Activities

v.1.0

Ni’am Habibiy Sahid

Detail Dokumen

Judul Dokumen	: Lab Manual for Sharing Session
Tujuan Dokumen	: Universitas Amikom Purwokerto
Tanggal	: 25 Juni 2023
Tipe Dokumen	: Lab Manual
Klasifikasi	: Publik

A. Vulnerability Assesment

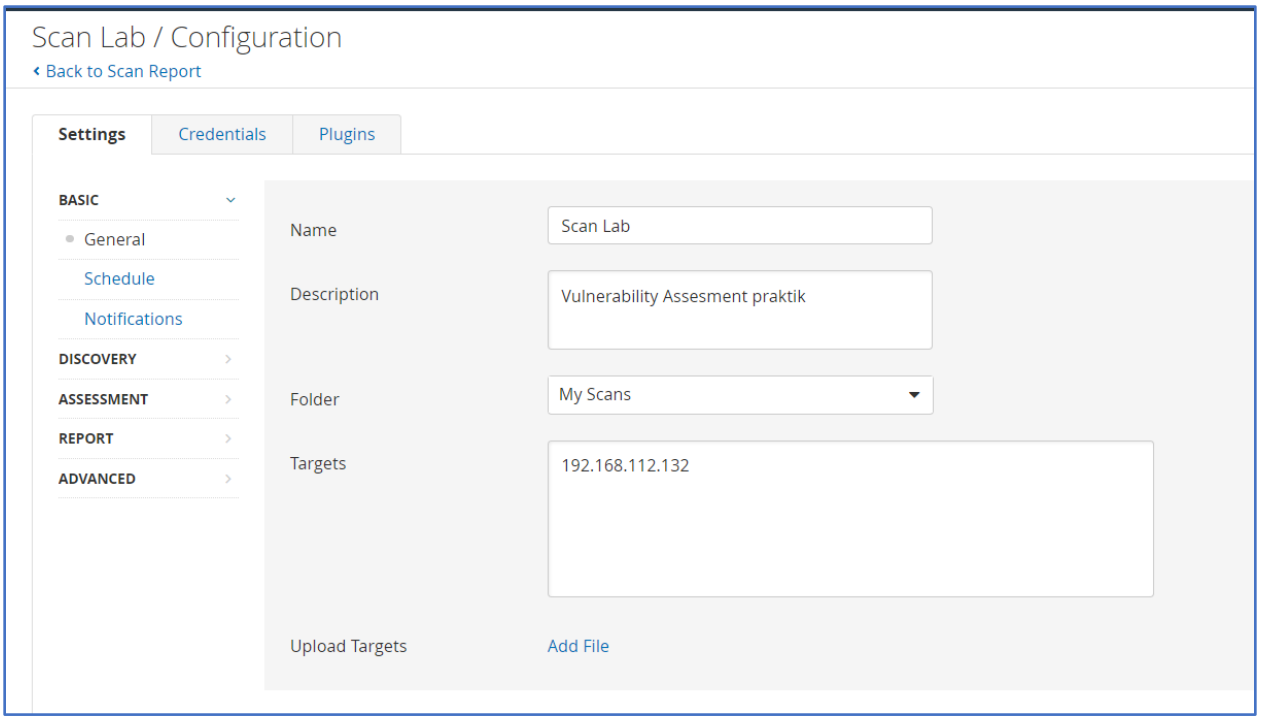
Asumsi scan dilakukan secara **black**-box

1. Nyalakan nessus
2. Klik new scan pilih advanced scan
3. Pastikan sedang ada di tab settings > basic > general
4. Isikan informasi target :

