

# Documentación del Proceso: Análisis de Vulnerabilidades en la Aplicación DIVA

## Introducción

El presente documento detalla el proceso de análisis de vulnerabilidades llevado a cabo en la aplicación DIVA, que se centra en aspectos críticos de seguridad, como el almacenamiento inseguro de datos, la validación de entradas y los problemas de control de acceso. Cada actividad se abordó con el objetivo de identificar y explotar vulnerabilidades comunes en aplicaciones móviles, utilizando técnicas de análisis y explotación.

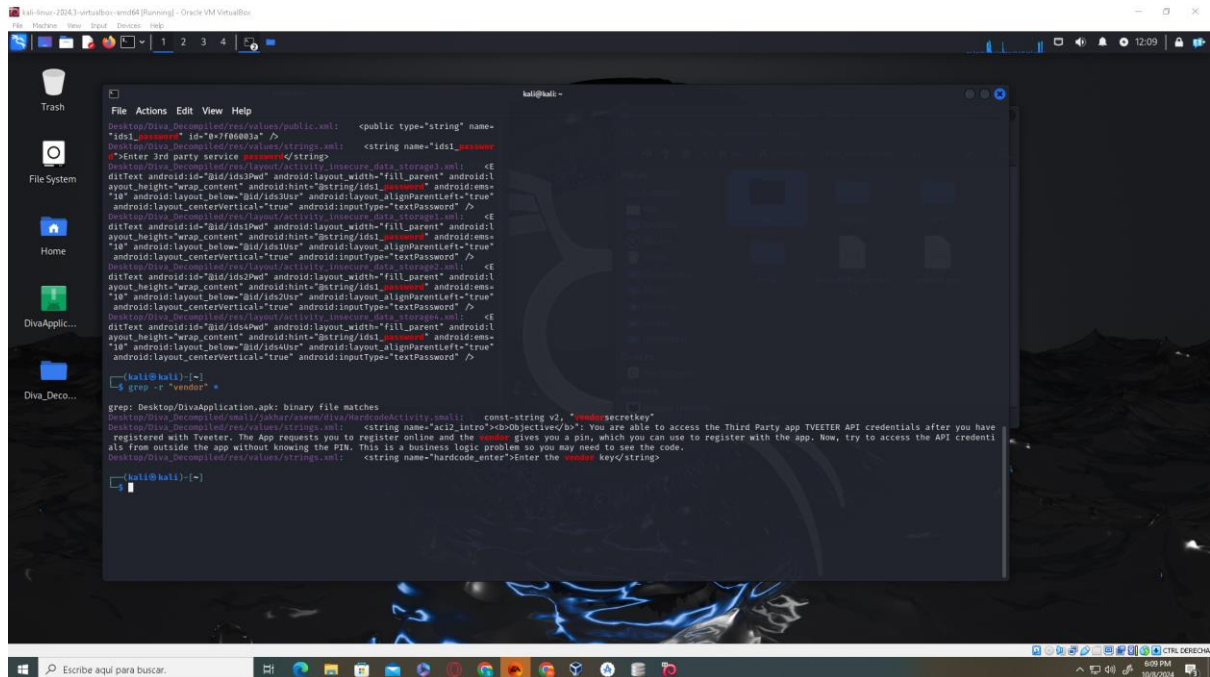
## Índice

<b>Hardcoding Issues.....</b>	<b>pág3.</b>
<b>Input Validation Issues – Parte 1.....</b>	<b>pág4.</b>
<b>Input Validation Issues – Parte 2.....</b>	<b>pág5.</b>
<b>Insecure Data Storage – Parte 1.....</b>	<b>pág6.</b>
<b>Insecure Data Storage – Parte 2.....</b>	<b>pág7.</b>
<b>Biografía.....</b>	<b>pág9.</b>

## **Hardcoding Issues**

La primera actividad se centró en la identificación de valores sensibles hardcodeados en la aplicación DIVA. Utilizando la herramienta APKTool, se decompiló la aplicación para

