

Guía del usuario de Marvin

Juan Heguiabehere

1. Who, Why, What, When (Introducción)

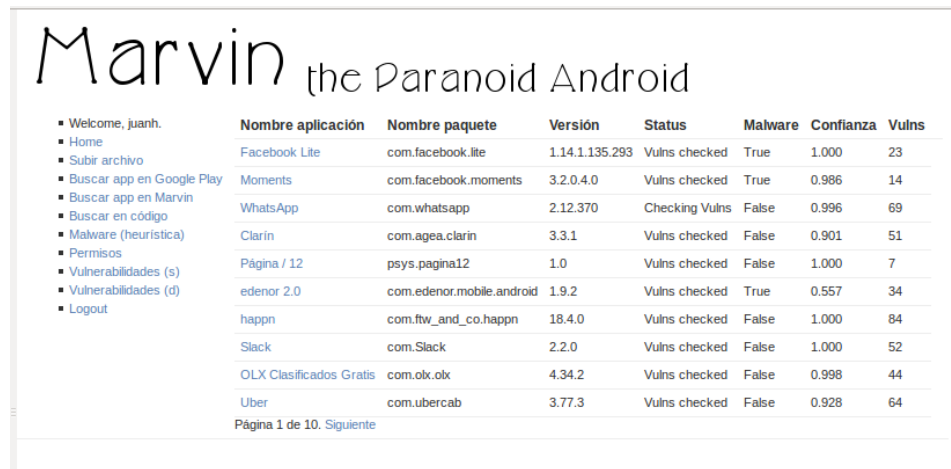
Marvin es una plataforma para análisis y seguimiento de aplicaciones sobre la plataforma Android. Permite levantar aplicaciones desde el Google Play Store o desde archivos `.apk`, los analiza estática y dinámicamente, y lleva un registro de las diferentes versiones en una instancia de GitLab. Los componentes principales de Marvin son:

- **marvin-frontend**: se ocupa de la interfaz de usuario, la decompilación de aplicaciones, la base de datos y la interacción con **marvin-static-analyzer**
- **marvin-static-analyzer**: se ocupa de buscar tipos específicos de vulnerabilidades en una aplicación.
- **marvin-dynamic-analyzer**: se ocupa de verificar si las vulnerabilidades encontradas estáticamente por **marvin-static-analyzer** se pueden disparar.

En principio **marvin-static-analyzer** y **marvin-dynamic-analyzer** funcionan sin interacción con el usuario, así que esta es mayormente una guía de uso de **marvin-frontend**.

Marvin fue desarrollado por Juan Heguiabehere y Joaquin Rinaudo del equipo STIC de la Fundación Manuel Sadosky: <http://www.fundacionsadosky.org.ar/programas/seguridad-en-tic/>.

2. Pantalla principal



| Nombre aplicación | Nombre paquete | Versión | Status | Malware | Confianza | Vulns |
|---|---------------------------|----------------|----------------|---------|-----------|-------|
| Facebook Lite | com.facebook.lite | 1.14.1.135.293 | Vulns checked | True | 1.000 | 23 |
| Moments | com.facebook.moments | 3.2.0.4.0 | Vulns checked | True | 0.986 | 14 |
| WhatsApp | com.whatsapp | 2.12.370 | Checking Vulns | False | 0.996 | 69 |
| Clarín | com.agea.clarin | 3.3.1 | Vulns checked | False | 0.901 | 51 |
| Página / 12 | psys.pagina12 | 1.0 | Vulns checked | False | 1.000 | 7 |
| edenor 2.0 | com.edenor.mobile.android | 1.9.2 | Vulns checked | True | 0.557 | 34 |
| happn | com.ftw_and_co.happn | 18.4.0 | Vulns checked | False | 1.000 | 84 |
| Slack | com.Slack | 2.2.0 | Vulns checked | False | 1.000 | 52 |
| OLX Clasificados Gratis | com.olx.olx | 4.34.2 | Vulns checked | False | 0.998 | 44 |
| Uber | com.ubercab | 3.77.3 | Vulns checked | False | 0.928 | 64 |

Página 1 de 10. [Siguiente](#)

Figura 1: Pantalla de inicio de Marvin

La pantalla principal de Marvin se divide en dos partes: a la izquierda está el menú de acciones y a la derecha la lista de aplicaciones. En esta lista podemos ver las últimas 10 aplicaciones subidas, con algo de información sobre las mismas. De izquierda a derecha, podemos ver:

- El nombre “de fantasía” de la aplicación.
- El nombre de paquete de la aplicación, con el que la identifica Google Play Store.
- El número de versión de la aplicación.
- El estado de proceso de la aplicación (puede estar encolada, en chequeo de vulnerabilidades o ya chequeada)
- Si la heurística de permisos determinó que la aplicación podía o no ser malware y con cuánta confianza
- La cantidad de potenciales vulnerabilidades encontradas para la aplicación.