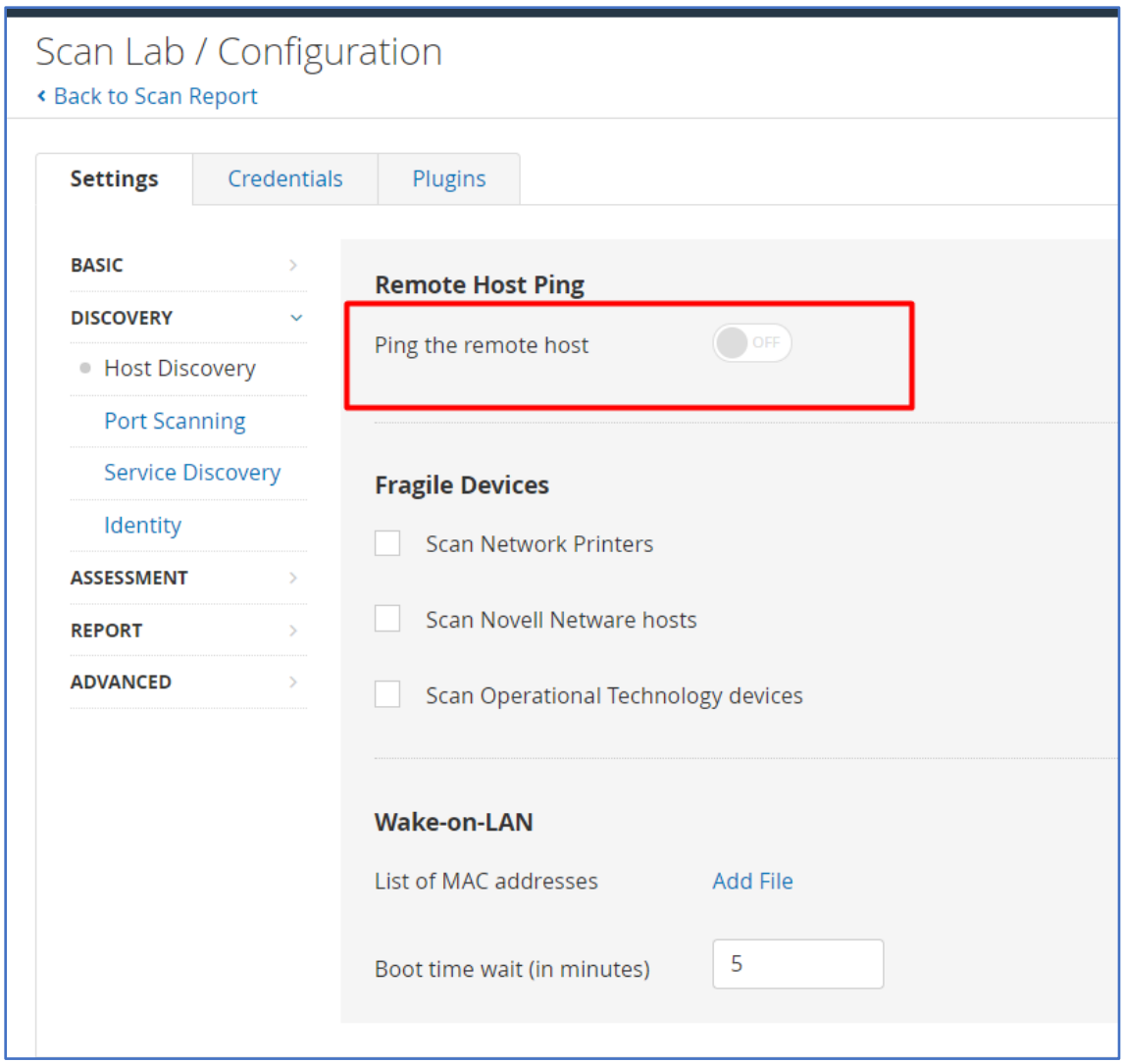
Name : Scan Lab

Description : Vulnerability Assesment praktik

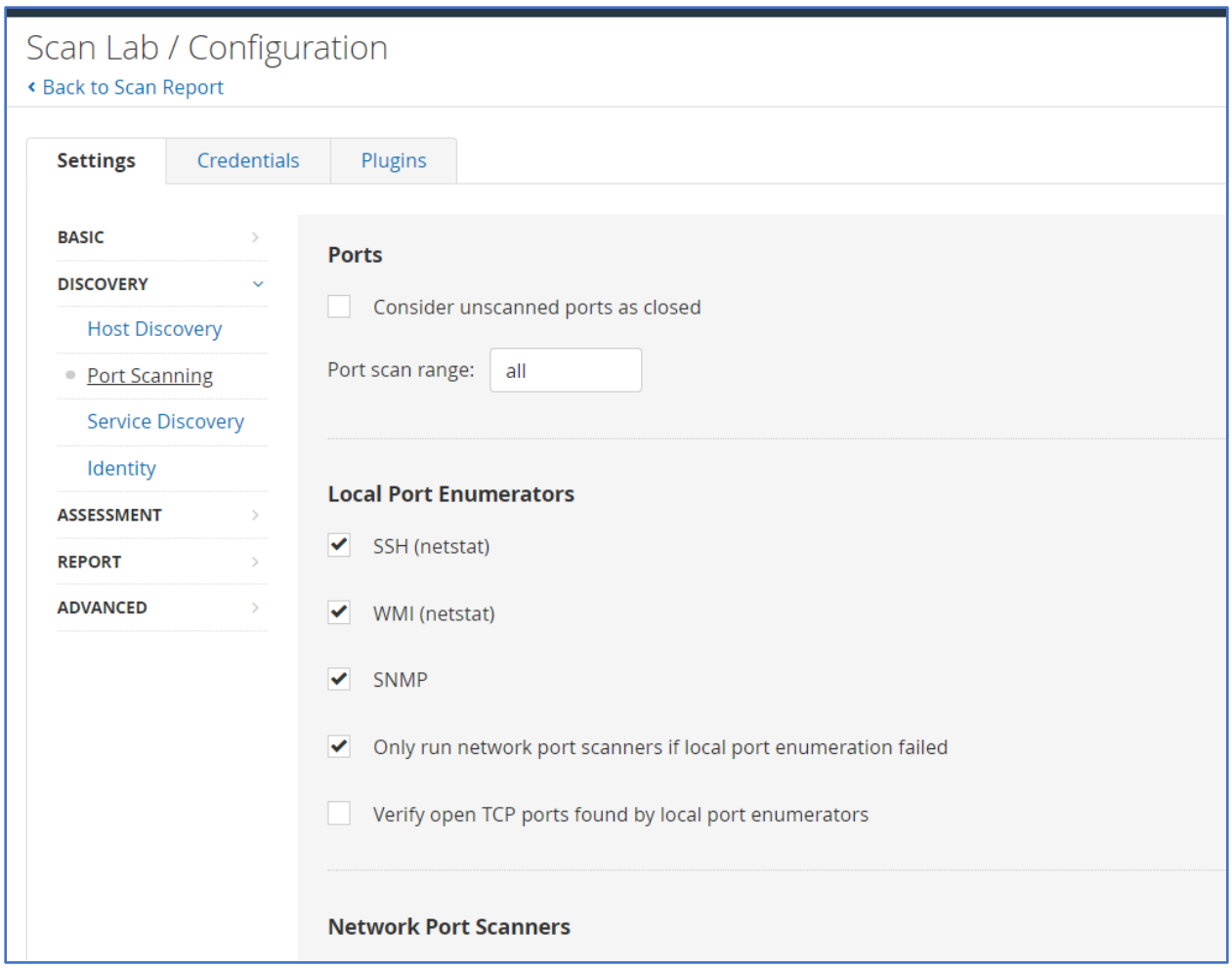
Targets : 192.168.112.132



5. Pindah ke menu Discovery > Host Discovery, matikan "Ping the remote Host"



6. Pada menu Discovery > Port Scanning, ubah "Port Scan Range" dari default menjadi all



7. Klik tombol Save
8. Launch scan
9. Ambil contoh validasi kerentanan smb signing

   nmap -p 445 --script smb2-security-mode 192.168.112.132

10. Generate report raw di Nessus
11. Contoh report va :

https://purplesec.us/wp-content/uploads/2019/12/Sample-Vulnerability-Assessment-Report-PurpleSec.pdf

B. Penetration Testing – Web Application Pentest

1. Buka port 8080, menemukan easychat server
2. Cari exploit easychat server di internet
3. Coba exploit easychat server ke target
4. Mendownload testplan wstg
   https://github.com/OWASP/wstg

5. Cara menemukan testing guide point, contohnya clickjacking
   a. Kopikan nama test nya : testing for clickjacking
   b. Kopikan kode testnya : wstg-clnt-09
   c. Cari di google : "wstg-clnt-09 testing for clickjacking"
6. Test clickjacking ke target port 80

```
<html>
  <head>
    <title>Clickjack test page</title>
  </head>
  <body>
    <iframe src="http://192.168.112.132" width="500" height="500"></iframe>
  </body>
</html>
```

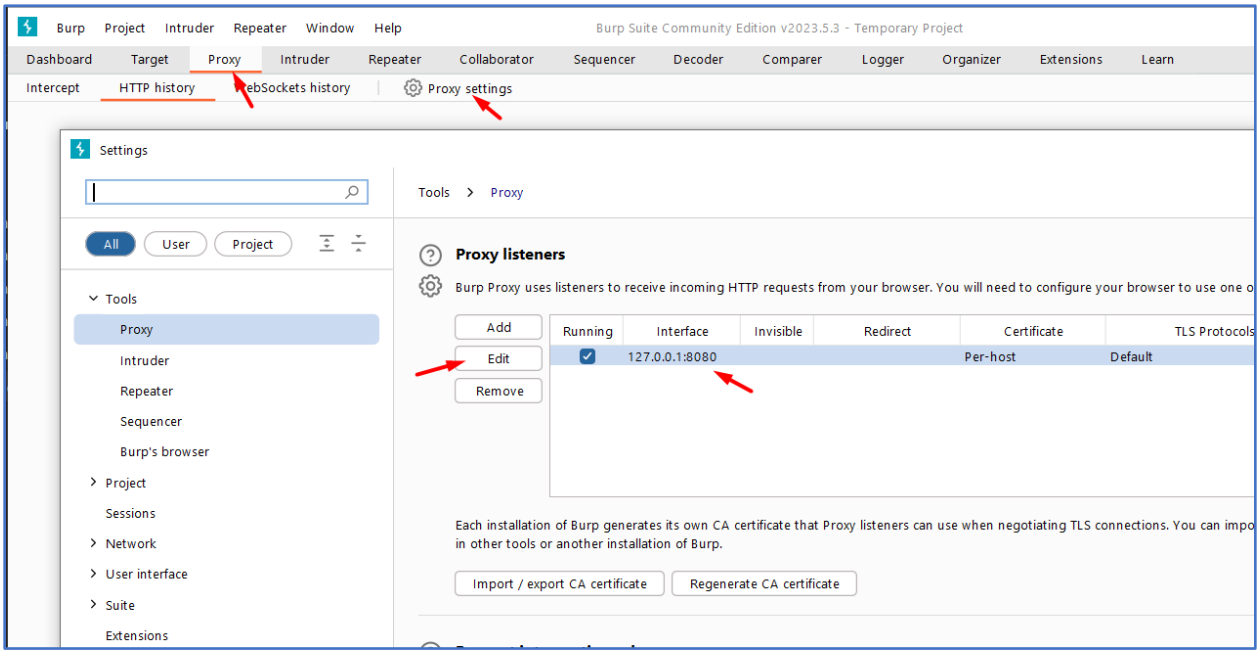
7. Buka website cvss 3.1
8. Hitung cvss 3.1 nya

