Rapport TP2

# Introduction

Il est demandé de prendre une application opensource sur le marché de faussé une interface de login afin de volé les identifiants d’un utilisateur puis de les envoyé sur un C2 développé par nos soin, ou de stocker les identifiants en local sur l’appareil.

# Réalisation

J’ai choisi d’implémenté ma propre applications android avec une fausse page de login mdp et de mot de passe qui redirige sur la même page et qui se ferme après cela simule assez bien le comportement d’un phishing que l’on pourrait reproduire en vrai mais vu que le but de cette exercice n’es pas de crée une réelle arme qui pourrait servir à hameçonner dans le futur, c’est pour des raison éthique que je souhaite fournir qu’un simple POC. Ma méthode a été la suivante générer une activity de login avec android studio, la dupliqué, effectué les changements nécessaires dans le manifest (ajouter l’’activity, supprimer le fait que ce soit une activity launcher) et redirigé la première activité vers la deuxième puis ajouter les strings nécessaires au débogage et au test de mon application tel que :



Figure 1 chaine de caractère utilisé

« file\_writed » utilisé pour le debogage de l’application et « error\_503 » pour trompé l’utilisateur, en effet j’ai choisi cette erreur qui est totalement plausible dans un cadre réel en effet l’erreur http 503 signifie une erreur du coté serveur plus particulièrement une indisponibilité du service (dû au fait d’une maintenance, ou d’une surcharge du serveur), et les application communique constamment via le protocole HTTP vers les serveurs à l’aide API.

Voici la portion de code malveillante.

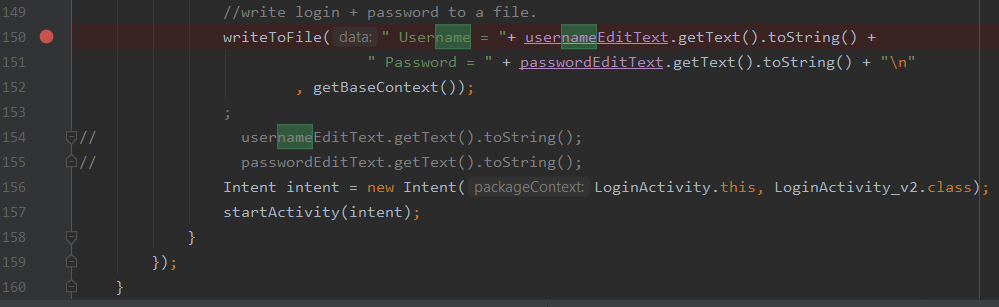


Figure 2 charge malveillante / charge utile

Ici se trouve le code qui écrit ce que l’utilisateur rentre dans le champ de login et de mot de passe dans un fichier sur le téléphone. Et le redirige sur une nouvelle page (activité) identique dans le but de tromper l’utilisateur.

Voici à quoi ressemble l’application :