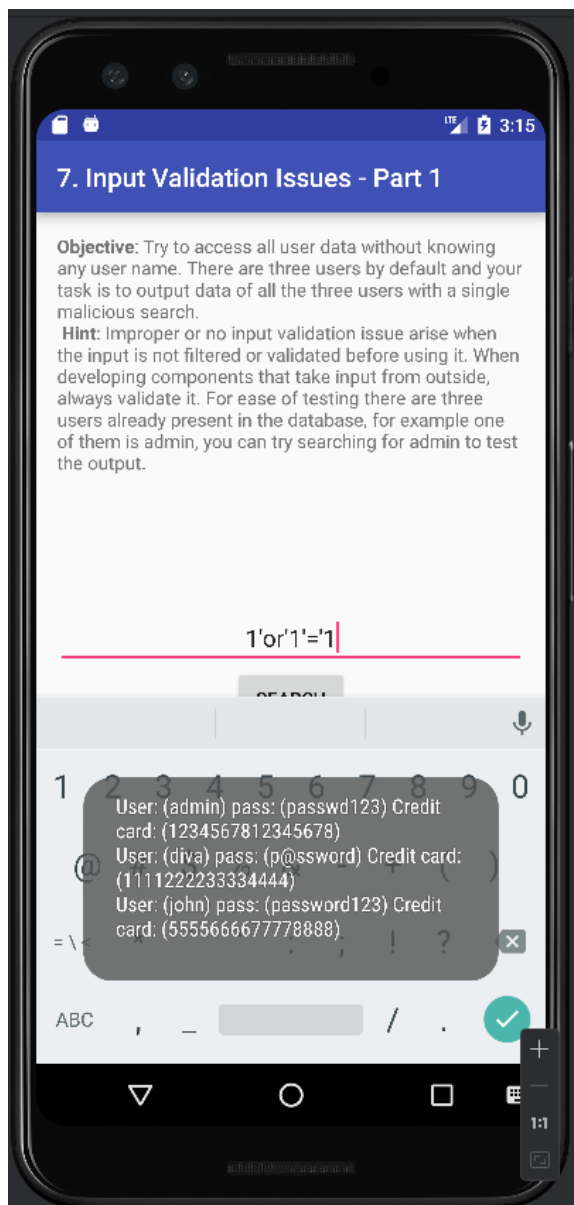
examinar su código. A través de búsquedas específicas en el código decompilado, se identificaron claves y credenciales, incluyendo la clave `vendorsecretkey`. Esta práctica representa una grave vulnerabilidad de seguridad, ya que permite el acceso no autorizado a información sensible.



## Input Validation Issues – Parte 1

En la segunda actividad, se buscó acceder a los datos de usuario sin conocer las credenciales, utilizando técnicas de inyección SQL. Se abrió la aplicación en un emulador y se accedió a la