C. Penetration Testing – Mobile Application Pentest

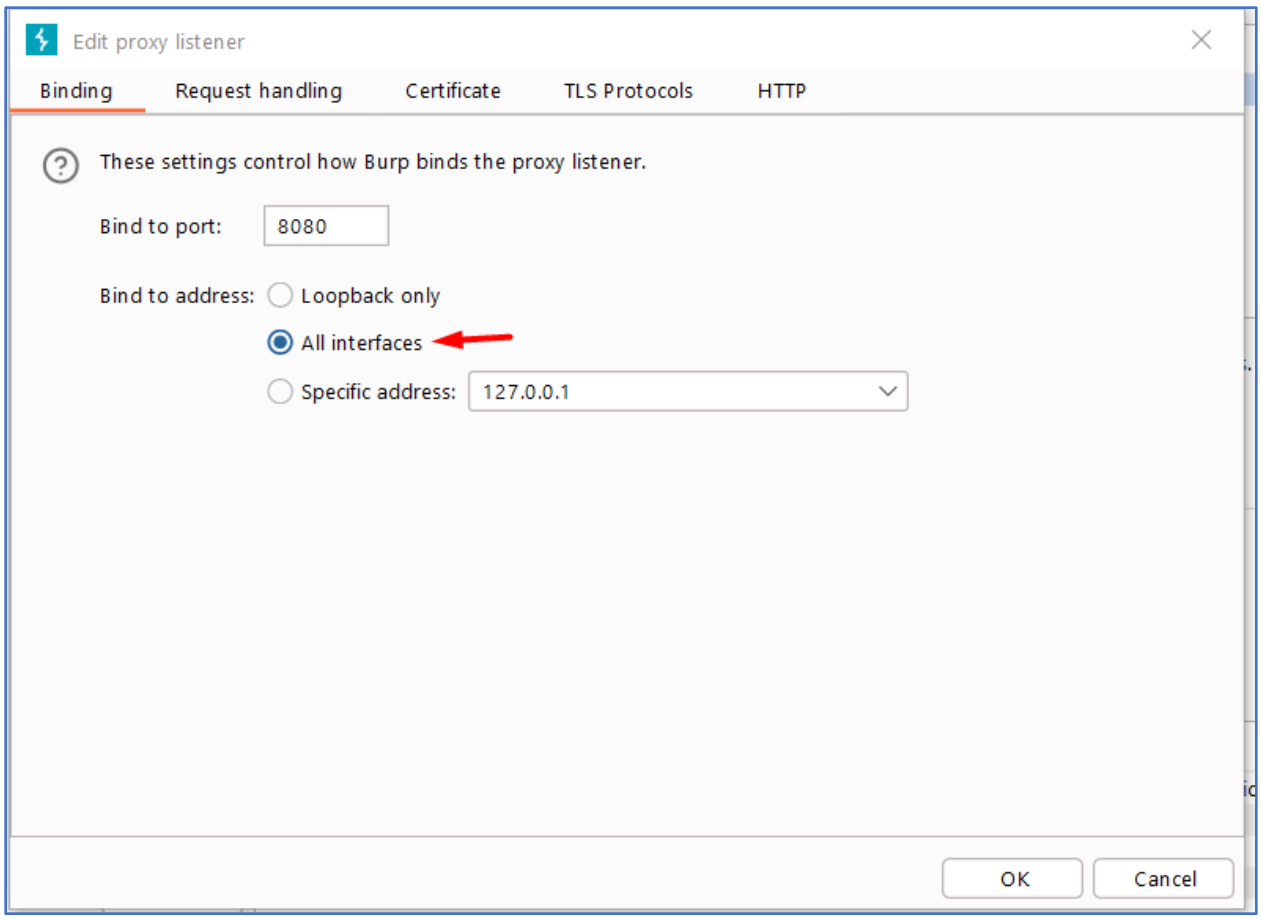
Saya mendetailkan pada bagian dynamic testing (bypass ssl pinning), mengingat kemungkinan besar waktu tidak cukup untuk menjelaskan masing masing detil langkahnya.

1. Jalankan mobsf
2. Upload file apk ke mobsf
3. Generate report
4. Jalankan aplikasi di emulator
   - Buka nox
   - Install apps pinning-demo.apk
5. Proxy kan nox ke burpsuite
   - Download burpsuite dari sini : https://portswigger.net/burp/communitydownload
   - Instalasi burpsuite lihat sini : https://portswigger.net/burp/documentation/desktop/getting-started/download-and-install

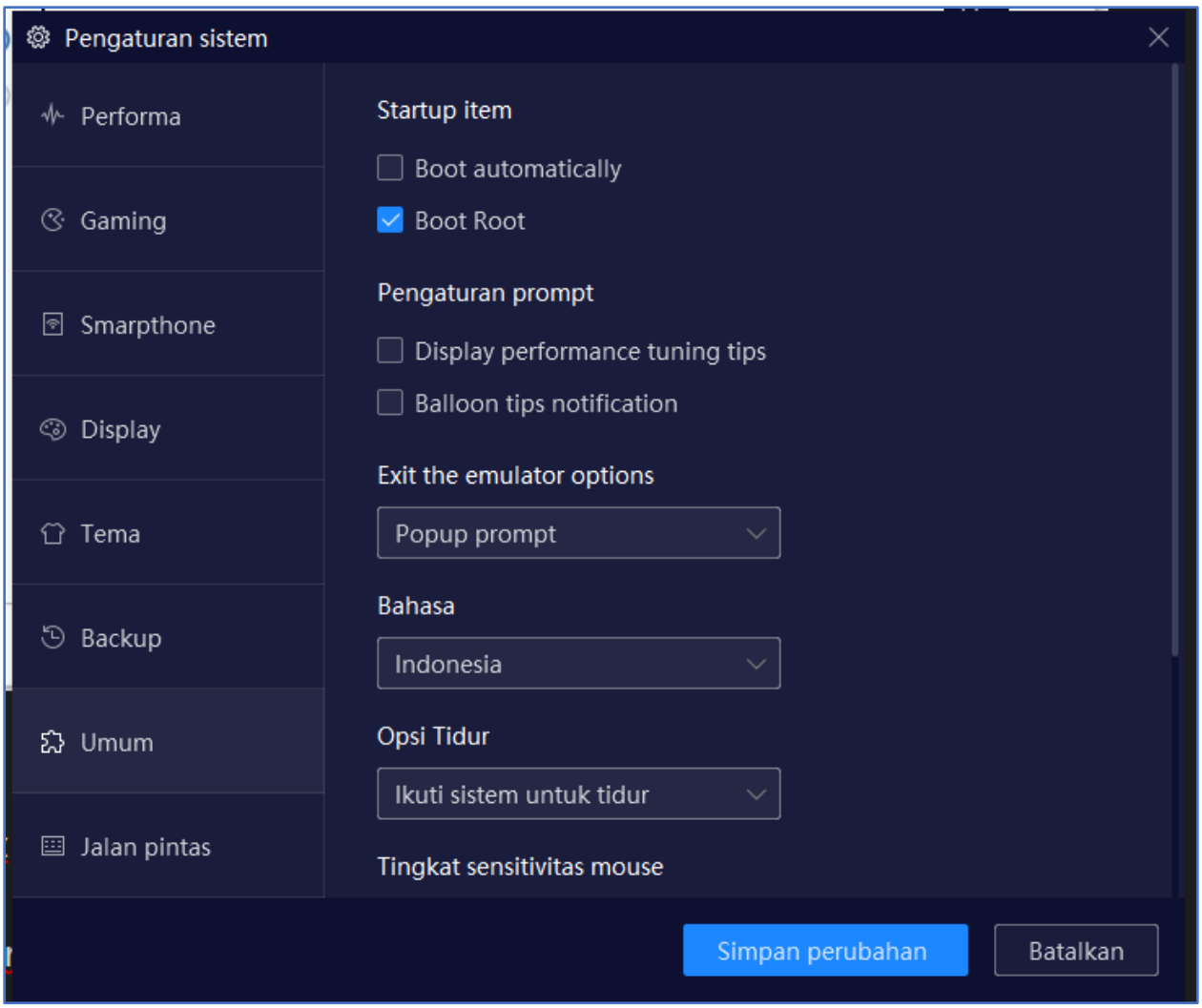
6. Setel port proxy di burpsuite untuk bisa listen di semua ip address
   - Di burpsuite pergi ke proxy > proxy setting, kemudian klik pilih proxy yang berjalan (127.0.0.1:8080) dan klik edit



