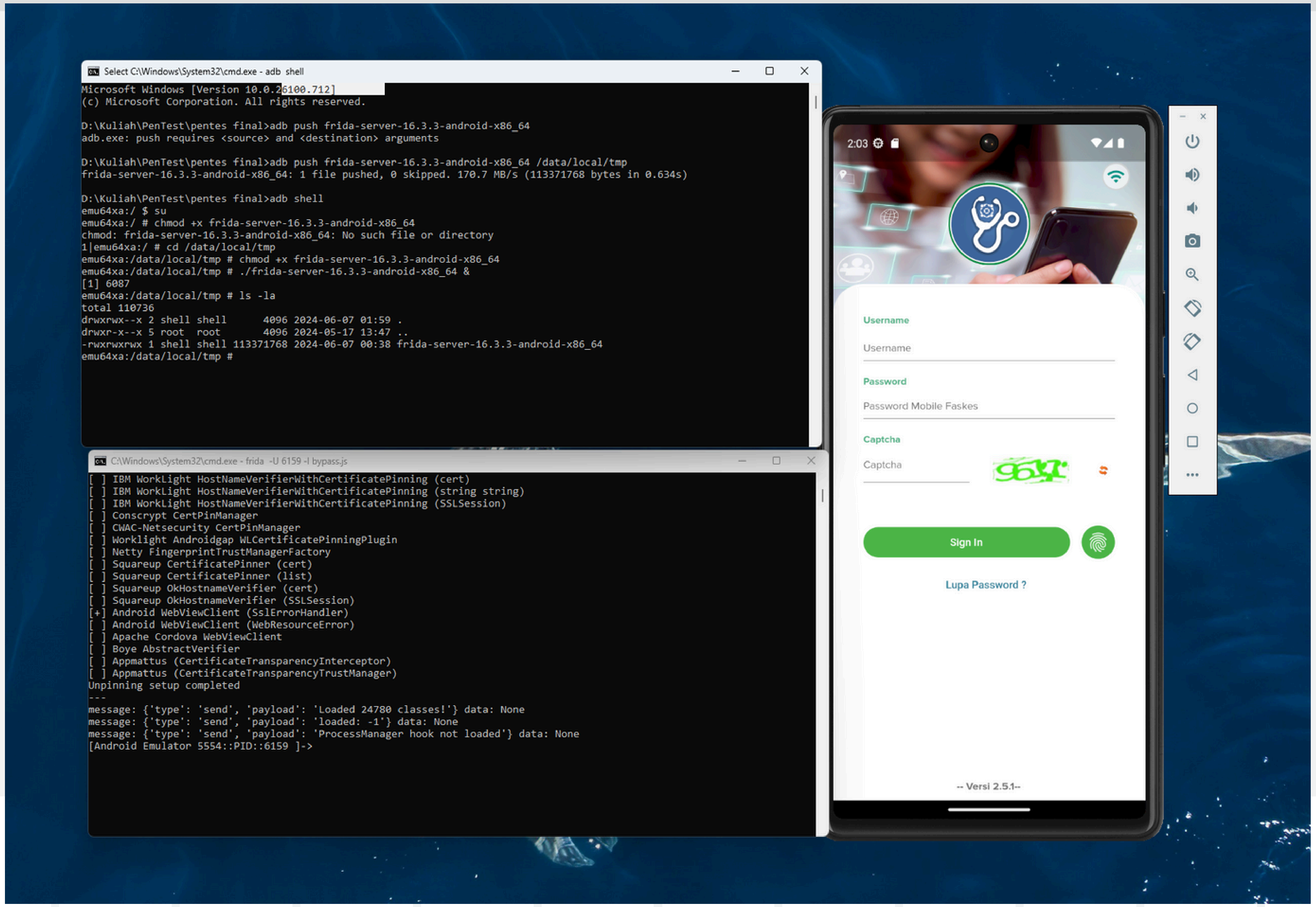
Request

Pretty Raw Hex

```
DELETE /subscriber//subscriptions/4444329 HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 13; sdk_gphone64_x86_64 Build/TE1A.220922.010)
Host: moco.co.id:6060
Connection: keep-alive
Accept-Encoding: gzip, deflate, br
Content-Length: 0


```

Trying out SSL pinning bypass using Frida

BYPASS ROOT WITH FRIDA



Select C:\Windows\System32\cmd.exe - adb shell

```
Microsoft Windows [Version 10.0.26100.712]
(c) Microsoft Corporation. All rights reserved.

D:\Kuliah\PenTest\pentes final>adb push frida-server-16.3.3-android-x86_64
adb.exe: push requires <source> and <destination> arguments

D:\Kuliah\PenTest\pentes final>adb push frida-server-16.3.3-android-x86_64 /data/local/tmp
frida-server-16.3.3-android-x86_64: 1 file pushed, 0 skipped. 170.7 MB/s (113371768 bytes in 0.634s)

D:\Kuliah\PenTest\pentes final>adb shell
emu64xa:/ $ su
emu64xa:/ # chmod +x frida-server-16.3.3-android-x86_64
chmod: frida-server-16.3.3-android-x86_64: No such file or directory
1|emu64xa:/ # cd /data/local/tmp
emu64xa:/data/local/tmp # chmod +x frida-server-16.3.3-android-x86_64
emu64xa:/data/local/tmp # ./frida-server-16.3.3-android-x86_64 &
[1] 6087
emu64xa:/data/local/tmp # ls -la
total 110736
drwxrwx--x 2 shell shell      4096 2024-06-07 01:59 .
drwxr-x--x 5 root  root       4096 2024-05-17 13:47 ..
-rwxrwxrwx 1 shell shell 113371768 2024-06-07 00:38 frida-server-16.3.3-android-x86_64
emu64xa:/data/local/tmp #
```

C:\Windows\System32\cmd.exe - frida -U 6159 -l bypass.js

```
[ ] IBM WorkLight HostNameVerifierWithCertificatePinning (cert)
[ ] IBM WorkLight HostNameVerifierWithCertificatePinning (string string)
[ ] IBM WorkLight HostNameVerifierWithCertificatePinning (SSLSession)
[ ] Conscrypt CertPinManager
[ ] CWAC-Netsecurity CertPinManager
[ ] Worklight Androidgap WLCertificatePinningPlugin
[ ] Netty FingerprintTrustManagerFactory
[ ] Squareup CertificatePinner (cert)
[ ] Squareup CertificatePinner (list)
[ ] Squareup OkHostnameVerifier (cert)
[ ] Squareup OkHostnameVerifier (SSLSession)
[+] Android WebViewClient (SslErrorHandler)
[ ] Android WebViewClient (WebResourceError)
[ ] Apache Cordova WebViewClient
[ ] Boye AbstractVerifier
[ ] Appmattus (CertificateTransparencyInterceptor)
[ ] Appmattus (CertificateTransparencyTrustManager)
Unpinning setup completed
---
message: {'type': 'send', 'payload': 'Loaded 24780 classes!'} data: None
message: {'type': 'send', 'payload': 'loaded: -1'} data: None
message: {'type': 'send', 'payload': 'ProcessManager hook not loaded'} data: None
[Android Emulator 5554::PID::6159 ]->
```

JKN Mobile