ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

Факультет безопасности информационных технологий

Дисциплина:

«Обеспечение информационной безопасности мобильных устройств»

ОТЧЕТ ПО ЛАБАРАТОРНОЙ РАБОТЕ №3

«Основы анализа защищенности мобильных приложений»

Выполнил:

Гаврилова В. В., студент группы N33471

Проверил:

Федоров Иван Романович

24.02.2022

(отметка о выполнении)

(подпись)

Санкт-Петербург

2022г.

Содержание

1. Цель работы

Ознакомиться с Owasp Mobile Top 10, на практике изучить возможные уязвимости мобильных приложений при помощи приложения Diva и моделирования в Genymotion.

2. Основная часть

2.1 Описание выбранных средств реализации и обоснования выбора

Для эмулирования был использован Genymotion, эмулировался Android 4.4 на Google Nexus 5. Для изучения уязвимостей был установлен diva-beta.apk.

2.2 Сборка стенда для пентестинга

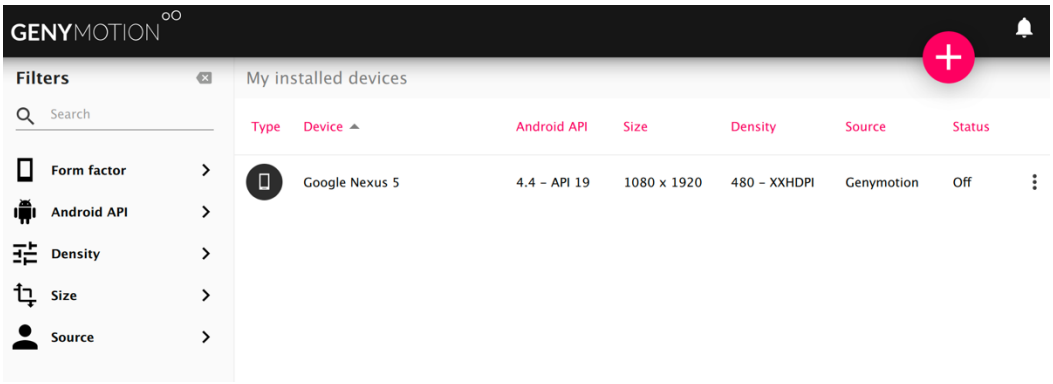

Рисунок 1 – Стенд в Genymotion

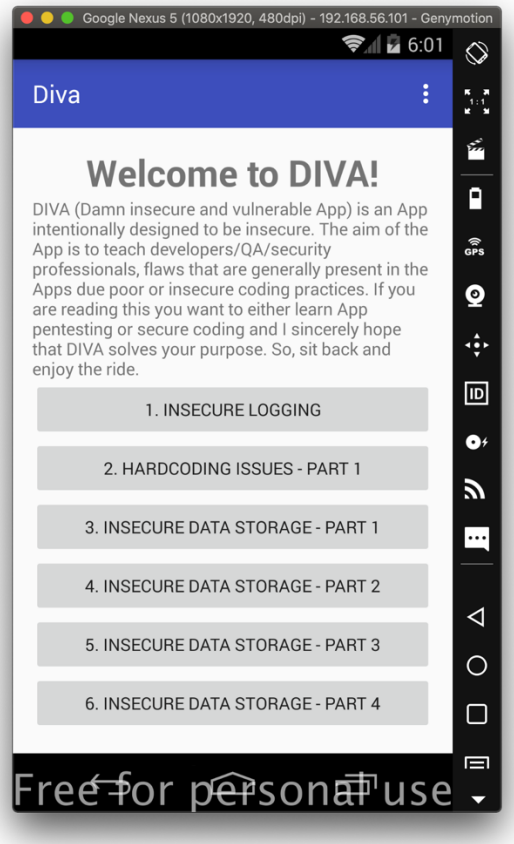

Рисунок 2 – Diva на Nexus 5

```
MBP-Veronika:~ veronikagavrilova$ adb devices
List of devices attached
192.168.56.101:5555     device

MBP-Veronika:~ veronikagavrilova$ adb connect 192.168.56.101
already connected to 192.168.56.101:5555
MBP-Veronika:~ veronikagavrilova$ adb logcat
```

Рисунок 3 – Подключенное устройство

2.3 Insecure logging

Цель эксплуатации уязвимости – выяснить пароль, введенный пользователем. Часто приложения для Android записывают конфиденциальную информацию в logcat.

