**Report BoardBanker Aplliaction**

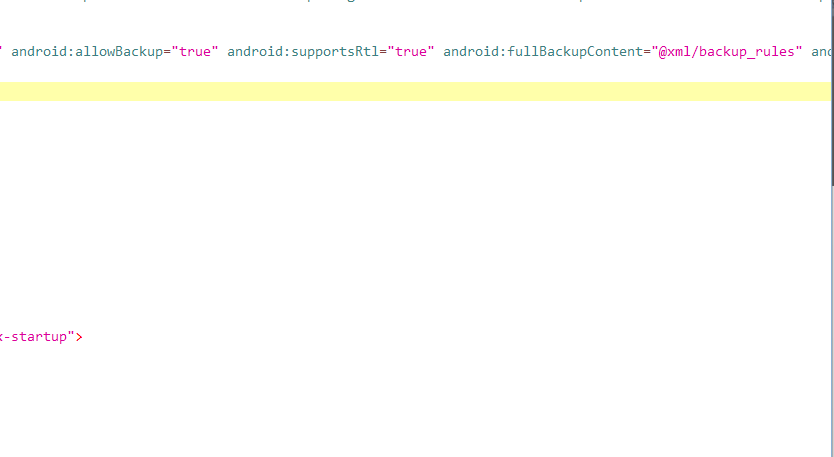
* Authentication and Session Management Requirements (MSTG-AUTH-\*)
* Network Communication Requirements (MSTG-NETWORK-\*)
* Data Storage and Privacy Requirements (MSTG-STORAGE-4\*) Executive Summary :

Disini Pada AndroidManifest.xml Di temukan bahwa allowBackup= true yang dimana membuat aplikasi dapat di backup. Hal ini dapat mengakibatkan data sensitif aplikasi

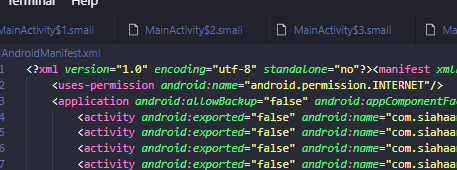
ikut terbawa seperti password dan dokumen penting dalam proses backup data, yang dapat menimbulkan risiko keamanan.

POC:

## AndroidManifest.xml



Recommendation:



mengatur "allowBackup" sebagai "false". Dengan mengatur "allowBackup" sebagai

"false", data aplikasi tidak akan disertakan dalam backup data perangkat, sehingga dapat mengurangi risiko kebocoran data sensitif.

Data Storage and Privacy Requirements (MSTG-STORAGE-7\*) Executive Summary :

Pada Activity New session dan menginput Master Password tidak encrypt yang mana text dari Master Password dapat di lihat secara langsung mana itu dapat membuat password tersebar ketika user lengah dan attacker melakukan shoulder surfing yang membuat attacker mengetaui master password.

POC:

## A screenshot of a computer Description automatically generatedActivityNewSession

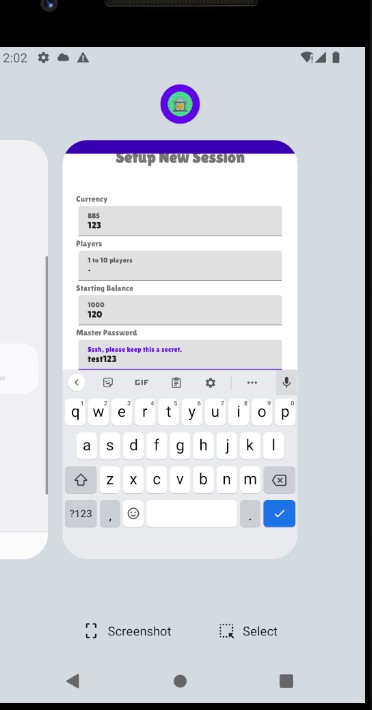
Recommendation:

Membuat Text Menjadi tanda “\*” supaya text tidak dapat di baca secara langsung dan kerahasiaan password tetap terjaga

Data Storage and Privacy Requirements (MSTG-STORAGE-9\*) Executive Summary :

Master Password pada aplikasi tidak encrypt yang mana ketika aplikasi terlihat di background,text dapat di lihat secara langsung mana itu dapat membuat password tersebar

POC:



Recommendation:

Membuat Text Menjadi tanda “\*” supaya text tidak dapat di baca secara langsung dan kerahasiaan Master password tetap terjaga

Data Storage and Privacy Requirements (MSTG-STORAGE-2\*) Executive Summary :

Pada SharePreference terdapat ID pengguna terenkripsi, ID pengguna, dan token JWT (JSON Web Token). Yang mana ini menyimpan dan mengambil informasi terkait

pengguna dalam sistem SharePreference. Ini menjadi vulnerability karena jika data sensitif, seperti token otentikasi atau informasi pengguna, disimpan dalam

SharePreference tanpa enkripsi atau tindakan keamanan tambahan, aplikasi lain yang tidak berwenang dapat mengakses dan mengambil data tersebut.

