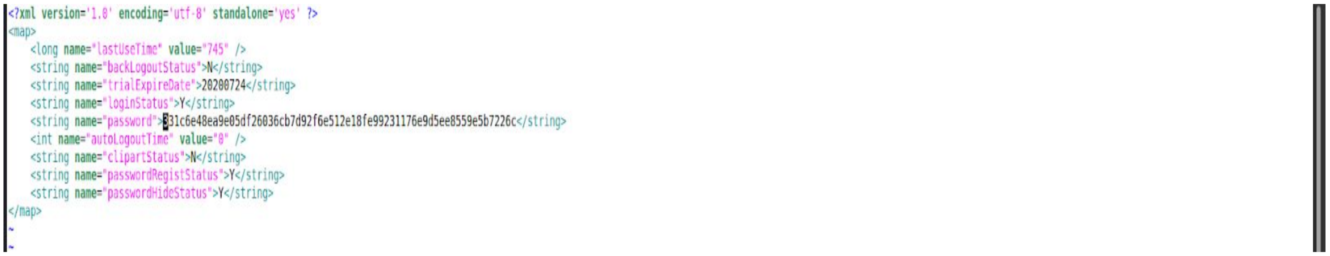
Insecure hashing/storing HidePass

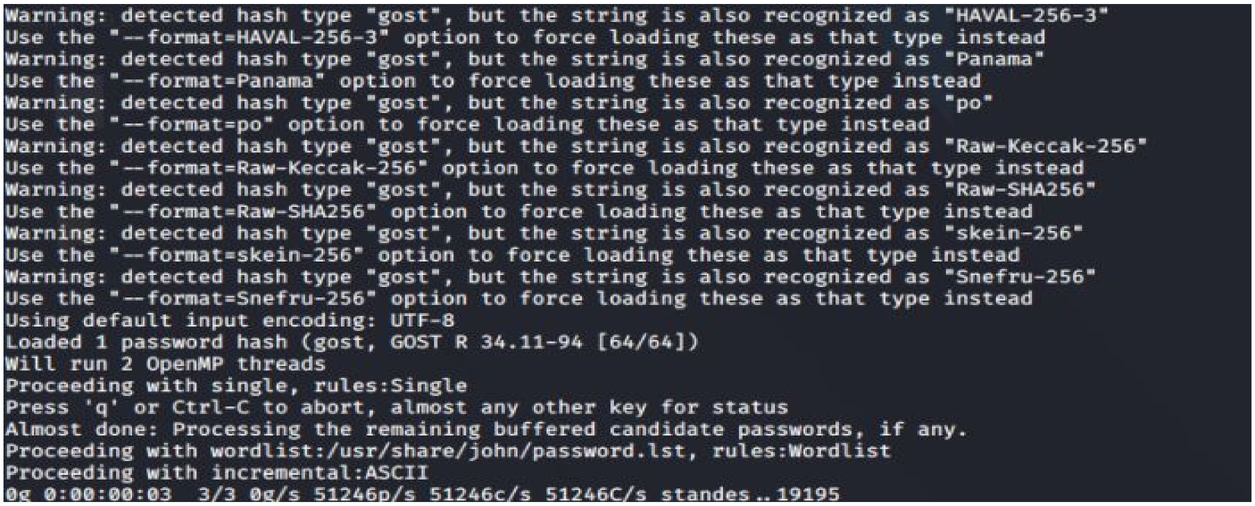
https://play.google.com/store/apps/details?id=com.sisomobile.android.passwordsafe

Basic password vault for android from what i could see. 1. Made a account with name and password(main) PW 2. Saved a ransom password inside a vault, then i started testing looking through filesystems and noticed .dbs but the info in them was not valuable then i came across preferences. XML



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <long name="lastUseTime" value="745" />
    <string name="backLogoutStatus">N</string>
    <string name="trialExpireDate">20200724</string>
    <string name="loginStatus">Y</string>
    <string name="password">331c6e48ea9e05df26036cb7d92f6e512e18fe99231176e9d5ee8559e5b7226c</string>
    <int name="autoLogoutTime" value="0" />
    <string name="clipartStatus">N</string>
    <string name="passwordRegistStatus">Y</string>
    <string name="passwordHideStatus">Y</string>
</map>
~
~
```

Above in the /data/data/com.sisomobile.android.passwordsafe/shared_prefs/com.sisomobile.android.passwordsafe_preferences.xml directory the main password for password manager is stored in ghost-256 bit vulnerable to collision attacks and pure hash cracking as seen below it's also labeled as a insure hashing algo.



```
Warning: detected hash type "gost", but the string is also recognized as "HAVAL-256-3"
Use the "--format=HAVAL-256-3" option to force loading these as that type instead
Warning: detected hash type "gost", but the string is also recognized as "Panama"
Use the "--format=Panama" option to force loading these as that type instead
Warning: detected hash type "gost", but the string is also recognized as "po"
Use the "--format=po" option to force loading these as that type instead
Warning: detected hash type "gost", but the string is also recognized as "Raw-Keccak-256"
Use the "--format=Raw-Keccak-256" option to force loading these as that type instead
Warning: detected hash type "gost", but the string is also recognized as "Raw-SHA256"
Use the "--format=Raw-SHA256" option to force loading these as that type instead
Warning: detected hash type "gost", but the string is also recognized as "skein-256"
Use the "--format=skein-256" option to force loading these as that type instead
Warning: detected hash type "gost", but the string is also recognized as "Snefru-256"
Use the "--format=Snefru-256" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (gost, GOST R 34.11-94 [64/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
Proceeding with incremental:ASCII
0g 0:00:00:03  3/3 0g/s 51246p/s 51246c/s 51246C/s standes..19195
```

Keep in mind even though it's password cracking. With how easy it is to gather info on people today, all the breaches etc and also how you can hire an Amazon/Google cloud machine with 200 CPUs and crack the hash. Add collision attack’s and it's safe to say it's not safe at all.

This is my first write up so please forgive me if i did something wrong.

My References:

https://en.wikipedia.org/wiki/Collision_attack
https://www.iacr.org/archive/crypto2008/51570163/51570163.pdf
https://www.solarwindsmsp.com/blog/sha-256-encryption#:~:text=How%20secure%20is%20SHA-256,sensitive%20information%20using%20SHA-256.
https://play.google.com/store/apps/details?id=com.sisomobile.android.passwordsafe

By: xR1NGxZ3R0x