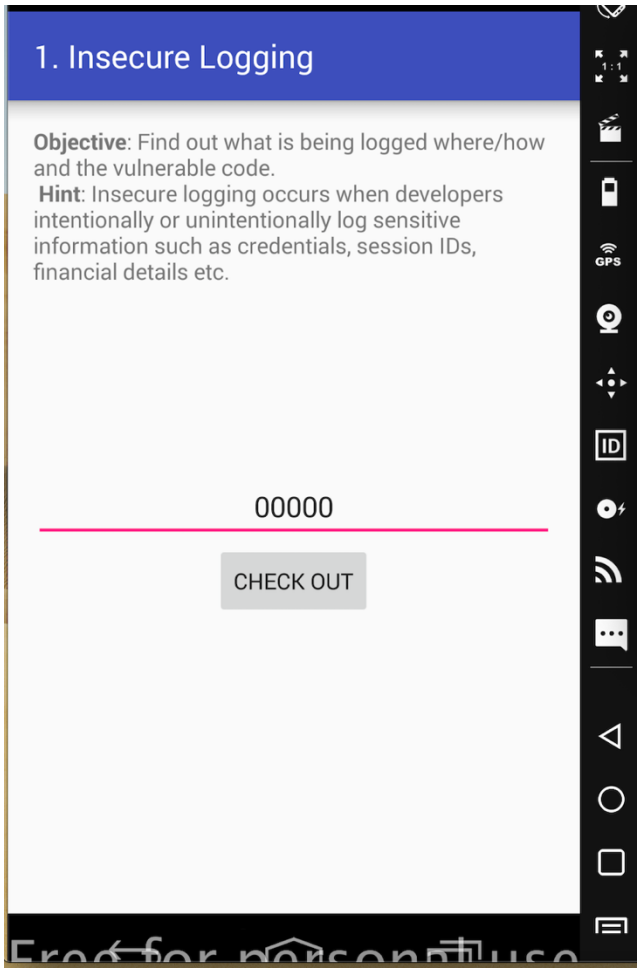

Рисунок 4 – Ввод пароля

```
MBP-Veronika:~ veronikagavrilova$ adb shell
root@vbox86p:/ # ps | grep diva
u0_a59    4853  1036  573712 47412 ffffffff b765407b S jakhar.aseem.diva
root@vbox86p:/ # logcat | grep 4853
```

Рисунок 5 – Просмотр логов, относящихся к процессам Diva

```
E/EGL_emulation( 4853): tid 4853: eglSurfaceAttrib(1210): error 0x3009 (EGL_BAD_MATCH)
W/HardwareRenderer( 4853): Backbuffer cannot be preserved
E/diva-log( 4853): Error while processing transaction with credit card: 0000000000
D/dalvikvm( 4853): Debugger has detached; object registry had 1 entries
```

Рисунок 5 – Пароль

2.4 Hardcoding issues – part 1

Цель – узнать пароль производителя, чтобы получить доступ. Разработчик может оставить пароль в нешифрованном виде в коде приложения.