POC:

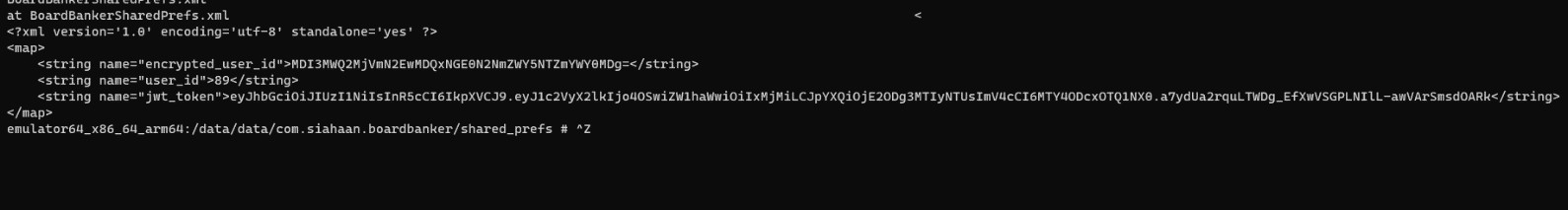
adb shell su

cd ./data/data

cd com.siahaan.boardbanker cd sharedpreference

cd shared\_prefs ls

cat BoardBankerSharedPrefs.xml



Recommendation:

Pada SharePreference harus ada autentifikasi dan enkripsi tambahan yang kuat seperti penggunakan fingerprint, hashing atau salting untuk melindungi data yang disimpan dalam SharePreference.

# \*API Vunrebility:

Network Communication Requirements (MSTG-NETWORK-1\*) Executive Summary :

Ketika di lakukan intercept pada aplikasi terlihat bahwa email dan password tidak di lakukan enkripsi yang mana ini memberikan peluang bagi attacker untuk melakukan

bruteforce atau sql injection pada password maupun email.Serta pada activity register terlihat bahwa text tidak di lakukan enkripsi.

POC:

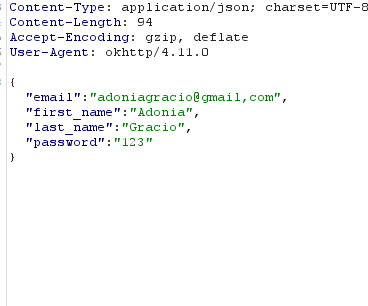
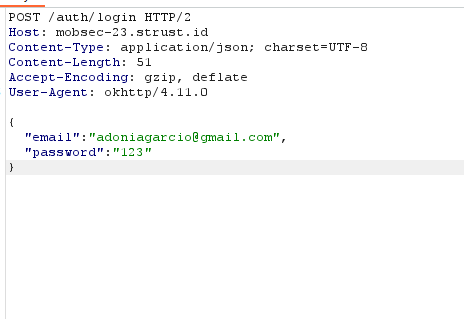
-Buka Tools Burp kemudian atur proxy dan sesuai kan proxy yang ada di android dengan yang di burp

-Nyalakan frida-server pada android

-masukan script SSL UNPINNING

-jalankan SSL UNPINING guna melakukan intercept pada aplikasi karena aplikasi terdapat SSL Pinning

-nyalakan intercept



Recommendation:

Melakukan enkripsi pada inputan tersebut sebelum disimpan atau dikirimkan melalui jaringan guna mencegah terjadinya brute forcing atau serangan seperti sql injection

Network Communication Requirements (MSTG-NETWORK-1\*) Executive Summary:

Ketika di lakukan intercept pada aplikasi terlihat bahwa OTP tidak di lakukan enkripsi yang mana ini memberikan peluang bagi attacker untuk melakukan bruteforce dan mendapatkan code OTP.

POC:

-Buka Tools Burp kemudian atur proxy dan sesuai kan proxy yang ada di android dengan yang di burp

-Nyalakan frida-server pada android

-masukan script SSL UNPINNING

-jalankan SSL UNPINING guna melakukan intercept pada aplikasi karena aplikasi terdapat SSL Pinning

-nyalakan intecept



Recommendation:

Melakukan enkripsi pada code otp tersebut sebelum dikirimkan melalui jaringan guna mencegah terjadinya brute forcing pada otp dan attacker dapat memiliki akses yang tidak sah ke account kita

Authentication and Session Management Requirements (MSTG-AUTH-8\*) Executive Summary :

Ketika di lakukan intercept pada aplikasi terlihat bahwa sesi OTP dapat di lewati karena edit pada intercept yang merubah NeedOTP menjadi false yang mana ini memberikan peluang bagi attacker untuk melakukan jumping activity dan bisa langsung login tanpa harus melawati proses verifikasi code OTP.

POC:

-Buka Tools Burp kemudian atur proxy dan sesuai kan proxy yang ada di android dengan yang di burp

-Nyalakan frida-server pada android

-masukan script SSL UNPINNING

-jalankan SSL UNPINING guna melakukan intercept pada aplikasi karena aplikasi terdapat SSL Pinning

-nyalakan intecept

-Ubah needOtp yang sebelumnya true menjadi false



Recommendation:

Di ubah pada needOtp menjadi sebuah keystore bukan true atau false dan Pastikan validasi OTP dilakukan di sisi server, bukan hanya di sisi Aplikasi. Dengan melakukan validasi di sisi server, perubahan pada intercept tidak akan mempengaruhi proses verifikasi OTP yang sebenarnya.

# \*BONUSPOINT

**CTF: j4ngan\_jadi\_peNjahats\_y4\_f33llas**

Melakukan fungsi decrypt menggunakan frida tools yang mana saya melakukan hook function base64 dan pemanggilan method decoder guna mengubah string flag menjadi byte yang nanti akan di lakukan decrypt dengan melakukan hook pada method yang

terdapat pada activities com.siahaan.boardbanker.utilities.EncUtils. kemudian flag di tampilkan menggunakan console.log

Berikut hasil dan Scriptnya:

# A screenshot of a computer program Description automatically generatedHasil:

**ScriptFrida:**