Clickear en el nombre de la aplicación nos lleva a su página de información (ver Sección 3.1)

3. Menú de acciones

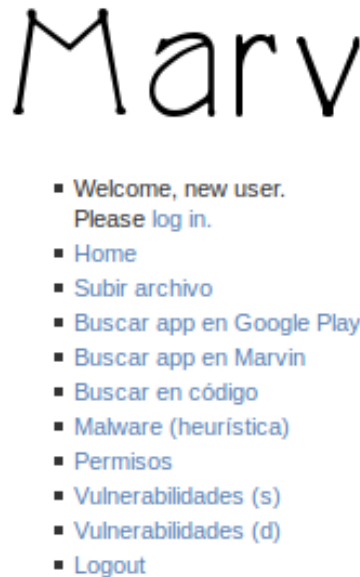


Figura 2: Menú de acciones

El menú de acciones es desde donde se disparan todas las actividades de Marvin. De arriba hacia abajo, estas son:

- Ingresar (algunas acciones requieren identificarse como usuario)
- Ir a la pantalla de inicio
- Subir un archivo: Permite subir un archivo `.apk` que uno tenga.
- Buscar app en Google Play: Permite descargar aplicaciones desde Google Play Store.
- Buscar app en Marvin: Permite buscar una aplicación en Marvin, por nombre de aplicación o de paquete.
- Buscar en código: Permite hacer búsquedas por texto en el código fuente de las aplicaciones.

- Malware (heurística): Da una lista de las aplicaciones que el método heurístico calificó como posible malware, ordenados por la confianza en el resultado.
- Permisos: Da una lista de los permisos encontrados por Marvin, junto con la cantidad de aplicaciones que los solicitan.
- Vulnerabilidades(s): Da una lista de las vulnerabilidades que busca estáticamente Marvin, ordenadas por cantidad de instancias encontradas.
- Vulnerabilidades(d): Da una lista de las vulnerabilidades que busca dinámicamente Marvin, ordenadas por cantidad de instancias encontradas.
- Logout (desconectarse)

3.1. Información de las aplicaciones

En cualquier lista de aplicaciones, clickear en el nombre de la aplicación nos lleva a la pantalla de información de aplicaciones. Esta pantalla tiene tres secciones:

- Metadatos y acceso a repositorios
- Heurística y permisos
- Componentes
- Vulnerabilidades

Marvin the Paranoid Android

- Welcome, new user.
Please [log in](#).
- [Home](#)
- [Subir archivo](#)
- [Buscar app en Google Play](#)
- [Buscar app en Marvin](#)
- [Buscar en código](#)
- [Malware \(heurística\)](#)
- [Permisos](#)
- [Vulnerabilidades \(s\)](#)
- [Vulnerabilidades \(d\)](#)
- [Logout](#)

Clarín

| | |
|-----------------------|--|
| Package name | com.agea.clarin |
| Version | 3.3.1 |
| Subida a Google Play | 13 nov. 2015 |
| Autor | AGEA MOBILE |
| Nombre en Google Play | Clarín |
| Subida a Google Play | 13 nov. 2015 |
| Enlace Google Play | Última versión |
| md5 | 0e2d0a7926317f3144171214ec0f90e2 |
| sha1 | 08060ba17094d654085353af3d39d7631a58ca90 |
| Subida a Marvin | Nov. 30, 2015 |

[Git](#)
[APK](#)
[Borrar](#)

Figura 3: Metadatos y acceso a repositorios

En la sección de metadatos y acceso a los repositorios, podemos ver datos como la fecha de subida de una aplicación a Google Play, el número de versión o los checksums del archivo, así como acceder a los repositorios de código fuente (el botón llamado Git¹), del APK propiamente dicho, o de Google Play (aunque en ese caso nos lleva a la última versión sin importar cuál estemos viendo). También nos permite borrar una aplicación de Marvin.

¹Este botón permanecerá grisado hasta que los fuentes hayan terminado de cargarse en el repositorio.