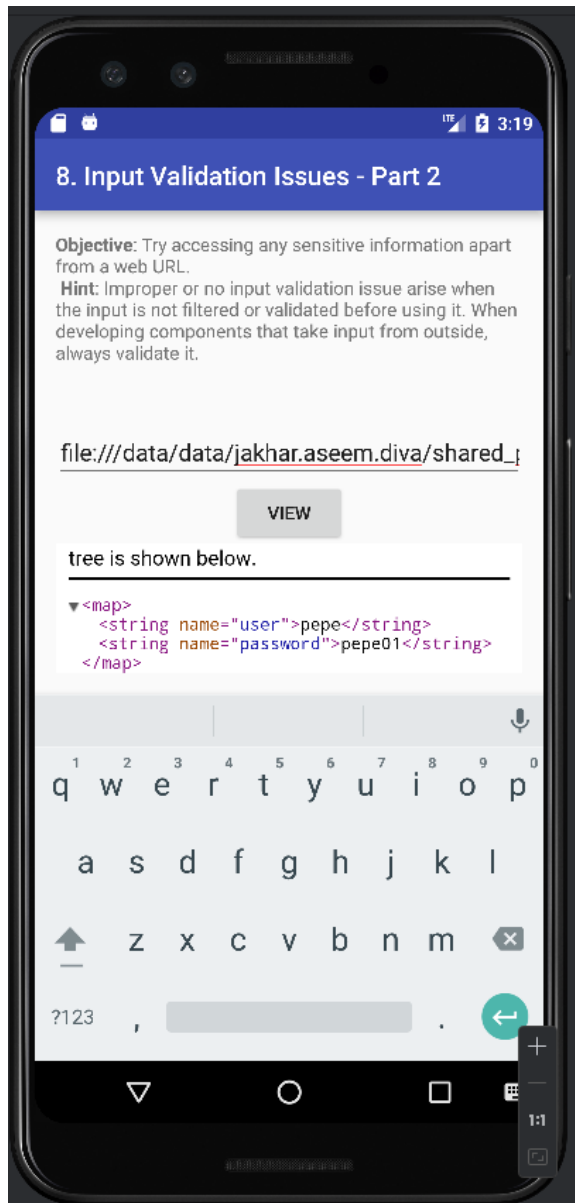
sección de "Input Validation Issues – Part 1". Al identificar el campo para ingresar un nombre de usuario, se ingresó la consulta SQL `1' OR '1'=1`, que es conocida por forzar condiciones siempre verdaderas. Al ejecutar la consulta, se logró recuperar todos los registros de la tabla de usuarios, evidenciando que la aplicación no valida adecuadamente las entradas. Esta actividad subrayó la importancia de implementar medidas de seguridad para prevenir inyecciones SQL.



## Input Validation Issues – Parte 2

La tercera actividad se enfocó en el acceso a información sensible dentro de la aplicación sin recurrir a enlaces web. Nuevamente, se accedió a la aplicación y se navegó hacia la sección