   - Ubah ke All Interfaces

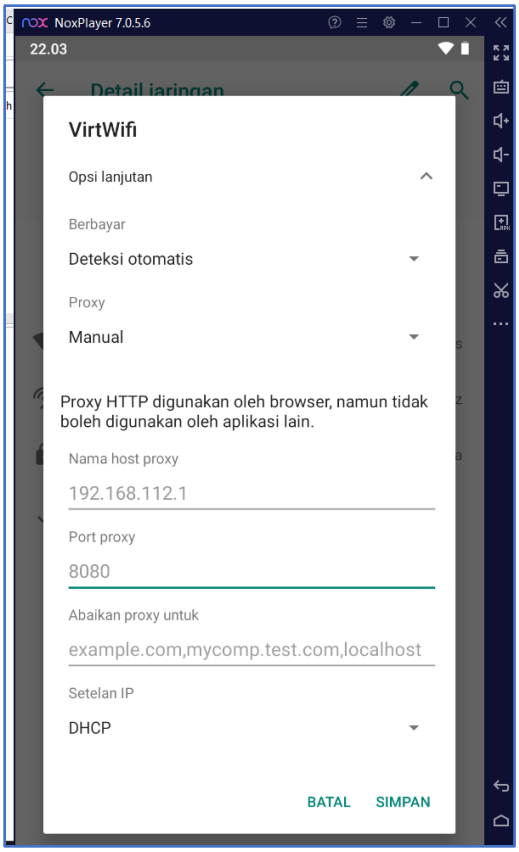


7. Setting proxy di nox (setting nox untuk boot root, install proxy droid dan setel di proxy droid)
    - Pada Nox Player, pergi ke pengaturan System > Umum, dan centang Boot Root. Nox akan merestart vm, setelah itu kita akan booting dg kondisi Rooted di nox.

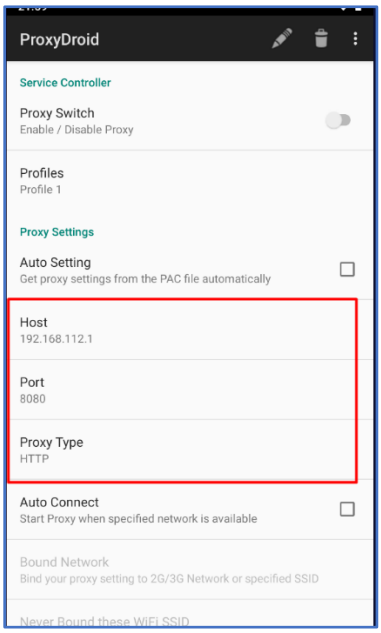


- Ada dua alternatif ketika menggunakan proxy di android, bisa dengan menyetel proxy di pengaturan wifi atau menggunakan proxydroid. Gunakan cara yang paling nyaman saja

a. Setel Proxy pada settingan koneksi di nox



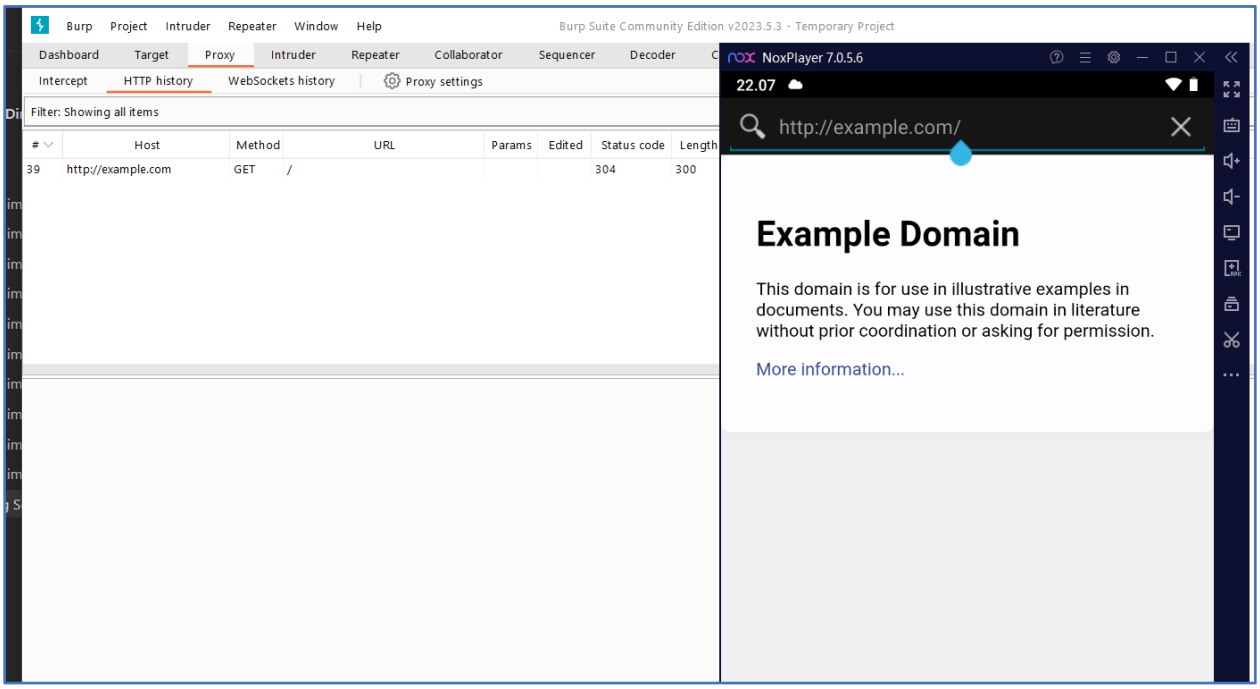
b. Menggunakan Proxy Droid. Lakukan Instalasi aplikasi proxyDroid terlebih dahulu