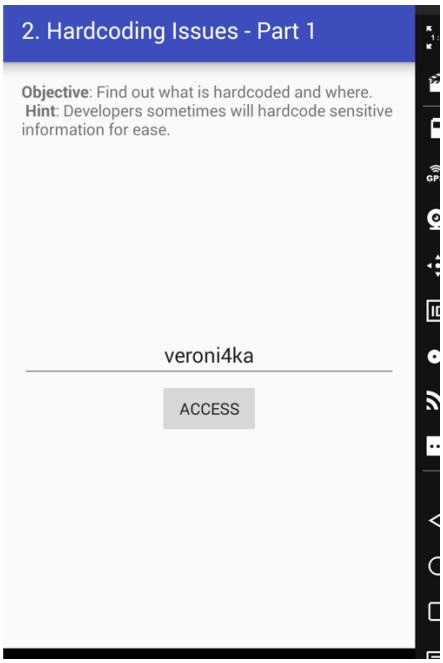

Рисунок 6 – Ввод пароля

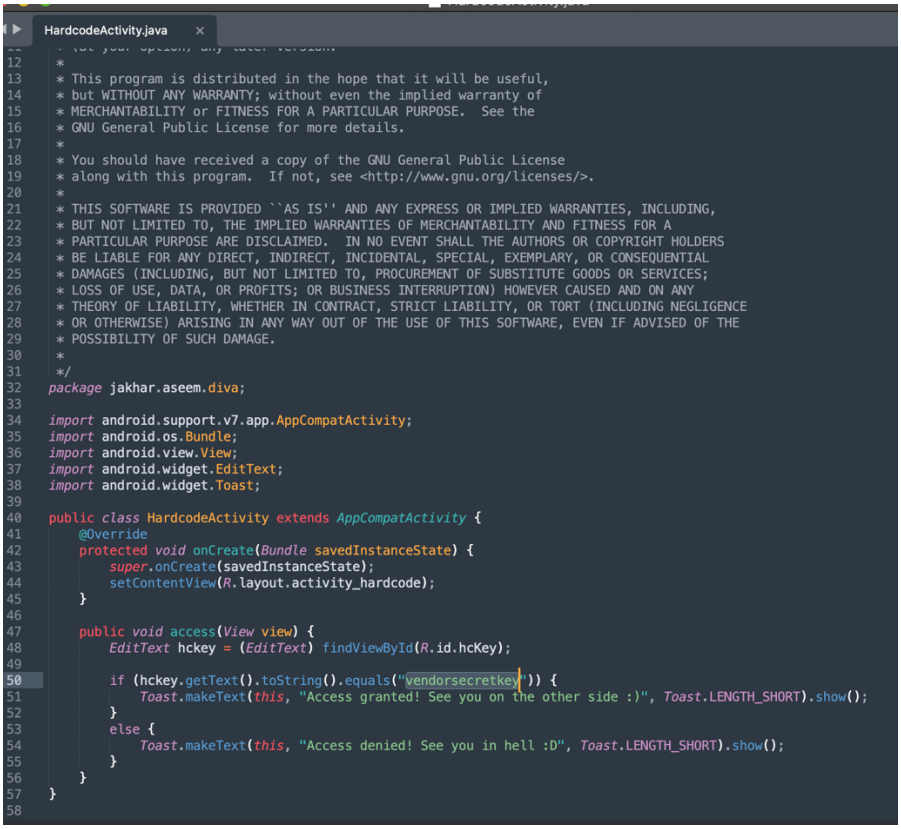

Рисунок 7 – Содержимое HardcodeActivity.java и пароль в явном виде

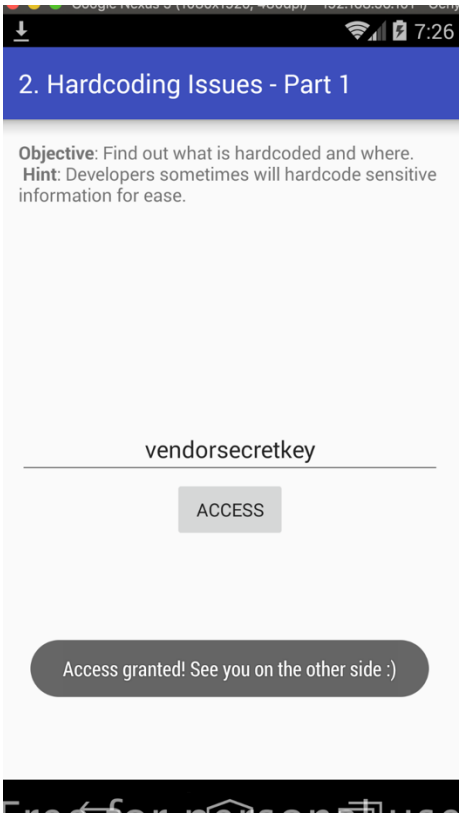

Рисунок 8 – Ввод найденного пароля

2.5 Input Validation Issues - Part I

После прочтения описания можно понять, что существует 3 пользователя. При помощи SQL инъекций можно выяснить логины и пароли пользователей.

