Mobile Application Pentesting-Part 3

Piyush Patil
May 18 · 4 min read ★

Insecure Data Storage

> *PART-2*

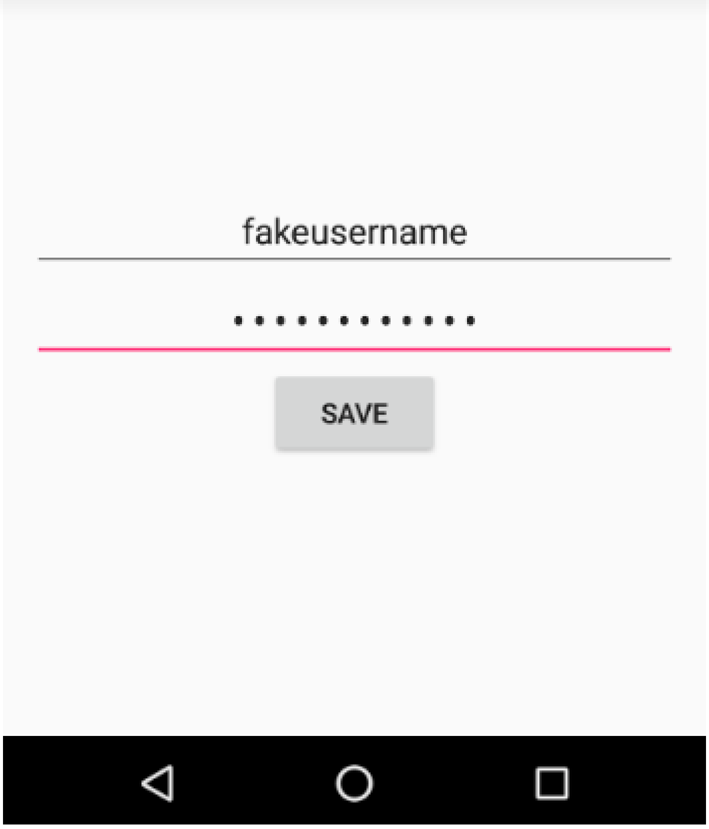
Get one more story in your member preview when you sign up. It's free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

confidential information insecurely on the system i.e.


fakeusername
•••••••••••••
SAVE

username=fakeusername

password=fakepassword

Let’s check the code of **InsecureDataStorage2Activity.java** to know what is happening.

Get one more story in your member preview when you sign up. It’s free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

As you can see, username and password are stored in SQL database name “ids2”.

That means if we read the database file in the application folder, we can find credentials there. let’s get the database file:

```
# database directory: /data/data/<app-package-path>/databases
```

```
adb pull “/data/data/jakhar.aseem.diva/databases/ids2”
```

“ids2” file exists, I don’t know the reason why it is showing the error.

Solution to solve this error:-

```
adb shell su

cd /data/data/jakhar.aseem.diva/databases

cp ids2 /data/local/tmp
```

Get one more story in your member preview when you sign up. It’s free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

. . .

Insecure Data Storage

> PART- 3

×

Get one more story in your member preview when you sign up. It’s free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

cat InsecureDataStorage3Activity.java

A temporary file **uinfo** is created, where the credentials coming from the user input are saved:

cat info-419988827tmp

. . .

Insecure Data Storage

PART 4

Get one more story in your member preview when you sign up. It's free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

cat InsecureDataStorage4Activity.java

Get one more story in your member preview when you sign up. It’s free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

If the application uses the **WRITE_EXTERNAL_STORAGE** permission, then it has also permission to read the external storage from SD card.

adb shell “cat /storage/emulated/0/.uinfo.txt”

Input Validation Issues

Input Validations Attacks are when an attacker purposefully sends strange inputs to confuse an application. Input validation routines serve as the first line of defense for such attacks. Examples of input validation attacks include buffer overflow, directory traversal, cross-site scripting, and SQL injection.

> ***Part 1- SQL INJECTION***

Get one more story in your member preview when you sign up. It’s free.