- Atur Host dg IP Addres PC kamu yang menjalankan burpsuite
- Port 8080 sesuai dengan settingan Burpsuite
- Proxy Type HTTP

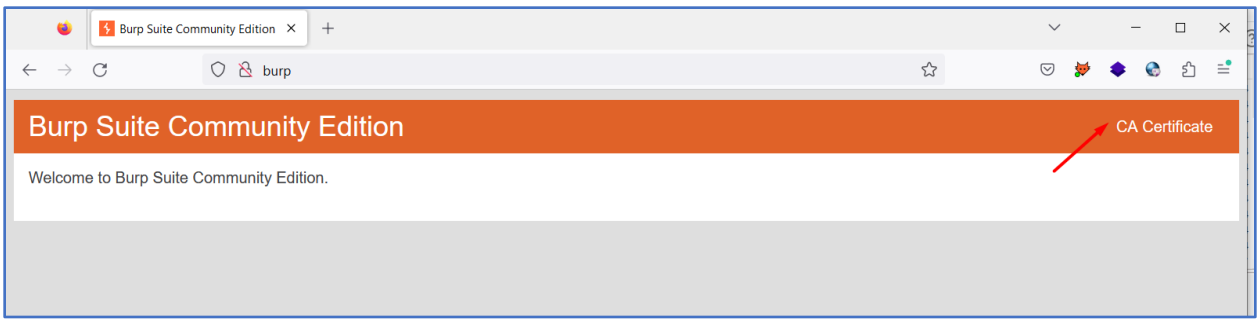
- Kemudian Turn On proxy dg meng-klik Proxy Switch

c. Kemudian untuk memastikan apakah burpsuite sudah dapat menangkap request HTTP dari nox adalah dengan mengunjungi http://example.com atau web dg koneksi http lainnya, ingat bukan https.
d. Jika burpsuite sudah menangkap request, kita akan lanjutkan dengan instalasi sertifikat postwigger di nox.

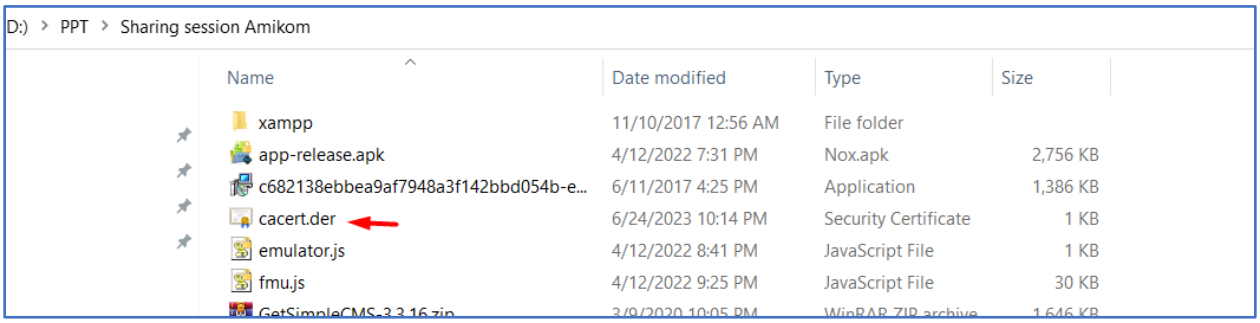


e. ketika mengunjungi website https, akan ada peringatan dari browser bahwa certificate ssl tidak valid. Hal ini dapat diatasi dengan menginstall certificate burpsuite ke device kita.

8. Install certificate burpsuite di nox
   a. Kunjungi http://burp di browser yang sudah di set proxy ke burpsuite, kemudian klik tombol CA Certificate.

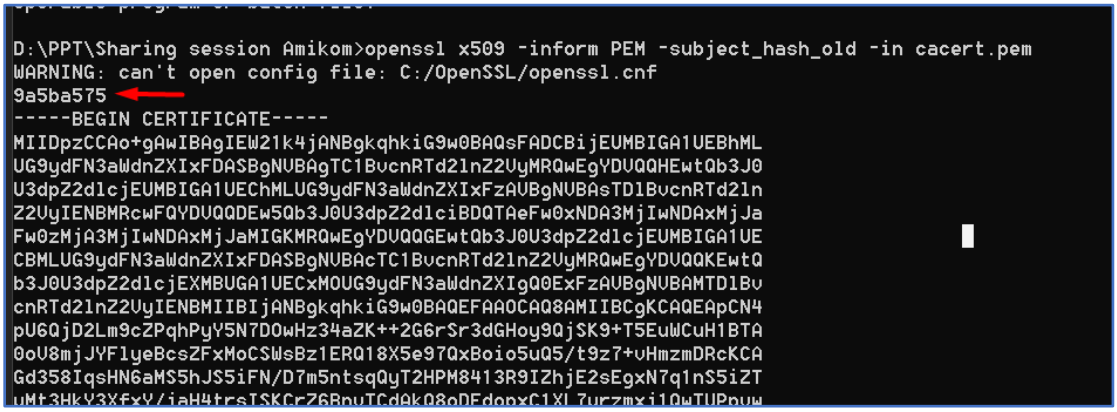


b. Cacert file akan terunduh ke PC
c. File akan tersimpan dengan ekstensi .der



d. Gunakan openssl, buat file .pem dari file der tersebut
openssl x509 -inform DER -in cacert.der -out cacert.pem

e. Kemudian cek hash nya dg parameter subject_hash_old
openssl x509 -inform PEM -subject_hash_old -in cacert.pem



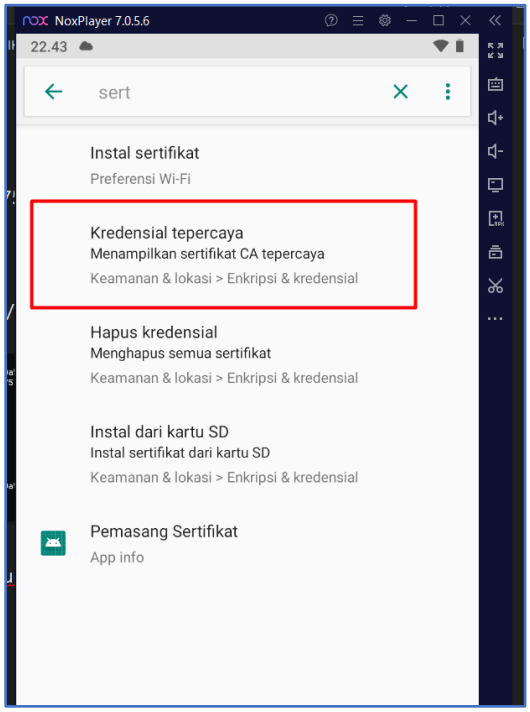
f. Ambil baris hash nya, dalam hal ini file cacert.pem saya adalah **9a5ba575**
- Kita akan upload filenya ke nox dengan nama berikut :
  <cert_hash>.0

