



Código: FOR-SIG-GTI-06 Ver.:00 Fecha de implementación:08-Oct-18 Vigencia: Julio 2022

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.







Código: FOR-SIG-GTI-06 Ver.:00 Fecha de implementación:08-Oct-18 Vigencia: Julio 2022

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.







Código: FOR-SIG-GTI-06

Ver.:00

Fecha de implementación:08-Oct-18

Vigencia: Julio 2022

El resultado es el siguiente.





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







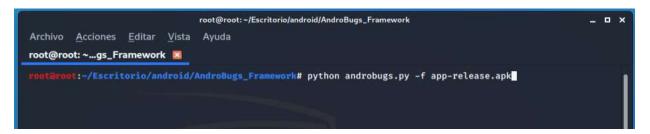
Código: FOR-SIG-GTI-06 Ver.:00 Fecha de implementación:08-Oct-18 Vigencia: Julio 2022

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.







Código: FOR-SIG-GTI-06 | Ver.:00 | Fecha de implementación:08-Oct-18 | Vigencia: Julio 2022

Comenzará el escaneo.

```
root@root: -/Escritorio/android/AndroBugs_Framework
                                                                                                                  _ D X
Archivo Acciones Editar Vista Ayuda
root@root: ~...gs_Framework III
[Ljava/lang/String; )V

    Lcom/itextpdf/text/xml/xmp/DublinCoreProperties;→addAuthor(Lcom/itextpdf/xmp/XMPMeta;

Ljava/lang/String;)V
                       Lcom/itextpdf/text/xml/xmp/DublinCoreProperties;→addSubject(Lcom/itextpdf/xmp/XMPMeta;
 Ljava/lang/String;)V
                      > Lcom/itextpdf/text/xml/xmp/DublinCoreProperties;→setDescription(Lcom/itextpdf/xmp/XMPM
eta; Ljava/lang/String;
Ljava/lang/String; Ljava/lang/String;)V

⇒ Lcom/itextpdf/text/xml/xmp/DublinCoreProperties;→addDescription(Lcom/itextpdf/xmp/XMPM

→ Lcom/itextpdf/text/xml/xmp/DublinCoreProperties;→addDescription(Lcom/itextpdf/xmp/XMPMeta;

→ Lcom/itextpdf/xmp/impl/XMPNormalizer; → migrateAudioCopyright(Lcom/itextpdf/xmp/XMPMeta;

                     Lcom/itextpdf/xmp/impl/XMPNode;)V

→ Lcom/itextpdf/xmp/impl/XMPNormalizer;→touchUpDataModel(Lcom/itextpdf/xmp/impl/XMPMetaI
mpl;)V
a; [Ljava/lang/String;)V

→ Lcom/itextpdf/text/xml/xmp/XmpWriter;→<init>(Ljava/io/OutputStream; Ljava/lang/String;
 IN
```

El resultado es el siguiente.