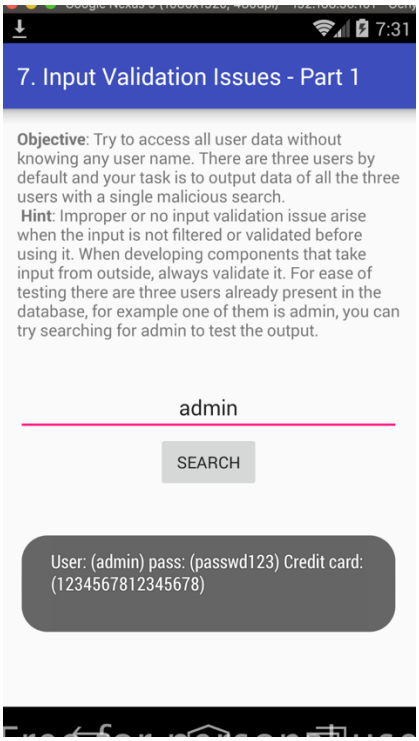

Рисунок 9 – Результат при вводе пользователя admin

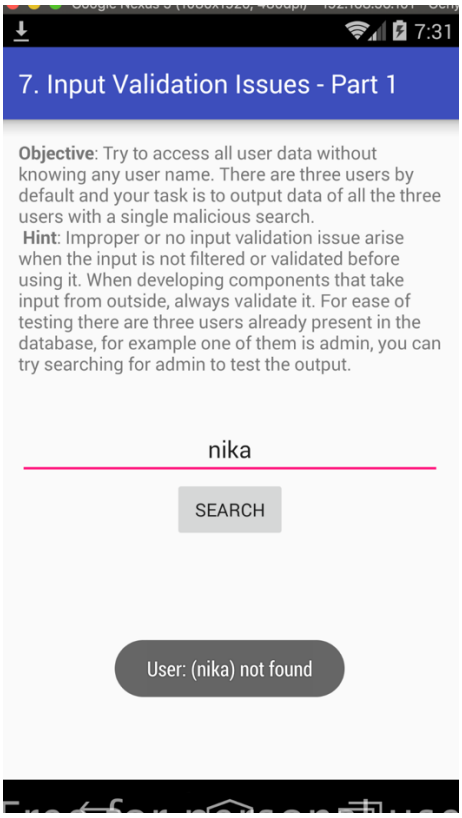

Рисунок 10 – Результат при вводе пользователя nika

Можно попробовать ввести в поле специальные символы, такие как $ “ ‘ #

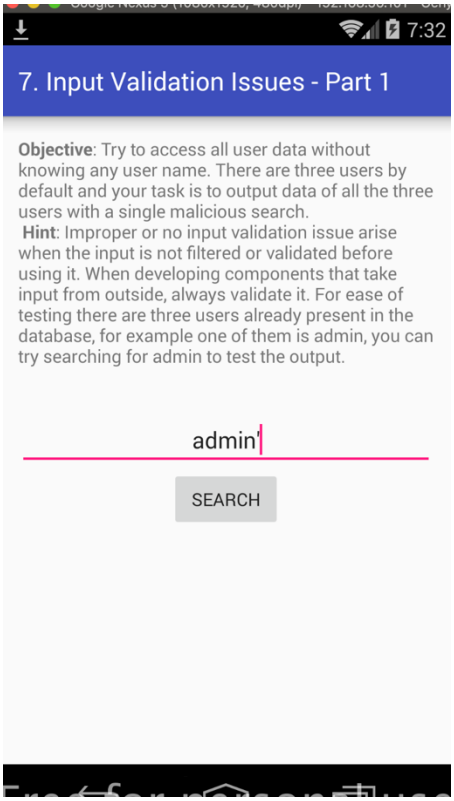

Рисунок 11 – Результат ввода специального символа – невидимая ошибка

