



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-V1.2-CTRLC02
No. De Pruebas	EDS-MV-V1.2-PFVDA03

Software:	EstratecDataStore
Tipo:	Aplicación móvil
Versión:	1.2
Desarrollador:	Emmanuel Arizmendi Carrillo
Supervisor de desarrollo:	Abel Uriel Martínez Vallejo
Fecha:	26-03-2021

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

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

Buttons: INICIAR, SALIR

El resultado es el siguiente.



Iniciar Sesión

Usuario: admin

Contraseña: pass = 'or'1'='1'

Técnico: *

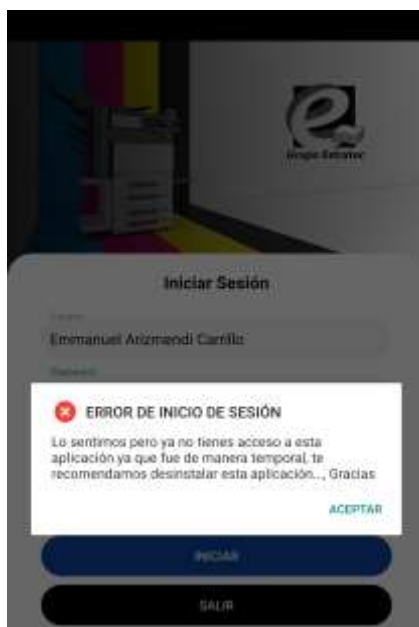
ISSSTE: *

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/android/AndroBugs_Framework
Archivo Acciones Editar Vista Ayuda
root@root: ~/gs_Framework
root@root: ~/Escritorio/android/AndroBugs_Framework# python androbugs.py -f EstratecDataStore1.2.apk
```

Comenzará el escaneo.

```
[Info] <System> AndroidManifest sharedUserId Checking:
      This app does not use "android.uid.system" sharedUserId.
[Info] <SSL_Security> SSL Implementation Checking (Verifying Host Name in Custom Classes):
      Self-defined HOSTNAME VERIFIER checking OK.
[Info] <SSL_Security> SSL Implementation Checking (Verifying Host Name in Fields):
      Critical vulnerability "ALLOW_ALL_HOSTNAME_VERIFIER" field setting or "AllowAllHostnameVerifier" c
lass instance not found.
[Info] <SSL_Security> SSL Implementation Checking (Insecure component):
      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.
```

El resultado es el siguiente.

```
      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: 29.796295 secs
Total elapsed time: 104.511639 secs
<<< Analysis report is generated: /root/Escritorio/android/AndroBugs_Framework/Reports/com.codinginflow.seden
a_5e4b043d34f0a29cdec7fdd35655c0f66f6350257a45070d58d0e273b26c3e216d29a16e81ae5c41220fbae2afe47f9092afae55d5
932ba575c210600136bd2.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



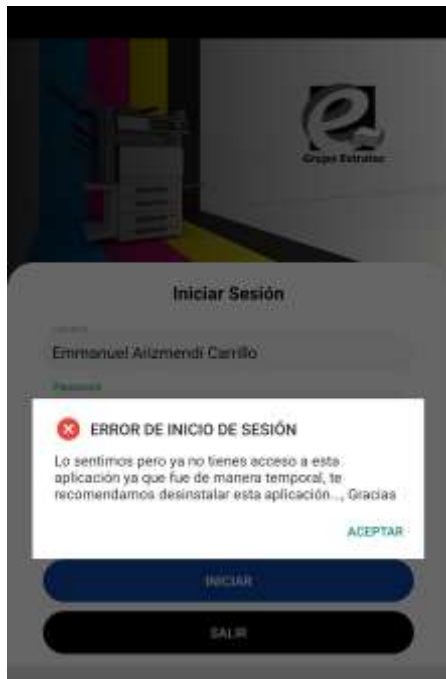
Código: FOR-SIG-GTI-06

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.



Edición de datos.

ISSSTE

DATOS DEL USUARIO

Cliente
ISSSTE

Nombre del usuario
EJEM: JUAN CASTRO MORALES

Puesto
EJEM: JEFE DE OFICINA

No. de Empleado
EJEM: 20052

Email
EJEM: usuario@issste.gob.mx

No. de Red
EJEM: 20

DATOS DE LA UBICACIÓN

Edición de campo Piso.

ISSSTE

DATOS DE LA UBICACIÓN

ID Unidad Administrativa

Unidad Administrativa
DELEGACION TEST DATAS

Área de Adscripción
TEST 4

Nombre del enlace
Jguillen

Calle y Número
Av test #3

Piso
Piso 5

Colonia
Fovissste

CP
11111

Interfaz de carga de evidencias

ISSSTE

Carga de Evidencias

Recuerda esta sección solo guarda los datos localmente, si deseas que tu supervisor visualice los datos tendras que Guardar en el Servidor (con Conexión a Internet)

FUA



CONTADOR



GUARDAR LOCALMENTE



Captura de evidencias en foto.



Cambio de color de evidencia guardada.

ISSSTE

Carga de Evidencias

Recuerda esta sección solo guarda los datos localmente, si deseas que tu supervisor visualice los datos tendras que Guardar en el Servidor (con Conexión a Internet)

FUA



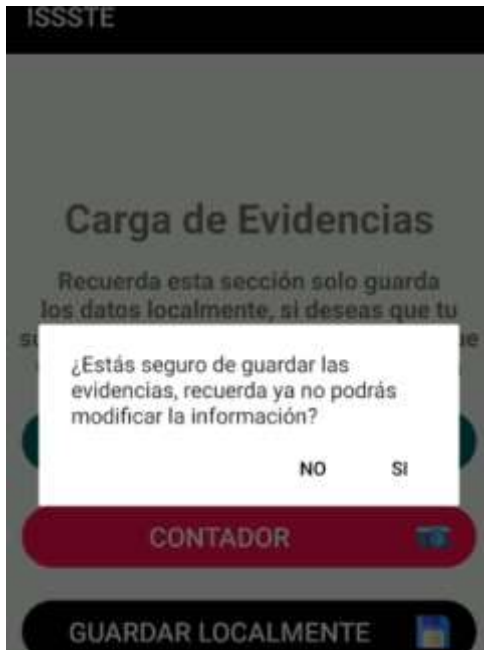
CONTADOR



GUARDAR LOCALMENTE



Evidencia de Contador opcional.



Lista de series completas.





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

Guardar en el servidor