Análisis según permisos

Malware: False

Confianza en el resultado: 0.901

Permisos

| Nombre | Nivel de peligro | Cantidad de paquetes | Descripción |
|---|------------------|----------------------|--|
| android.permission.VIBRATE | normal | 42 | control vibrator |
| android.permission.RECEIVE_BOOT_COMPLETED | normal | 32 | automatically start at boot |
| com.google.android.c2dm.permission.RECEIVE | normal | 41 | Unknown permission from android reference |
| android.permission.ACCESS_NETWORK_STATE | normal | 88 | view network status |
| android.permission.WAKE_LOCK | normal | 55 | prevent phone from sleeping |
| android.permission.INTERNET | dangerous | 94 | full Internet access |
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | 73 | modify/delete SD card contents |
| android.permission.GET_ACCOUNTS | normal | 44 | discover known accounts |
| android.permission.ACCESS_FINE_LOCATION | dangerous | 45 | fine (GPS) location |
| android.permission.READ_PHONE_STATE | dangerous | 45 | read phone state and identity |
| android.permission.ACCESS_COARSE_LOCATION | dangerous | 41 | coarse (network-based) location |
| android.permission.ACCESS_WIFI_STATE | normal | 47 | view Wi-Fi status |
| android.permission.ACCESS_LOCATION_EXTRA_COMMANDS | normal | 7 | access extra location provider commands |
| android.permission.READ_EXTERNAL_STORAGE | normal | 21 | read from external storage |
| android.permission.USE_CREDENTIALS | dangerous | 15 | use the authentication credentials of an account |
| com.agea.clarin.permission.C2D_MESSAGE | signature | 1 | C2DM permission. |

Figura 4: Heurística y permisos

La sección de heurística y permisos nos muestra el resultado del análisis bayesiano de permisos, y los permisos que solicita la aplicación. La lista de permisos nos muestra el nombre, el nivel de peligro del mismo, la cantidad de paquetes que lo solicitan y una descripción somera de lo que permite hacer o acceder. Clickear en el nombre de alguno de los permisos nos lleva a una página con información y estadísticas del mismo (ver Sección 3.5).

Actividades

com.facebook.lite.MainActivity
com.facebook.lite.photo.AlbumGalleryActivity
com.facebook.lite.photo.PreviewActivity

Proveedores

com.facebook.lite.photo.MediaContentProvider
com.facebook.lite.diode.UserValuesProvider

Servicios

com.facebook.lite.FbnsIntentService
com.facebook.rti.push.service.FbnsService
com.facebook.lite.GCMIntentService

Receptores

com.google.android.gcm.GCMBroadcastReceiver
com.facebook.lite.campaign.CampaignReceiver
com.facebook.lite.deviceid.UniqueDeviceIdBroadcastSender\$LocalBroadcastReceiver
com.facebook.lite.deviceid.UniqueIdSupplier
com.facebook.lite.net.ConnectivityReceiver
com.facebook.lite.FbnsIntentService\$CallbackReceiver
com.facebook.rti.push.service.MqttSystemBroadcastReceiver
com.facebook.lite.notification.PushRegistrationBroadcastReceiver

Figura 5: Componentes

La sección de componentes nos muestra las actividades, proveedores, servicios y receptores de una aplicación. Si se terminó de decompilar, clicar en alguno de estos items nos lleva a una nueva pestaña con el código fuente que lo implementa.

| Vulnerabilidades | | | | |
|-------------------------|-----------|---|---------|-------------------|
| Nombre | Severidad | Clase | Método | Pruebas dinámicas |
| SSL_WEBVIEW_ERROR | 1 | com/facebook/internal/WebViewDialog\$DialogWebViewClient.java | | True |
| SSL_WEBVIEW_ERROR | 1 | com/innobits/e/a/t/b/j.java | | True |
| SSL_WEBVIEW_ERROR | 1 | com/innobits/a/d/k.java | | True |
| SSL_WEBVIEW_ERROR | 1 | com/innobits/b/e.java | | True |
| SSL_WEBVIEW_ERROR | 1 | com/smartadserver/android/library/controller/SASWebViewClient.java | | True |
| SSL_CUSTOM_TRUSTMANAGER | 1 | org/apache/http/conn/ssl/SSLContextBuilder\$TrustManagerDelegate.java | | True |
| INTENT_HIJACKING | 3 | com/agea/c/clarif/m.java | c | False |
| INTENT_HIJACKING | 3 | com/agea/c/clarif/m.java | onClick | False |

Figura 6: Vulnerabilidades

La sección de vulnerabilidades nos muestra una lista de las vulnerabilidades encontradas por **marvin-static-analyzer**; podemos ver el nombre de la vulnerabilidad, la severidad de la misma, la clase en que fue encontrada, el método si corresponde, y si la vulnerabilidad se puede verificar mediante análisis dinámico. Clicar en el nombre de la vulnerabilidad nos da infor-

mación sobre la misma en general, mientras que clickear en el nombre de la clase nos abre una nueva pestaña con la página de GitLab correspondiente al código fuente de la misma.