- Punya saya menjadi :
  9a5ba575.0

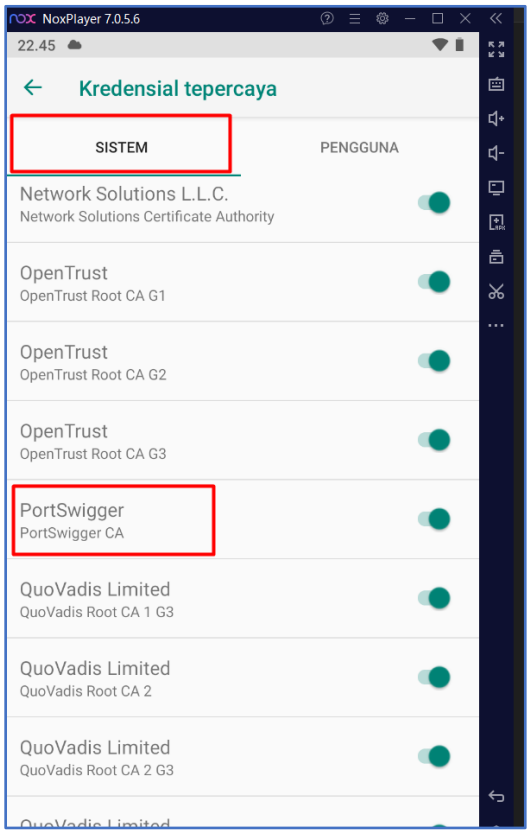
g. Ubah cacert.pem jadi 9a5ba575.0
   move cacert.pem 9a5ba575.0
h. Gunakan adb shell untuk mengupload file 9a5ba575.0 ke /system/etc/security/cacerts/
- *adb root*
- *adb remount*
- *adb push 9a5ba575.0 /system/etc/security/cacerts/9a5ba575.0*

```
D:\PPT\Sharing session Amikom>adb push 9a5ba575.0 /system/etc/security/cacerts/9a5ba575.0
adb: error: failed to copy '9a5ba575.0' to '/system/etc/security/cacerts/9a5ba575.0': couldn't create file: Read-only file system

D:\PPT\Sharing session Amikom>adb root

D:\PPT\Sharing session Amikom>adb remount
remount succeeded

D:\PPT\Sharing session Amikom>adb shell
star2lte:/ # exit

D:\PPT\Sharing session Amikom>adb push 9a5ba575.0 /system/etc/security/cacerts/9a5ba575.0
[100%] /system/etc/security/cacerts/9a5ba575.0

D:\PPT\Sharing session Amikom>
```

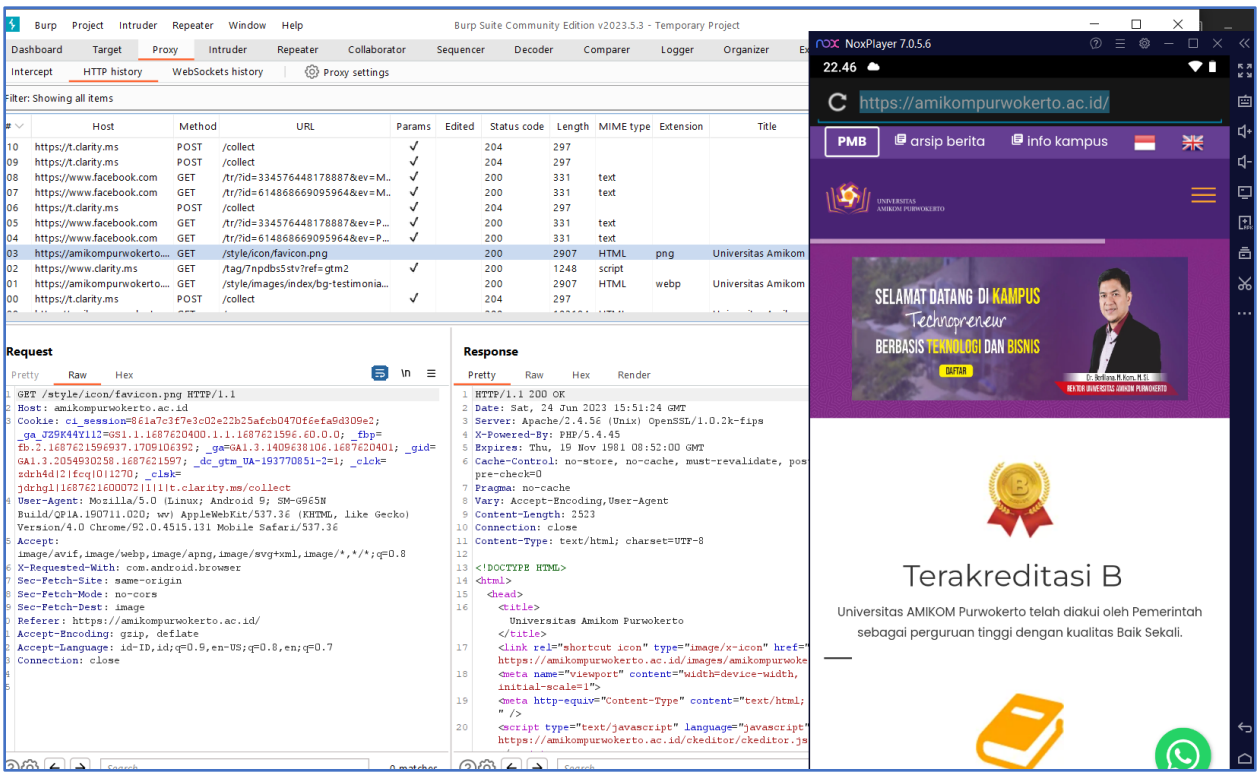
9. Masuk ke nox, pergi ke setelan, dan cari dg kata kunci "sert" atau "cert" apa bila dalam bahasa inggris.
10. Pilih Kredensial terpercaya > Kredensial Terpercaya



11. Pada bagian sistem di menu Kredensial Terpercaya, kita bisa menmukan PortSwigger sudah menjadi certificate yang terpercaya