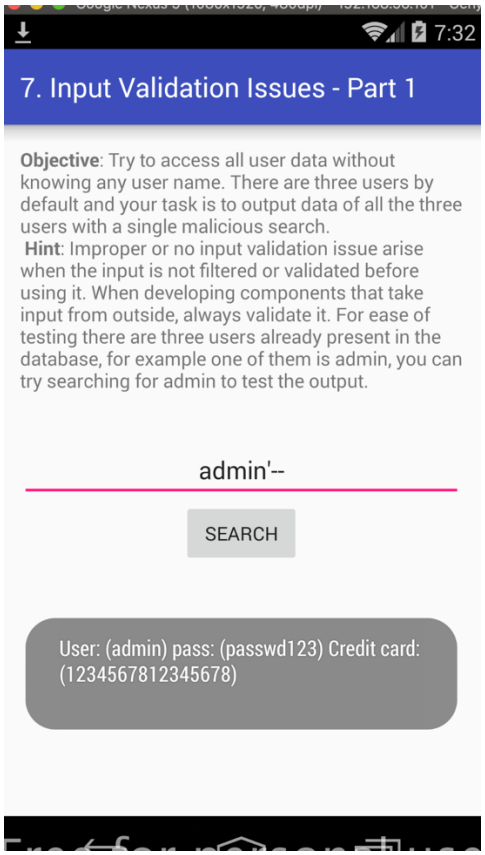

Рисунок 12 – Успешная попытка запроса с синтаксисом SQL

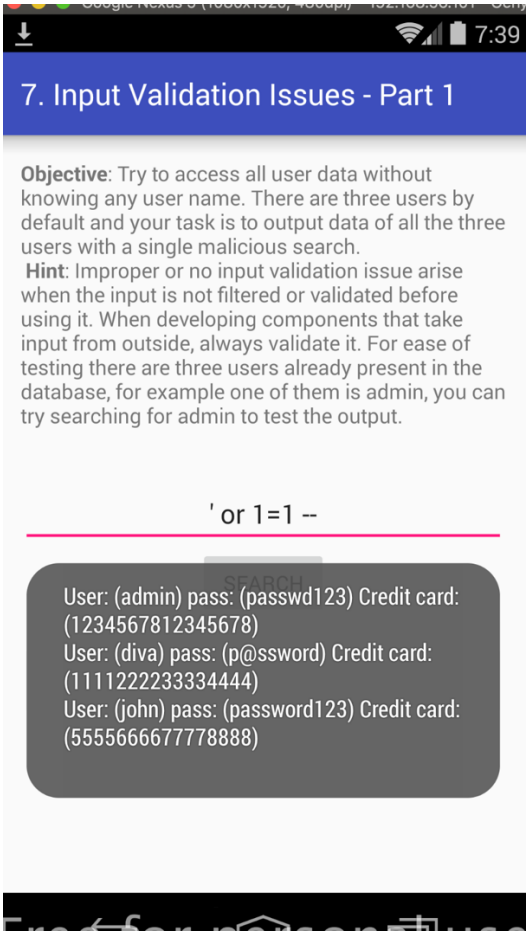

Рисунок 13 – Успешный запрос SELECT * FROM Table WHERE user='' or 1=1—‘

3. Вывод

В результате выполнения работы я научилась настраивать и производить эмуляцию в Genymotion, изучила основные уязвимости в мобильных приложениях и проэксплуатировала их на практике в Diva.