3.2. Búsqueda en Google Play Store

Marvin puede buscar y descargar aplicaciones de Google Play. Para esto, seleccionar “Buscar app en Google Play” en el menú de acciones, ingresar los términos de búsqueda deseados en el campo de texto que aparece al final del menú, y presionar Enter (o el botón de Search).

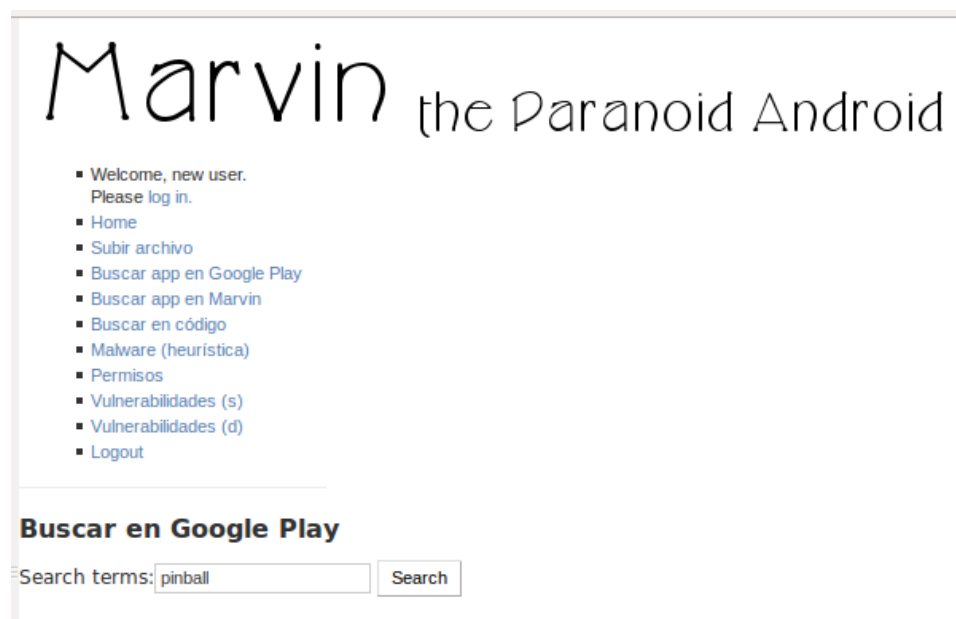


Figura 7: Búsqueda en Google Play - Términos de búsqueda

La pantalla de resultados es como se ve en la Figura 8: tiene algunos datos básicos de cada aplicación, más la fecha de carga en Google Play y la cantidad de descargas. Si elegimos alguna de estas aplicaciones, pasamos a una pantalla como la de la Figura 9, donde se ven algunos datos más de la aplicación tales como la descripción y los permisos que solicita, y se puede solicitar la descarga de la aplicación desde Google Play Store. Esto hace que se descargue la aplicación y se procese. El análisis: Primero la aplicación es decompilada, luego se realiza el análisis estático. Sin embargo, como el

proceso de carga de los fuentes en la base de datos y el GitLab toma tiempo, usualmente el análisis termina antes de que el repositorio esté listo. Hasta que los fuentes no están terminados de subir a GitLab, los links al código fuente darán error 404.

Marvin

the Paranoid Android

- Welcome, juanh.
- Home
- Subir archivo
- Buscar app en Google Play
- Buscar app en Marvin
- Buscar en código
- Malware (heurística)
- Permisos
- Vulnerabilidades (s)
- Vulnerabilidades (d)
- Logout