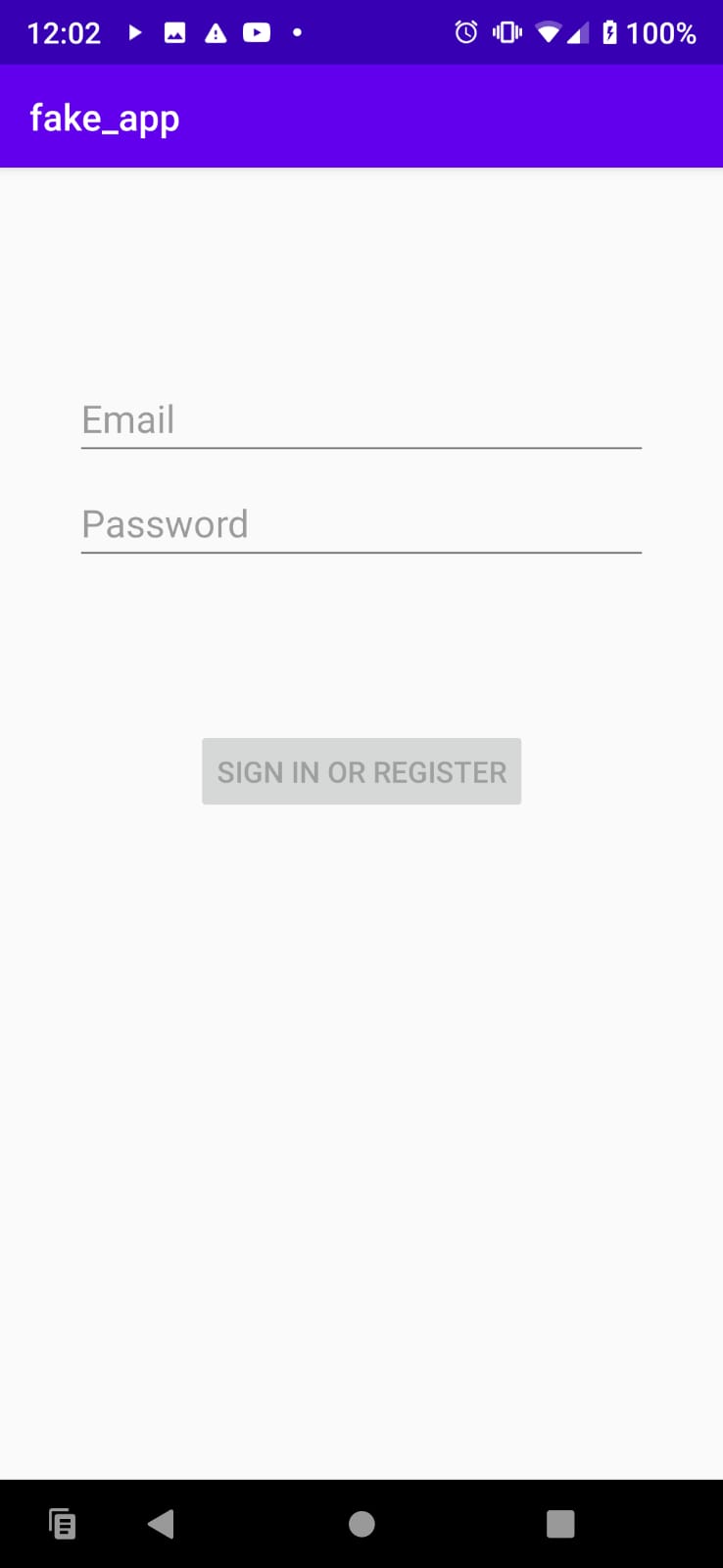


Figure 3 interface de l’application

Une fois l’application utilisé et les identifiant rentré sont enregistré sur le téléphone :

Voici là où ils sont enregistrés sur mon téléphone : Les identifiants sont au chemin : « /data/media/storage/emulated/android/data/com.example.fakeapp/files/db\_passwd.txt »