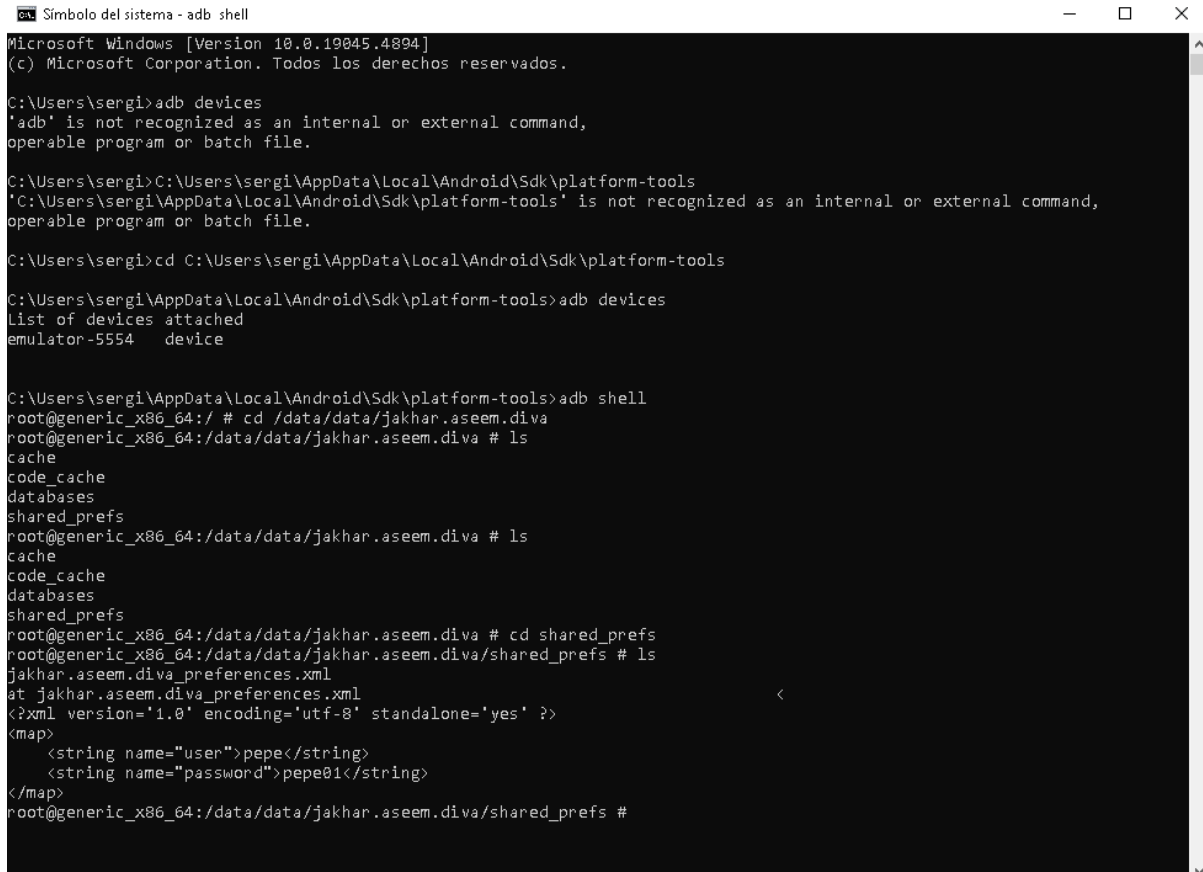
"Input Validation Issues – Part 2". Se ingresó una ruta de archivo local, file:///data/data/jakhar.aseem.diva/private.txt, que pretendía acceder a datos sensibles almacenados. Al ejecutar la consulta, se recuperó información que debería estar protegida, lo que resaltó la vulnerabilidad de la aplicación en el manejo de datos sensibles.



## Insecure Data Storage – Parte 1

La quinta actividad se centró en identificar problemas de almacenamiento inseguro en la aplicación. Se revisó cómo se almacenan las credenciales de usuario, encontrando que la