| App name | Package name | Version | Author | Upload date | Downloads |
|----------------------------|--|---------|----------------------------|--------------|-------------|
| Pinball Pro | com.PinballGame | 11 | TerranDroid | 3 dic. 2015 | 10,000,000+ |
| Pinball | com.nix.game.pinball.free | 32 | Magma Mobile | 24 dic. 2013 | 10,000,000+ |
| Pinball Deluxe | com.greencod.pinball.android | 161507 | GreenCod Apps | 10 mar. 2015 | 5,000,000+ |
| Pinball Arcade Free | com.farsight.AndroidPinball.javaProject | 172 | Farsight Studios | 2 dic. 2015 | 5,000,000+ |
| Pinball Classic | com.janeking.pinball | 4 | TerranDroid | 13 ago. 2012 | 5,000,000+ |
| Destruction de Ladrillos | com.daf.archanoide | 36 | DAF | 21 nov. 2015 | 5,000,000+ |
| Zen Pinball | com.zenstudios.ZenPinball | 64 | Zen Studios | 16 dic. 2015 | 1,000,000+ |
| Pinball Fantasy HD | com.funfactory.pinball | 3075 | Creative Mobile Publishing | 5 ene. 2015 | 1,000,000+ |
| Ghostbusters™ Pinball | com.farsight.GhostBustersPinball.javaProject | 24 | Farsight Studios | 10 mar. 2015 | 100,000+ |
| PinBall.L | com.mebzey.bouncyy | 1 | MebZey | 8 mar. 2015 | 100,000+ |
| Pinball 3D FREE | aklimeart.com | 10 | alDine Games | 8 dic. 2012 | 100,000+ |
| Pinball Star | com.mobistar.pinballdeluxe | 15065 | mobistar | 17 dic. 2015 | 100,000+ |
| Zaccaria Pinball | hu.magicpixel.Zaccaria | 20 | Magic Pixel KFT. | 4 sep. 2015 | 50,000+ |
| The Walking Dead Pinball | com.zenstudios.TWDPinball | 10 | Zen Studios | 24 jun. 2015 | 10,000+ |
| South Park™ Pinball | com.zenstudios.SPPinball | 10 | Zen Studios | 24 jun. 2015 | 10,000+ |
| Pinball 3D | com.mtgames.pinball3d | 3 | Multi Touch Games | 2 dic. 2015 | 10,000+ |
| Pinball Juego Gratis | chat.sebastian.pinballpro | 5 | SebastianChat | 2 nov. 2014 | 10,000+ |
| Kickboard - Soccer Pinball | at.citrusmedia.kickboardgame | 2 | Citrus Media | 20 sep. 2014 | 10,000+ |
| Family Guy Pinball | com.zenstudios.FamilyGuyPinball | 5 | Zen Studios | 24 nov. 2015 | 1,000+ |
| Pro Pinball | com.barnstormgames.propinball | 11 | Barnstorm Games | 30 nov. 2015 | 100+ |

Page 1 of 1.

Figura 8: Búsqueda en Google Play - Resultados

Marvin the Paranoid Android

- Welcome, juanh.
- Home
- Subir archivo
- Buscar app en Google Play
- Buscar app en Marvin
- Buscar en código
- Malware (heurística)
- Permisos
- Vulnerabilidades (s)
- Vulnerabilidades (d)
- Logout

Pinball Pro

| | |
|--------------|-----------------|
| Package name | com.PinballGame |
| Version | 2.0 |
| Author | TerranDroid |
| Uploaded | 3 dic. 2015 |

Descripción

Pinball Pro es el juego de pinball No. 1 para el teléfono Android y cuenta con verdadera representación del juego más clásico de Pinball. En este juego de pinball se establece un nuevo estándar para simular colisiones físicas y el proceso de detalles gráficos del balón real, usted quedará sorprendido con el nivel de realismo y efectos visuales de pinball.<p>Como se Juega:
 Presione el botón en cualquier lugar para poner en marcha un nuevo balón
 Toque la pantalla hacia el lado derecho o izquierdo para controlar lanzamientos<p>Características del juego:
 Tres tablas innovadoras: la versión clásica, versión de piedra de la suerte y versión de rueda de la suerte.
 Deslumbrantes imágenes visuales
 Una banda sonora excepcional con la música atmosférica, efectos de sonido
 Movimiento físico del balón más avanzado<p>Pinball Pro is #1 pinball game for your Android phone and features exact recreations of the all-time greatest pinball tables.<p>This game sets a new standard for realistic ball physics and graphical detail in pinball video games. You will be stunned with the level of realism and cutting-edge visuals.<p>How to Play:
 Press and hold anywhere to launch a new ball
 Touch right or left side to control flips<p>Game Features:
 3 Innovative Table: Classic, Lucky Stones, Lucky Wheel
 Visually stunning graphics
 Unique soundtrack with atmospheric music, sound effects
 The most advanced ball physics

Permisos

```
android.permission.ACCESS_WIFI_STATE
android.permission.INTERNET
android.permission.WRITE_EXTERNAL_STORAGE
android.permission.ACCESS_NETWORK_STATE
android.permission.READ_PHONE_STATE
android.permission.VIBRATE
android.permission.READ_EXTERNAL_STORAGE
```