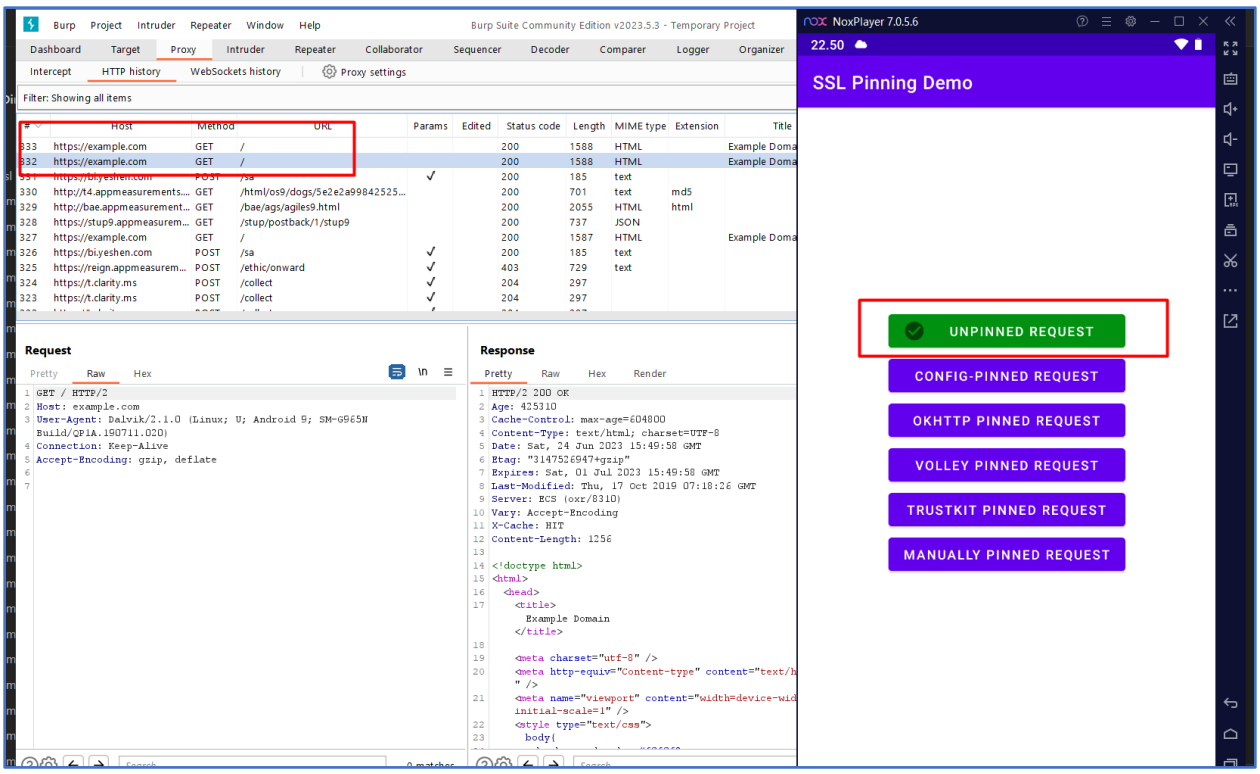


12. Untuk memastikan hasilnya, kita bisa membuka website dengan https. semisal wbesite portal amikom. Dan melihat sudah tidak ada lagi popup ydari browser yang menyatakan bahwa sertifikat tidak valid.

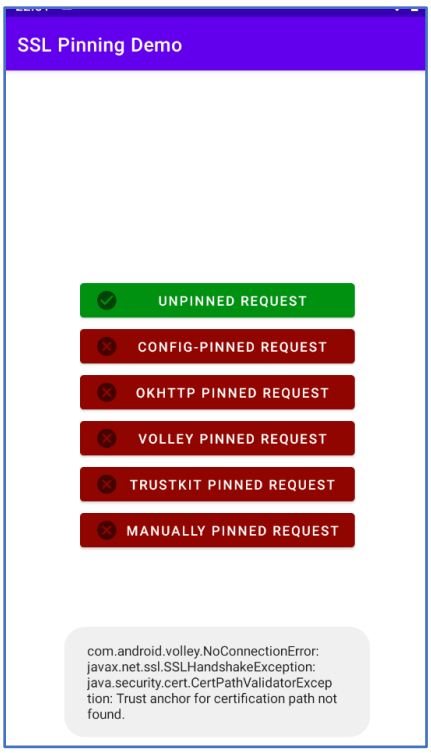


13. Kita sudah bisa melakukan tamper request dan response https pada browser di handphone, tapi proses di aplikasi, apabila ada ssl pinning, masih akan terjadi eror pada saat proses tampering, biasanya di tandai dengan request dan response tidak masuk ke HTTP History dan juga ada pesan eror pada dashboard Burpsuite.

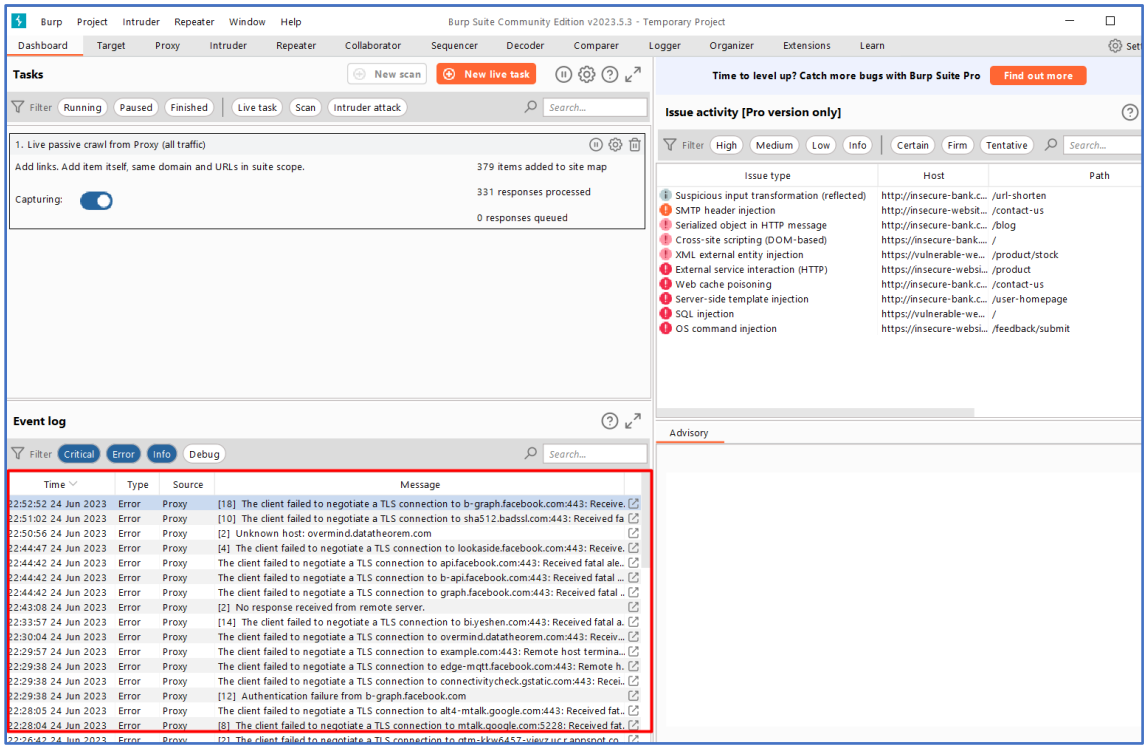
14. Jalankan apps pinning-demo.apk
15. Unpinned Request



16. Pinned Request akan menolak karena SSL certificate yang didapatkan berbeda dari yang mereka simpan.



- Pada HTTP History tidak akan ada request dan response yang berhasil di tangkap.
- Pada event log di dashboard, request yang gagal karena SSL ini dapat dilihat



17. Bypass pinning-demo.apk menggunakan frida
    a. Untuk proses upload frida, dan instalasi frida akan kita skip. Bisa cek url berikut : https://medium.com/my-infosec-write-ups/frida-installation-40f52845ae98
    b. Jalankan frida server di nox
        - adb shell
        - cd /data/local/tmp
        - ./frida15 &

