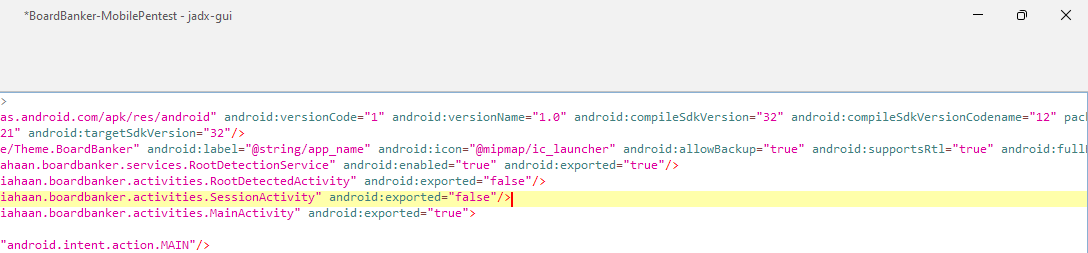
**Boardbanker**

**Report**

* 1. Issue: Allow Backup = true (MSTG-STORAGE-8)
  2. Executive Summary: pengaturan "allowBackup" yang diatur sebagai "true" dalam aplikasi Android membuat aplikasi dapat di backup. Hal ini dapat mengakibatkan data sensitif aplikasi ikut terbawa dalam backup data, yang dapat menimbulkan risiko keamanan.
  3. POC:

AndroidManifest.xml

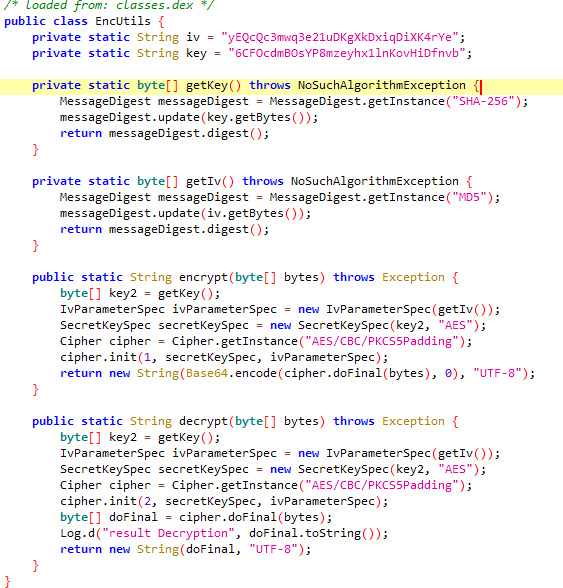


* 1. Recommendation: mengatur "allowBackup" sebagai "false" dalam aplikasi Android.

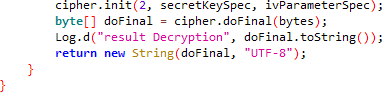
Dengan mengatur "allowBackup" sebagai "false", data aplikasi tidak akan disertakan dalam backup data perangkat, sehingga dapat mengurangi risiko kebocoran data sensitif.

1. Issue: HardCode Cryptographic key(MSTG-CRYPTO-1)
2. Executive Summary: Penggunaan hardcode pada key dapat mengakibatkan kerentanan keamanan integritas, kerahasiaan, dan autentikasi data yang dienkripsi
3. POC:

com/siahaan.boardbanker/utilities/EncUtils



1. Recommendation: Sebaiknya gunakan konfigurasi eksternal atau environment variable untuk menyimpan kunci kriptografi.
2. Issue: Decrpty result log (MSTG-STORAGE-3)
3. Executive Summary: hasil decryption log yang disimpan dalam penyimpanan yang dapat mengakibatkan data yang tidak dienkripsi atau yang sudah didekprisi tercatat pada log.
4. POC:

com/siahaan.boardbanker/utilities/EncUtils

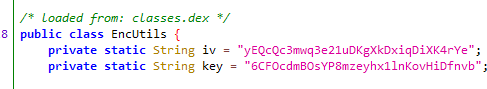
1. Recommendation:

hasil log atau catatan aplikasi yang disimpan dalam penyimpanan (storage) tetap dalam

bentuk yang dienkripsi dan hanya didekripsi atau didekompresi saat diperlukan atau dalam lingkup yang aman.

1. Issue: Using cryptographic key for multiple purpose (MSTG-CRYPTO-5 )
2. Executive Summary: kunci kriptografi yang sama untuk berbagai tujuan berisiko tinggi dan dapat mengompromikan keamanan aplikasi atau sistem. Ketika satu kunci digunakan untuk berbagai tujuan, seperti enkripsi dan autentikasi, hal ini meningkatkan permukaan serangan dan potensi kerentanan. Jika salah satu tujuan tersebut tercompromi, bisa mengakibatkan akses tanpa izin ke bagian lain dari sistem atau aplikasi yang menggunakan kunci yang sama.
3. POC:

com/siahaan.boardbanker/utilities/EncUtils



1. Recommendation: Kunci kriptografi harus disimpan dan dikelola secara aman bisa dengan menggunakan Hardware Security Module (HSM) atau Key Management Service (KMS) untuk melindungi key dari ancaman fisik atau logika.

**FLAG**

Dengan melakukan beberapa decompile membuat supaya fungsi decypt melakukan decypt pada string yang di encrypt dan menghasilkan string “j4ngan\_jadi\_peNjahats\_y4\_f33llas”