[Descargar de Play Store](#)

Figura 9: Búsqueda en Google Play - Descripción

3.3. Buscar en código

La opción “Buscar en código” nos permite buscar strings arbitrarios en la base de código de Marvin, por ejemplo para buscar casos de utilización de alguna biblioteca de Java o servicio de Android. Simplemente escribir los términos de búsqueda en el campo provisto y dar Enter, como se ve en la Figura 10. Los resultados se verán como los de la Figura 11: para cada coincidencia, se muestra el nombre de la clase, la aplicación a la que pertenece, y el largo del archivo fuente. Clickear en el nombre del archivo nos lleva al archivo mismo en el repositorio GitLab.

Marvin the Paranoid Android

- Welcome, new user.
Please [log in](#).
- [Home](#)
- [Subir archivo](#)
- [Buscar app en Google Play](#)
- [Buscar app en Marvin](#)
- [Buscar en código](#)
- [Malware \(heurística\)](#)
- [Permisos](#)
- [Vulnerabilidades \(s\)](#)
- [Vulnerabilidades \(d\)](#)
- [Logout](#)

Buscar en código fuente

Search terms:

Figura 10: Búsqueda en código fuente

Marvin

the Paranoid Android

- Welcome, juanh.
- Home
- Subir archivo
- Buscar app en Google Play
- Buscar app en Marvin
- Buscar en código
- Malware (heurística)
- Permisos
- Vulnerabilidades (s)
- Vulnerabilidades (d)
- Logout

Aplicacion

| App name | File name | Length |
|---|----------------------------|--------|
| com/squareup/okhttp/Address | BA 147 | 4186 |
| com/squareup/okhttp/OkHttpClient | BA 147 | 10934 |
| com/google/api/client/http/javanet/Net-HttpTransport\$Builder | BA WiFi | 2869 |
| com/google/api/client/http/javanet/Net-HttpTransport | BA WiFi | 2578 |
| org/apache/http/conn/ssl/SSLConnectionSocketFactory | Clarín | 11558 |
| org/apache/http/impl/client/HttpClientBuilder | Clarín | 26485 |
| Lcom/squareup/okhttp/Address; | EFF Alerts | 4082 |
| Lcom/squareup/okhttp/OkHttpClient; | EFF Alerts | 10605 |
| com/squareup/okhttp/Address | Fondos HD (Backgrounds HD) | 5963 |
| com/squareup/okhttp/OkHttpClient | Fondos HD (Backgrounds HD) | 16841 |
| com/squareup/okhttp/OkHttpClient | Fondos HD (Backgrounds HD) | 16841 |
| ch/boye/httpclientandroidlib/conn/ssl/SSLSocketFactory | Instagram | 12005 |
| com/squareup/okhttp/Address | OLX Clasificados Gratis | 5834 |
| com/squareup/okhttp/OkHttpClient | OLX Clasificados Gratis | 16999 |

Figura 11: Búsqueda en código fuente - Resultados

3.4. Malware (heurística)

En esta opción podemos ver las aplicaciones que según la heurística tienen más probabilidades de ser en realidad malware. Junto a la información de versión, se ve un indicador de la confianza que tiene Marvin en su resultado, y la cantidad de vulnerabilidades encontradas para cada aplicación.

Marvin the Paranoid Android

[illegible]

Figura 12: Malware según la heurística de permisos

3.5. Permisos

La opción Permisos nos permite ver los permisos relevados por Marvin entre todas las aplicaciones, y para éstos una descripción, su nivel de riesgo y la cantidad de aplicaciones relevadas que lo solicitan (ver Figura 13). Si clickeamos en el nombre de algún permiso, Marvin nos muestra las aplicaciones que lo solicitan, como se ve en la Figura 14

Marvin

the Paranoid Android

- Welcome, juanh.
- Home
- Subir archivo
- Buscar app en Google Play
- Buscar app en Marvin
- Buscar en código
- Malware (heurística)
- Permisos
- Vulnerabilidades (s)
- Vulnerabilidades (d)
- Logout