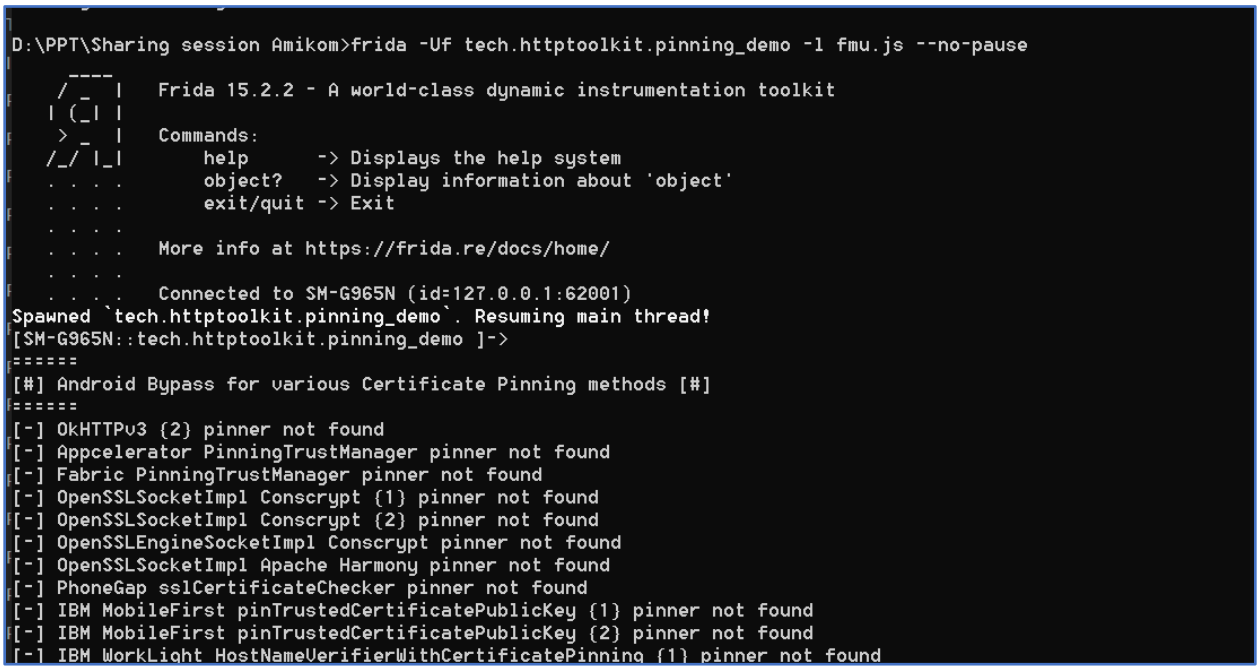
```
D:\PPT\Sharing session Amikom>adb shell
star2lte:/ # cd /data/local/tmp
star2lte:/data/local/tmp # ls
frida15 oat re.frida.server
star2lte:/data/local/tmp # ./frida15 &
[1] 9532
star2lte:/data/local/tmp #
```

    c. Cek aplikasi yang berjalan menggunakan frida pada windows
        - frida-ps -Uai

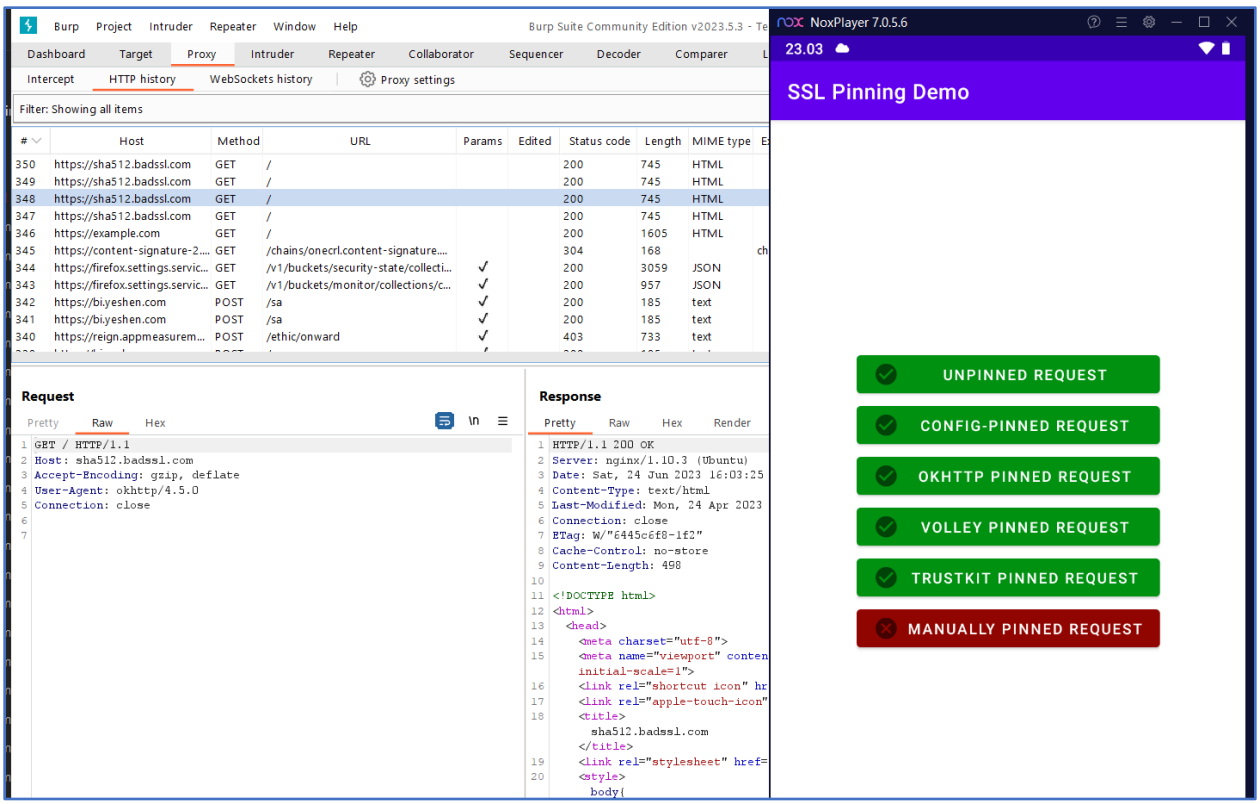
```
D:\PPT\Sharing session Amikom>frida-ps -Uai
 PID  Name                  Identifier
----  --------------------  ----------------------------
9070  Browser               com.android.browser
8792  Facebook              com.facebook.katana
7262  File                  com.android.documentsui
8284  Google Play Store     com.android.vending
4072  ProxyDroid            org.proxydroid
9292  SSL Pinning Demo      tech.httptoolkit.pinning_demo
   -  Amaze                 com.amaze.filemanager
   -  App Center            com.android.Calendar
   -  Fita                  com.muna.lively
   -  Galeri                com.android.gallery3d
   -  Gods and Demons: Legend  com.tzgames.gadand
   -  Google Play Game      com.google.android.play.games
   -  GoogleSign            com.pekall.fmradio
   -  KBM App               com.ketix.application
   -  Kamera                com.android.camera2
   -  Qoinpay               id.qoin.crypto
   -  Setelan               com.android.settings
   -  Tutorials             com.android.calculator2
   -  Wpk11 Qt              com.ytnxuul
   -  Wpk11 Qt              com.ytnxuul

D:\PPT\Sharing session Amikom>
```

d. Dapat dilihat nama package dari aplikasi SSL pinning demo, yaitu tech.httptoolkit.pinning_demo
e. Gunakan frida multiple unpinning script, untuk bypass SSL pinning
   - Script : https://codeshare.frida.re/@akabe1/frida-multiple-unpinning/
   - Saya simpan script di local dg nama fmu.js agar lebih mudah mengetik commandnya
   - Eksekusi command Frida

     frida -Uf tech.httptoolkit.pinning_demo -l fmu.js --no-pause



f. Kita sudah bisa melakukan bypass ssl pinning yang dilakukan oleh beberapa library



Untuk manually Pinned request, dapat dilakukan analisa manual dan membuat custom script, silahkan lakukan research sendiri.