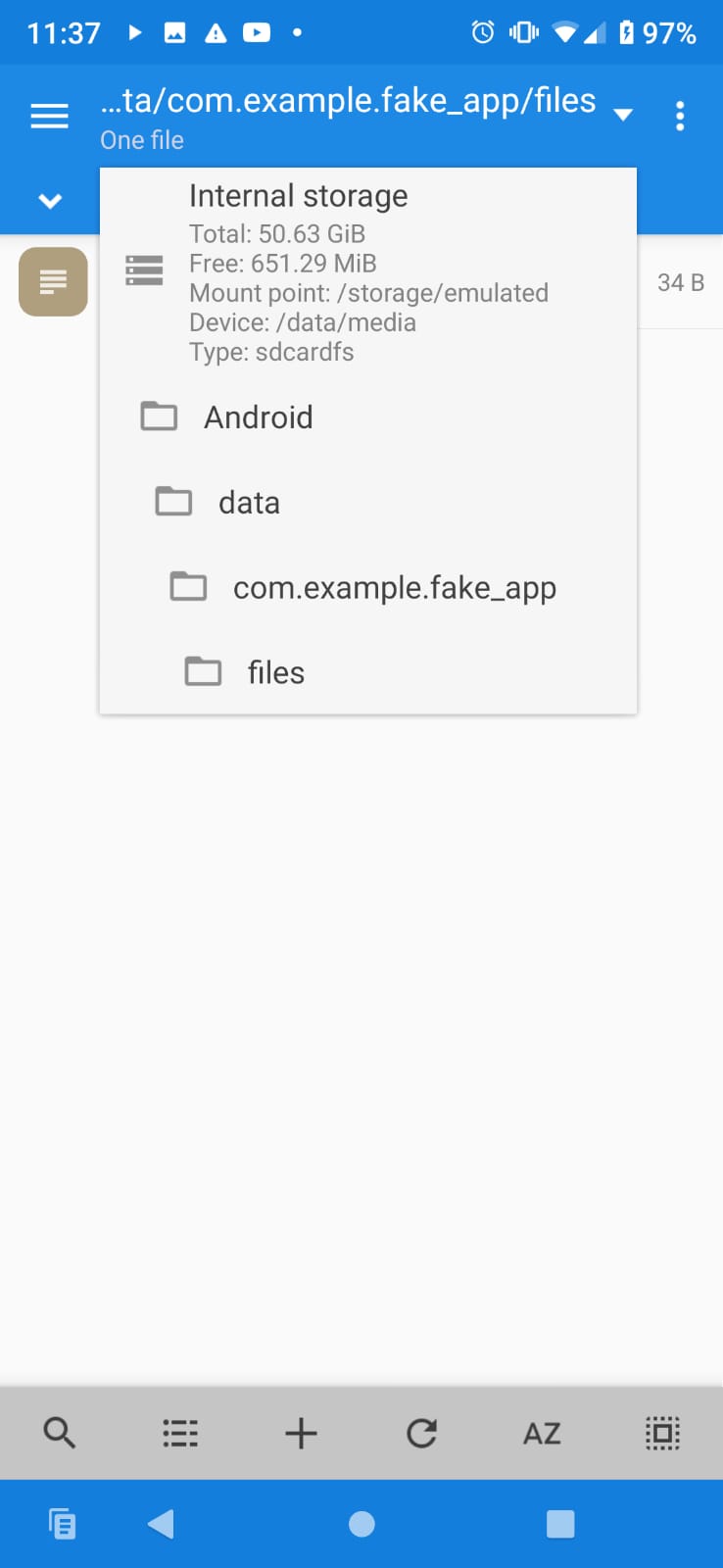


Figure 4 Path du fichier contenant les identifiants



Une fois le fichier ouvert on peut voir qu’il s’agit d’un simple fichier texte avec les identifiant et mot de passe de la personne attaquée.

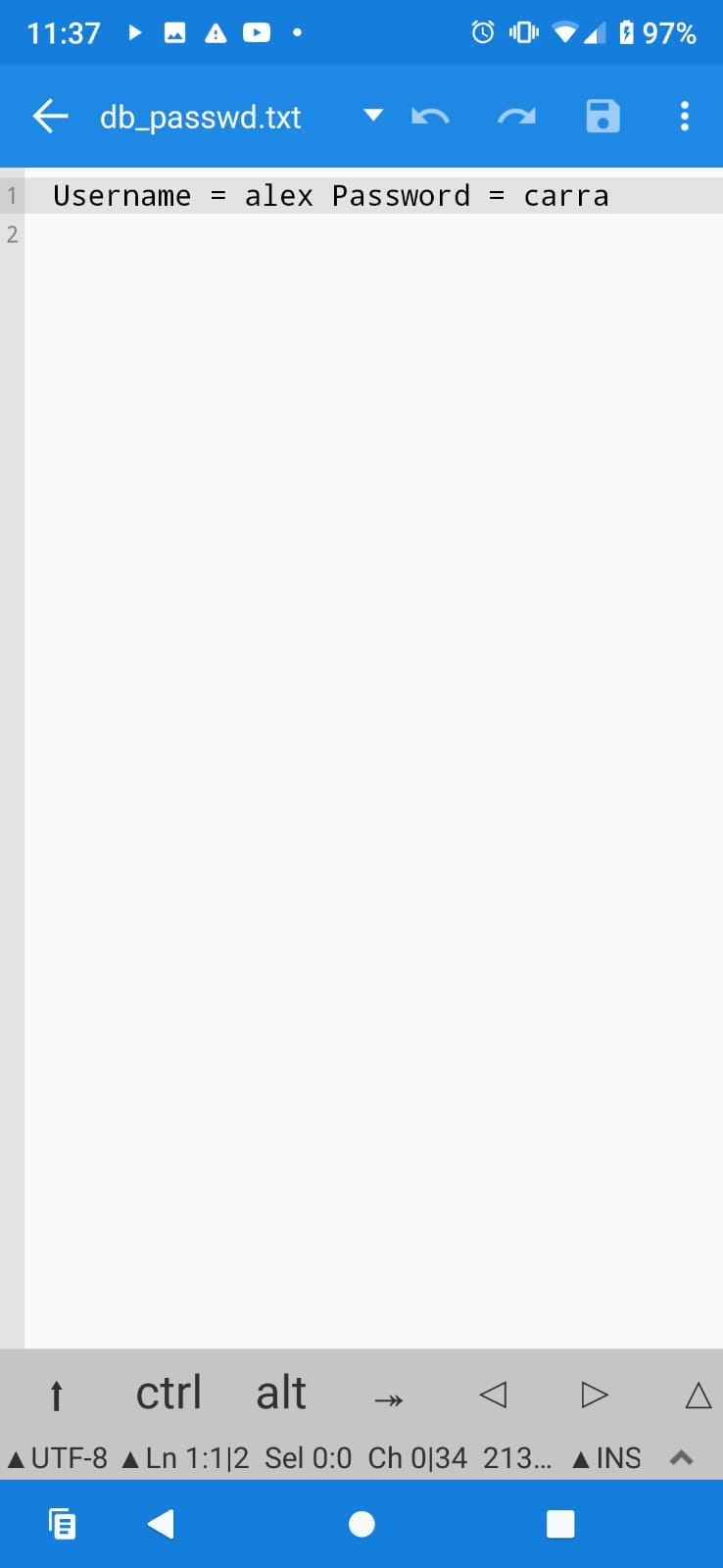


Figure fichier contenant les idnetifiant