| Permission name | Danger level | # of packages | Description |
|---|--------------|---------------|---|
| android.permission.VIBRATE | normal | 42 | control vibrator |
| android.permission.RECEIVE_BOOT_COMPLETED | normal | 32 | automatically start at boot |
| org.eff.actioncenter.permission.C2DM_MESSAGE | signature | 1 | C2DM permission. |
| com.google.android.c2dm.permission.RECEIVE | normal | 41 | Unknown permission from android reference |
| android.permission.ACCESS_NETWORK_STATE | normal | 88 | view network status |
| android.permission.WAKE_LOCK | normal | 55 | prevent phone from sleeping |
| android.permission.INTERNET | dangerous | 94 | full Internet access |
| android.permission.WRITE_EXTERNAL_STORAGE | dangerous | 73 | modify/delete SD card contents |
| android.permission.GET_ACCOUNTS | normal | 44 | discover known accounts |
| android.permission.ACCESS_FINE_LOCATION | dangerous | 45 | fine (GPS) location |
| android.permission.READ_PHONE_STATE | dangerous | 45 | read phone state and identity |
| com.google.android.providers.gsf.permissions.READ_GSERVICES | normal | 0 | Unknown permission from android reference |
| android.permission.ACCESS_COARSE_LOCATION | dangerous | 41 | coarse (network-based) location |
| android.permission.CALL_PHONE | dangerous | 18 | directly call phone numbers |

Figura 13: Permisos relevados por Marvin

Marvin

the Paranoid Android

- Welcome, juanh.
- Home
- Subir archivo
- Buscar app en Google Play
- Buscar app en Marvin
- Buscar en código
- Malware (heurística)
- Permisos
- Vulnerabilidades (s)
- Vulnerabilidades (d)
- Logout

Permiso android.permission.VIBRATE

Danger level

normal

Description

control vibrator

App count

42

| App name | Package name | Version | Status | APK | Source | Delete |
|---|---|--------------|----------------|-----|---------|--------|
| EFF Alerts | org.eff.actioncenter | 0.0.5 | Vulns checked | APK | Sources | Delete |
| com.tucarro | com.tucarro | 2.0.5 | Vulns checked | APK | Sources | Delete |
| com.con.vos.en.el.celu | com.con.vos.en.el.celu | 2.0 | QUEUED | APK | Sources | Delete |
| com.estrongs.android.pop | com.estrongs.android.pop | 3.2.2 | Checking Vulns | APK | Sources | Delete |
| Clean Master Pro | com.fastversion.master.motorola | 1.1 | Checking Vulns | APK | Sources | Delete |
| org.microemu.android.model.common.VTUserApplicationLINKMB | org.microemu.android.model.common.VTUserApplicationLINKMB | 3.0.2.21336 | Vulns checked | APK | Sources | Delete |
| com.clearmaster.security | com.clearmaster.security | 2.6.9 | Vulns checked | APK | Sources | Delete |
| com.antivirus | com.antivirus | 4.4.1.1 | Vulns checked | APK | Sources | Delete |
| com.lookout | com.lookout | 9.24-6a6396e | Vulns checked | APK | Sources | Delete |
| net.hideman | net.hideman | 4.4 | Vulns checked | APK | Sources | Delete |