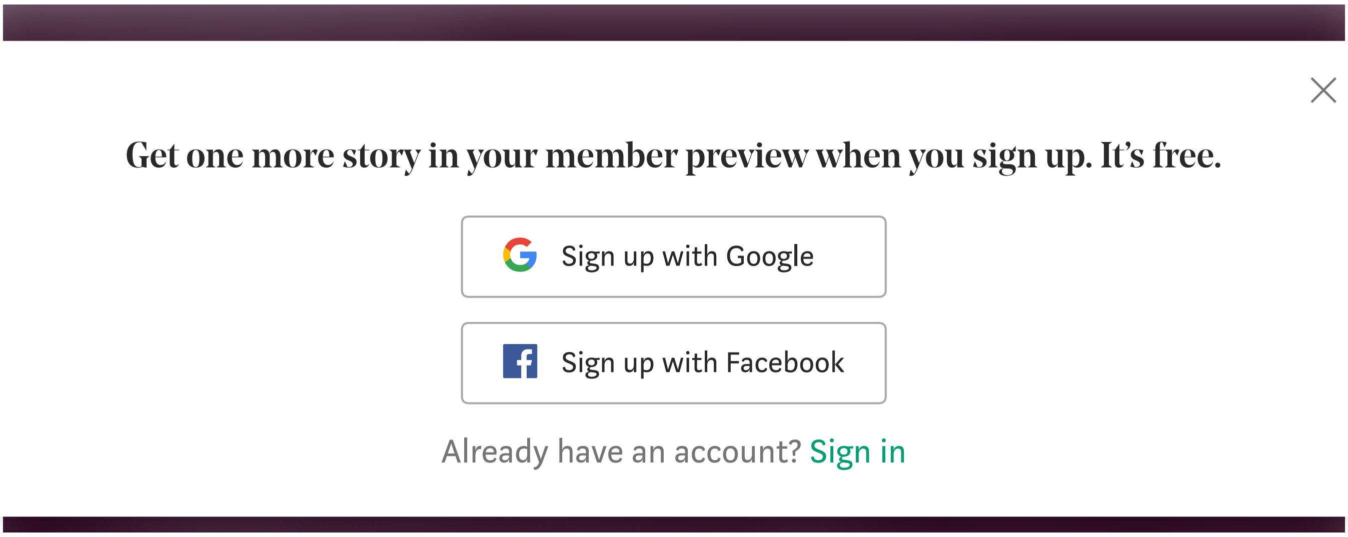
Sign up with Google

Sign up with Facebook

Already have an account? Sign in

Let’s look at the code.

cat SQLInjectionActivity.java



Get one more story in your member preview when you sign up. It’s free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

*SELECT * FROM sqliuser WHERE user=’admin’;*

*SELECT * FROM sqliuser WHERE user=’admin’ or ‘a’=’a’- -;*

- -==>There is no space between the dash.

- -*means consider anything which comes after- -as a commen*t.

Get one more story in your member preview when you sign up. It’s free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

Webview is a simply browser content being rendered into a mobile application.

As you can see in above image ,google.com is unreachable because the INTERNET permission has not included in the AndroidManifest.xml.

Using the File protocol, access to the uinfo file can be achieved:

Get one more story in your member preview when you sign up. It’s free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

. . .

Input Validation Issues

> *Part 3- Buffer Overflow*

Typing random string “hello” to check what happen.

The application is using JNI (Java Native Interface), what suggests that the method **DivaJni** is related to a program written in other language.

Get one more story in your member preview when you sign up. It’s free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

-The problem is that the function strcpy does not check whether the size of the destination's buffer is large enough to hold the source parameter.

-A consequence of function strcpy bad usage is the corruption of memory or buffer overflow, and eventually the crash of the application.

Android Hacking Cybersecurity Security Penetration Testing

56 claps

WRITTEN BY

Piyush Patil

Reverse Engineering, Penetration Testing(Web, Mobile, IoT, Network, Infra)

Get one more story in your member preview when you sign up. It's free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

Do They All Want To Sleep With Me? — And Other Questions Of A Guys' Girl

Tesia Blake in P.S. I Love You
Nov 21 · 7 min read ★

3K

Top on Medium

Get one more story in your member preview when you sign up. It's free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in

Apparently I Was Nothing But A Woo-Girl

Michelle Ann in Fearless She Wrote
Nov 13 · 4 min read ★

4.98K

Top on Medium

How to Predict the End of a Relationship

Colleen Murphy in Mindful Muse
Nov 22 · 5 min read ★

2.4K

Get one more story in your member preview when you sign up. It's free.

Sign up with Google

Sign up with Facebook

Already have an account? Sign in