Vulnerability in Tiny Password Free for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk
Mar 9, 2012 at 6:53 PM HKT

Abstract

We found that Tiny Password Free 1.64 has a vulnerability that allows a crafted application to read and modify user's sensitive information without permission, including all encrypted account information, e.g. username, password, notes, and website url in plaintext (similar to user's bookmark). Although Tiny Password has encrypted account information in AES, an experienced hacker is still able to decrypt them, because amount of user's pattern is limited. Once decrypted, user's all web account will be hacked.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1409-vulnerability-in-TinyPassword.html

2 Description

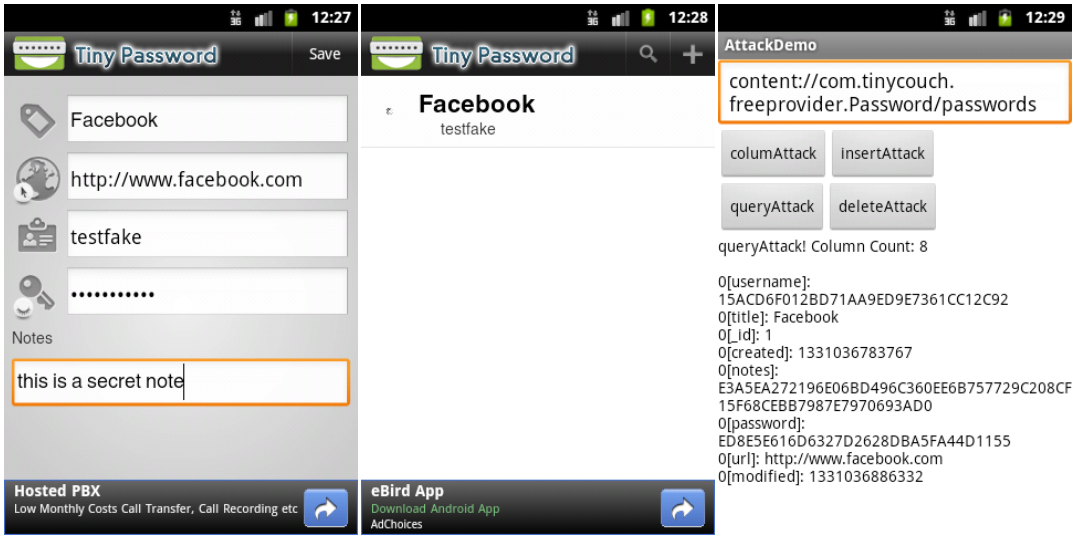
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

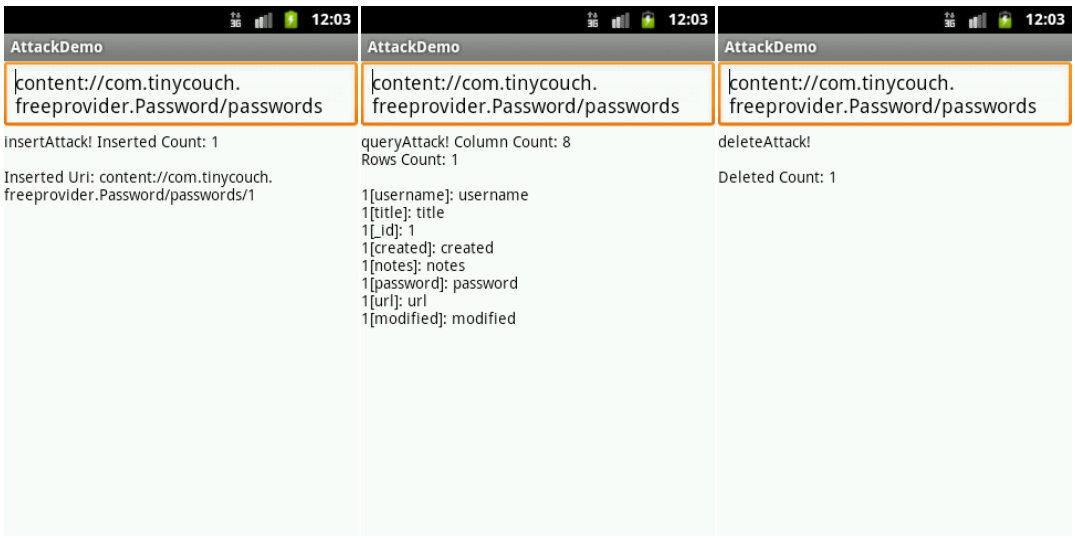
```
<provider android:name=".PasswordProvider"
android:authorities="com.tinycouch.freeprovider.Password" />
```

3 Impact

Please see the following snapshots generated by our arrack demo:

*** authors with equal contributions**





4 Solution

Our advice is to set the permission of these application's content providers properly, or avoid exporting these content providers in the AndroidManifest.xml file. Currently, a user could disable the application temporarily and wait for an official update.

5 Technical Description

Please see the following exposed content providers and tables:

Content Provider Authority	Table Name
com.tinycouch.freeprovider.Password	passwords