aplicación presenta fallas en el manejo seguro de datos sensibles. Mediante el uso de comandos de ADB se obtuvieron ambas credenciales de acceso “Username” y “Password”. Este hallazgo subraya la necesidad de adoptar prácticas más seguras en el almacenamiento de información crítica.



```
Símbolo del sistema - adb shell
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\sergi>adb devices
'adb' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\sergi>C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools
'C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\sergi>cd C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools

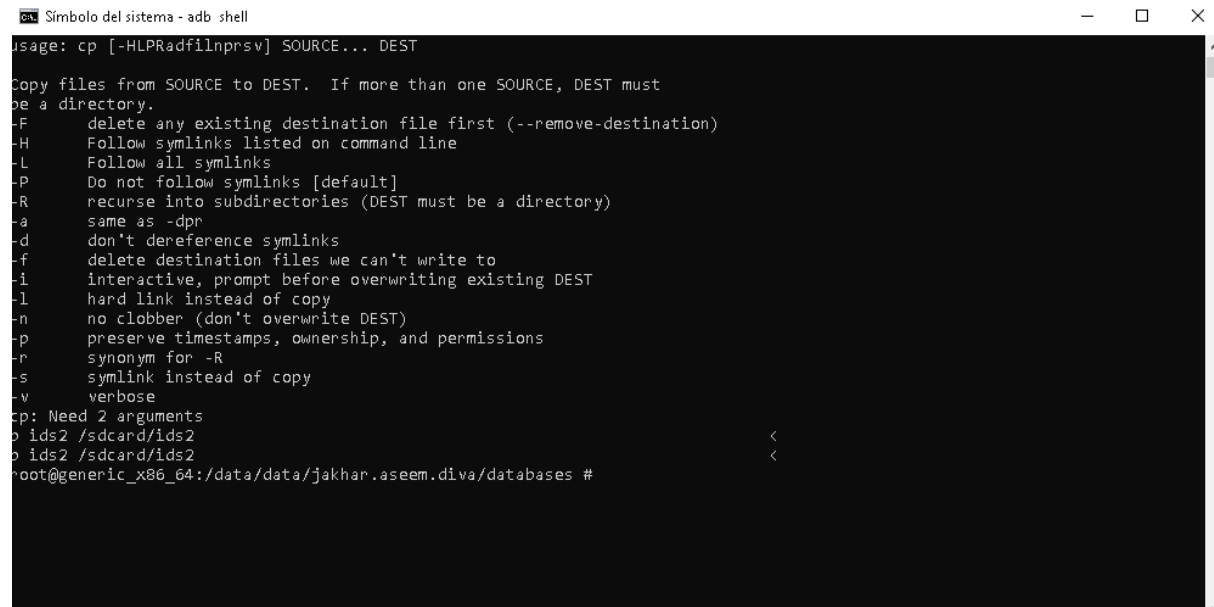
C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools>adb devices
List of devices attached
emulator-5554    device

C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools>adb shell
root@generic_x86_64:/ # cd /data/data/jakhar.aseem.diva
root@generic_x86_64:/data/data/jakhar.aseem.diva # ls
cache
code_cache
databases
shared_prefs
root@generic_x86_64:/data/data/jakhar.aseem.diva # ls
cache
code_cache
databases
shared_prefs
root@generic_x86_64:/data/data/jakhar.aseem.diva # cd shared_prefs
root@generic_x86_64:/data/data/jakhar.aseem.diva/shared_prefs # ls
jakhar.aseem.diva_preferences.xml
at jakhar.aseem.diva_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="user">pepe</string>
  <string name="password">pepe01</string>
</map>
root@generic_x86_64:/data/data/jakhar.aseem.diva/shared_prefs #
```

## Insecure Data Storage – Parte 2

Finalmente, en la última actividad se profundizó en el acceso a información sensible almacenada en la base de datos de la aplicación. Primero se utilizó la shell de ADB para localizar y extraer la base de datos. Finalmente se utilizó DB Browser for SQLite para abrir la

base de datos mediante una consulta SQL y se examinó su contenido. Al acceder a la tabla de usuarios, se recuperaron las credenciales, evidenciando serias vulnerabilidades en el manejo de datos en la aplicación.



```
Simbolo del sistema - adb shell
usage: cp [-HLPRadfilnprsv] SOURCE... DEST
Copy files from SOURCE to DEST.  If more than one SOURCE, DEST must
be a directory.
-F      delete any existing destination file first (--remove-destination)
-H      Follow symlinks listed on command line
-L      Follow all symlinks
-P      Do not follow symlinks [default]
-R      recurse into subdirectories (DEST must be a directory)
-a      same as -dpr
-d      don't dereference symlinks
-f      delete destination files we can't write to
-i      interactive, prompt before overwriting existing DEST
-l      hard link instead of copy
-n      no clobber (don't overwrite DEST)
-p      preserve timestamps, ownership, and permissions
-r      synonym for -R
-s      symlink instead of copy
-v      verbose
cp: Need 2 arguments
b ids2 /sdcard/ids2
b ids2 /sdcard/ids2
root@generic_x86_64:/data/data/jakhar.aseem.diva/databases #
```

