Solicitud No.	**1**
No. De Pruebas	**1**

Software:	*Estratec Data Store*
Tipo:	*Aplicación móvil*
Versión:	*1.0*
Desarrollador:	*Emmanuel Arizmendi Carrillo*
Supervisor de desarrollo:	*Abel Uriel Martínez Vallejo*
Fecha:	*02-02-2021*

1. OBJETIVO

Verificar si el funcionamiento e implementación de medidas de seguridad en la aplicación realmente funcionan, en caso de encontrarlas corregirlas.

2. ALCANCE

Se realizarán pruebas de vulnerabilidad y funcionalidad de la aplicación a fin de detectar errores o vulnerabilidades de seguridad haciendo uso de programas de uso libre.

3. PROCEDIMIENTO

Acceso no autorizado:

En este caso verificaremos el inicio de sesión y determinar si es susceptible a SQL Inyection.

Para ello usaremos la sentencia ***or pass LIKE %%a%% = true*** para validar si es susceptible a una función lógica.

El resultado es el siguiente.

En este caso usaremos la siguiente operación lógica *pass*=**"or '1'='1**' para determinar si el campo Password es susceptible a inyección SQL.

El resultado es el siguiente.

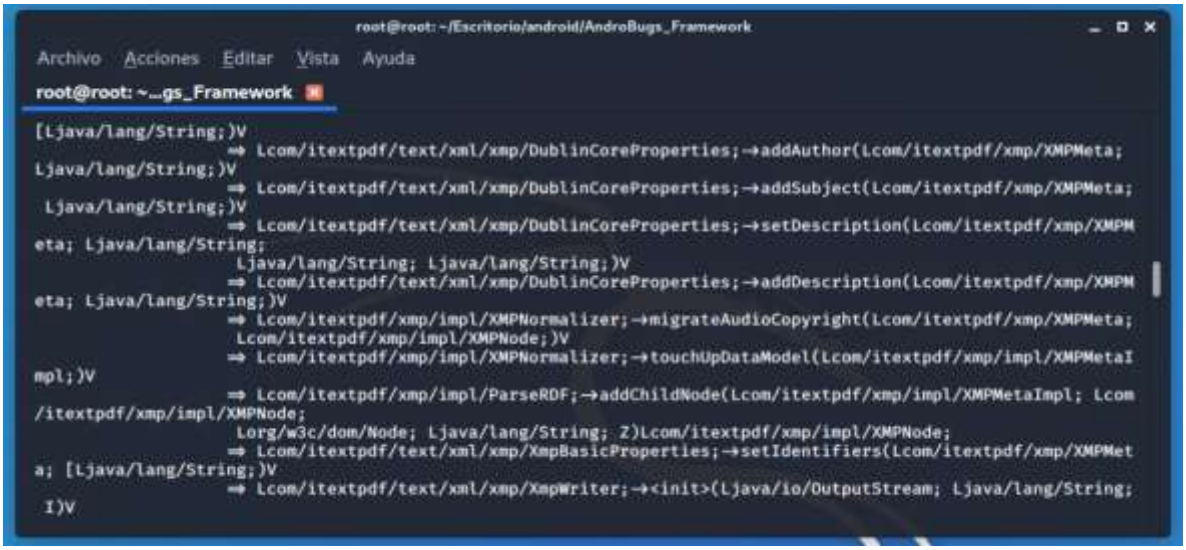
En este caos utilizaremos una combinación de dos campos usuario = 'admin' AND password = '' OR '1'='1';

El resultado es el siguiente.

Androbugs:

Para ello utilizaremos la versión reléase de nuestra aplicación, para ello usaremos la herramienta androbugs y verificaremos el apk.

Comenzará el escaneo.



El resultado es el siguiente.