



PRUEBAS DE FUNCIONALIDAD Y VULNERABILIDAD EN EL DESARROLLO DE APLICACIONES



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 Injection.

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.





PRUEBAS DE FUNCIONALIDAD Y VULNERABILIDAD EN EL DESARROLLO DE APLICACIONES



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'";



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.

```
root@root: ~/Escritorio/android/AndroBugs_Framework
Archivo Acciones Editar Vista Ayuda
root@root: ~/...gs_Framework x
root@root:~/Escritorio/android/AndroBugs_Framework# python androbugs.py -f app-release.apk
```

Comenzará el escaneo.

```
root@root: ~/Escritorio/android/AndroBugs_Framework
Archivo Acciones Editar Vista Ayuda
root@root: ~_gs_Framework
[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
eta; Ljava/lang/String;)V
    => 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
    => Lcom/itextpdf/xmp/impl/ParserRDF; -> addChildNode(Lcom/itextpdf/xmp/impl/XMPMetaImpl; Lcom
/itextpdf/xmp/impl/XMPNode;
    Lorg/w3c/dom/Node; Ljava/lang/String; Z)Lcom/itextpdf/xmp/impl/XMPNode;
    => Lcom/itextpdf/text/xml/xmp/XmpBasicProperties; -> setIdentifiers(Lcom/itextpdf/xmp/XMPMet
a; [Ljava/lang/String;)V
    => Lcom/itextpdf/text/xml/xmp/XmpWriter; -> <init>(Ljava/io/OutputStream; Ljava/lang/String;
```

El resultado es el siguiente.

```
root@root: ~/Escritorio/android/AndroBugs_Framework
Archivo Acciones Editar Vista Ayuda
root@root: ~_gs_Framework
Did not detect SSLSocketFactory by insecure method "getInsecure".
[Info] <SSL_Security> SSL Implementation Checking (HttpHost):
    DEFAULT_SCHEME_NAME for HttpHost check: OK
[Info] <SSL_Security> SSL Implementation Checking (WebViewClient for WebView):
    Did not detect critical usage of "WebViewClient"(MITM Vulnerability).
[Info] Unnecessary Permission Checking:
    Permission 'android.permission.ACCESS_MOCK_LOCATION' sets correctly.
[Info] Accessing the Internet Checking:
    This app is using the Internet via HTTP protocol.
[Info] AndroidManifest System Use Permission Checking:
    No system-level critical use-permission found.
[Info] <WebView> WebView Local File Access Attacks Checking:
    Did not find potentially critical local file access settings.
[Info] <WebView> WebView Potential XSS Attacks Checking:
    Did not detect "setJavaScriptEnabled(true)" in WebView.
[Info] <WebView><Remote Code Execution><CVE-2013-4710#> WebView RCE Vulnerability Checking:
    WebView addJavascriptInterface vulnerabilities not found.
-----
AndroBugs analyzing time: 29.741648 secs
Total elapsed time: 106.376697 secs
<<< Analysis report is generated: /root/Escritorio/android/AndroBugs_Framework/Reports/com.codinginflow.seden
```