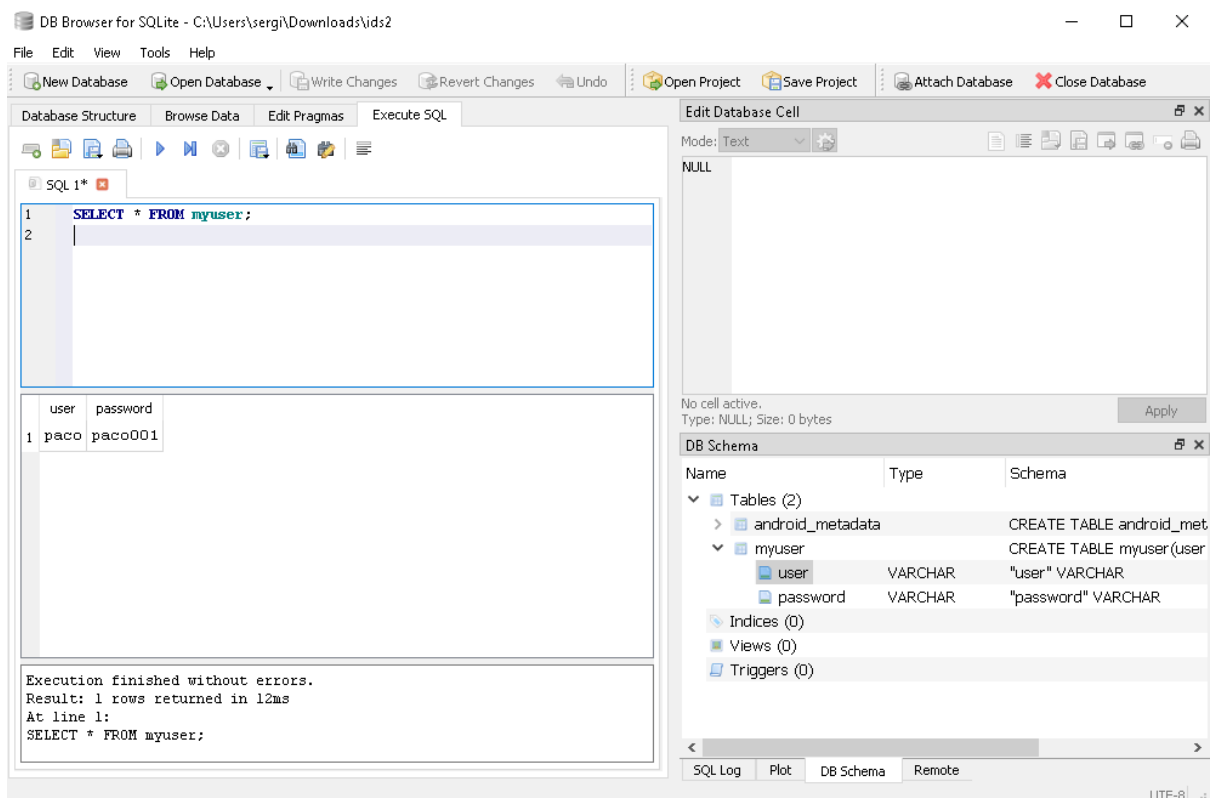
```
Simbolo del sistema
Microsoft Windows [Version 10.0.19045.4894]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\sergi>cd C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools

C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools>adb pull /sdcard/ids2 C:\Users\sergi\Downloads
adb: error: remote object '/sdcard/ids2' does not exist

C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools>adb pull /sdcard/ids2 C:\Users\sergi\Downloads
/sdcard/ids2: 1 file pulled, 0 skipped. 3.6 MB/s (16384 bytes in 0.004s)

C:\Users\sergi\AppData\Local\Android\Sdk\platform-tools>
```



## Bibliografía



*Hardcoding explained.* (2021, agosto 10). Appleute.

<https://www.appleute.de/en/app-developer-library/hardcoding-meaning/>

Jepson, D. (2023, junio 20). *What is improper input validation?* Snyk Learn.

<https://learn.snyk.io/lesson/improper-input-validation/>

*M9: Insecure Data Storage.* (s/f). Owasp.org. Recuperado el 11 de octubre de 2024, de <https://owasp.org/www-project-mobile-top-10/2023-risks/m9-insecure-data-storage>