



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.	EDS-MV-V1.1-CTRLC01
No. De Pruebas	EDS-MV-V1.1-PFVDA02

Software:	EstratecDataStore
Tipo:	Aplicación móvil
Versión:	1.1
Desarrollador:	Emmanuel Arizmendi Carrillo
Supervisor de desarrollo:	Abel Uriel Martínez Vallejo
Fecha:	13-03-2021

1. OBJETIVO

Verificar el correcto funcionamiento de los cambios realizados en el aplicativo y revisar si no existen vulnerabilidades o un mal funcionamiento en los cambios realizados.

2. ALCANCE

Verificar el correcto funcionamiento del aplicativo, realizar pruebas mediante aplicaciones externas para verificar si existen bugs o vulnerabilidades.

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.



The screenshot shows a login form titled "Iniciar Sesión" with the following fields and values:

- Usuario: `or pass LIKE '%a%' = true`
- Contraseña: `aaaa`
- Técnico: `ISSSTE`

Buttons: INICIAR, SALIR

Las credenciales de inicio de sesión son incorrectas. Inténtalo de nuevo.

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



The screenshot shows the same login form titled "Iniciar Sesión" with the following fields and values:

- Usuario: `admin`
- Contraseña: `pass = 'or '1'='1'`
- Técnico: `ISSSTE`

Buttons: INICIAR, SALIR



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.

Iniciar Sesión

Usuario: admin

Contraseña: pass = 'or'1'='1'

Técnico: *

ISSSTE: *

INICIAR

SALIR

Las credenciales de inicio de sesión son incorrectas. Inténtalo de nuevo!

Mostrar mensaje de termino de uso de aplicación.

Iniciar Sesión

Usuario: Emmanuel Arizmendi Carrillo

Contraseña: *

ERROR DE INICIO DE SESIÓN

Lo sentimos pero ya no tienes acceso a esta aplicación ya que fue de manera temporal, te recomendamos desinstalar esta aplicación... Gracias

ACEPTAR

INICIAR

SALIR

Androbugs:

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

```
root@root: ~/Escritorio/Data Store
Archivo Acciones Editar Vista Ayuda
root@root: ~/Escritorio/Data Store
root@root: ~/Escritorio/Data Store# python androbugs.py -f EstratecDataStore1.1.apk
```

Comenzará el escaneo.

```
root@root: ~/Escritorio/android/AndroBugs_Framework
Archivo Acciones Editar Vista Ayuda
root@root: ~/...gs_Framework
KeyStore 'BKS' type check OK
[Info] Google Cloud Messaging Suggestion:
Nothing to suggest.
[Info] <CVE-2013-4787#> Master Key Type I Vulnerability:
No Master Key Type I Vulnerability in this APK.
[Info] App Sandbox Permission Checking:
No security issues "MODE_WORLD_READABLE" or "MODE_WORLD_WRITEABLE" found on 'openOrCreateDatabase'
or 'openOrCreateDatabase2' or
'getDir' or 'getSharedPreferences' or 'openFileOutput'
[Info] Native Library Loading Checking:
No native library loaded.
[Info] AndroidManifest Dangerous ProtectionLevel of Permission Checking:
No "dangerous" protection level customized permission found (AndroidManifest.xml).
[Info] AndroidManifest PermissionGroup Checking:
PermissionGroup in permission tag of AndroidManifest sets correctly.
[Info] <Implicit_Intent> Implicit Service Checking:
No dangerous implicit service.
[Info] AndroidManifest "intent-filter" Settings Checking:
"intent-filter" of AndroidManifest.xml check OK.
[Info] AndroidManifest Normal ProtectionLevel of Permission Checking:
No default or "normal" protection level customized permission found (AndroidManifest.xml).
```

El resultado es el siguiente.

```
root@root: ~/Escritorio/android/AndroBugs_Framework
Archivo Acciones Editar Vista Ayuda
root@root: ~/...gs_Framework
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: 30.350611 secs
Total elapsed time: 106.287676 secs
<<< Analysis report is generated: /root/Escritorio/android/AndroBugs_Framework/Reports/com.codinginflow.seden
a_820bdeef10d3a5b18bf658fcf6d68e1dfe73ad7bfc7b42c3b82db4351e07873fb951f2d27113ac9d83bffe5aed6d2f174118a2ab1
b94dc7c23bce6fa3f71ff.txt >>>
```



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

Pruebas de funcionalidad:

Para ello realizaremos todas las acciones que realice la aplicación a fin de verificar si los cambios no alteraron el correcto funcionamiento del aplicativo.

Login: Permitir accesos de la aplicación.



Técnico sin acceso al cliente.





PRUEBAS DE FUNCIONALIDAD Y VULNERABILIDAD EN EL DESARROLLO DE APLICACIONES



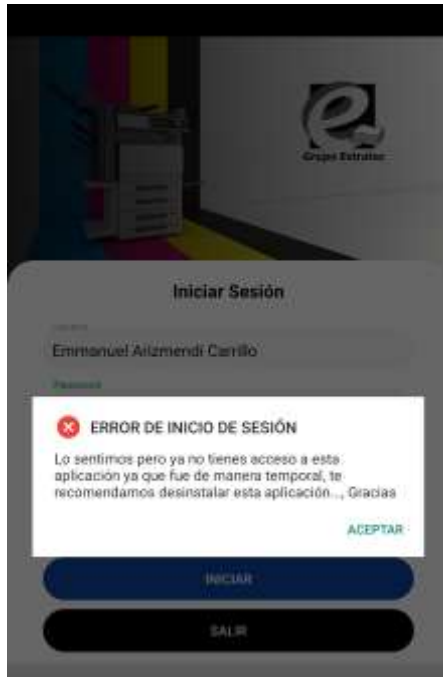
Código: FOR-SIG-GTI-06

Ver.:00

Fecha de implementación:08-Oct-18

Vigencia: Julio 2022

Técnico sin acceso al aplicativo.



Dashboard



Obtener series



Obtener series: mensaje exitoso.



Obtener series: Mensaje sin conexión.



Lista de series pendientes.





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

Interfaz de carga de evidencias



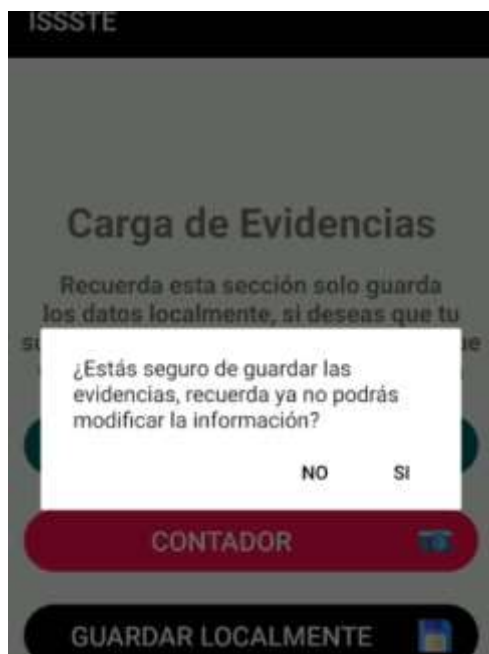
Captura de evidencias en foto.



Cambio de color de evidencia guardada.



Evidencia de Contador opcional.





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

Lista de series completas.

ISSSTE

SERIE

MODELO

UNIDAD

ZD7YBJEHB000QYX

SL-M4020ND

DELEGACION REGIONAL PON

Guardar en el servidor

Estratec Data Store

SINCRONIZANDO



Espera a que se sincronicen las series completas