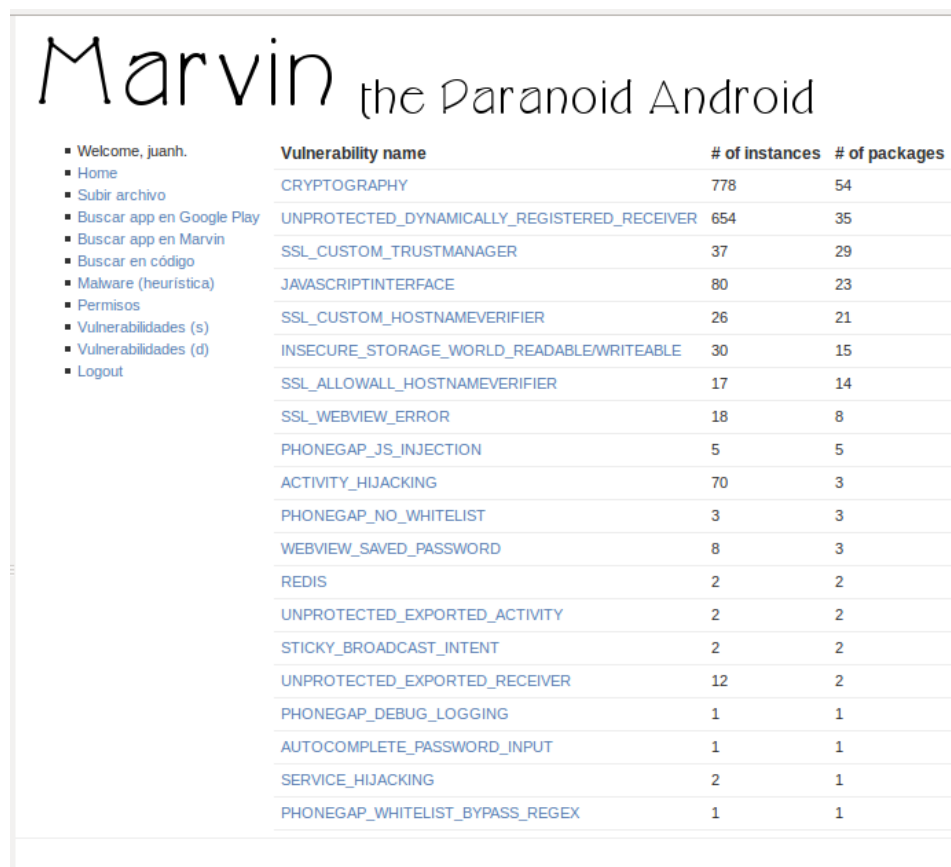
Page 1 of 5. next

Figura 14: Aplicaciones que solicitan un permiso dado

3.6. Vulnerabilidades

En esta sección, podemos ver las vulnerabilidades que Marvin conoce y puede detectar, tanto estática como dinámicamente. Algunas de las vulnerabilidades que encuentra mediante el análisis estático pueden ser verificadas mediante análisis dinámico, y otras se buscan directamente mediante el análisis dinámico. Para cada uno de los tipos de vulnerabilidades, Marvin

muestra una lista ordenada por la cantidad de aplicaciones en donde se encontró la vulnerabilidad (Ver Figura 15). Si clickeamos en el nombre de la vulnerabilidad, Marvin nos muestra una lista de aplicaciones en donde ésta se encontró (ver Figura 16).



The screenshot shows the Marvin application interface. At the top, it says "Marvin the Paranoid Android". On the left, there is a sidebar menu with the following items: Welcome, juanh., Home, Subir archivo, Buscar app en Google Play, Buscar app en Marvin, Buscar en código, Malware (heurística), Permisos, Vulnerabilidades (s), Vulnerabilidades (d), and Logout. The main content area displays a table of vulnerabilities, sorted by the number of instances. The table has three columns: Vulnerability name, # of instances, and # of packages.

| Vulnerability name | # of instances | # of packages |
|---|----------------|---------------|
| CRYPTOGRAPHY | 778 | 54 |
| UNPROTECTED_DYNAMICALLY_REGISTERED_RECEIVER | 654 | 35 |
| SSL_CUSTOM_TRUSTMANAGER | 37 | 29 |
| JAVASCRIPTINTERFACE | 80 | 23 |
| SSL_CUSTOM_HOSTNAMEVERIFIER | 26 | 21 |
| INSECURE_STORAGE_WORLD_READABLEWRITEABLE | 30 | 15 |
| SSL_ALLOWALL_HOSTNAMEVERIFIER | 17 | 14 |
| SSL_WEBVIEW_ERROR | 18 | 8 |
| PHONEGAP_JS_INJECTION | 5 | 5 |
| ACTIVITY_HIJACKING | 70 | 3 |
| PHONEGAP_NO_WHITELIST | 3 | 3 |
| WEBVIEW_SAVED_PASSWORD | 8 | 3 |
| REDIS | 2 | 2 |
| UNPROTECTED_EXPORTED_ACTIVITY | 2 | 2 |
| STICKY_BROADCAST_INTENT | 2 | 2 |
| UNPROTECTED_EXPORTED_RECEIVER | 12 | 2 |
| PHONEGAP_DEBUG_LOGGING | 1 | 1 |
| AUTOCOMPLETE_PASSWORD_INPUT | 1 | 1 |
| SERVICE_HIJACKING | 2 | 1 |
| PHONEGAP_WHITELIST_BYPASS_REGEX | 1 | 1 |

Figura 15: Lista de vulnerabilidades conocidas por Marvin

Marvin the Paranoid Android

| <div><div>Welcome, juanh.</div><div><div>Home</div><div>Subir archivo</div><div>Buscar app en Google Play</div><div>Buscar app en Marvin</div><div>Buscar en código</div><div>Malware (heurística)</div><div>Permisos</div><div>Vulnerabilidades (s)</div><div>Vulnerabilidades (d)</div><div>Logout</div></div></div> | <table><tr><th>Nombre aplicación</th><th>Nombre paquete</th><th>Versión</th><th>Status</th><th>Malware</th><th>Confianza</th><th>Vulns</th></tr><tr><td>BA Como Llego</td><td>ar.gob.buenosaires.comollego</td><td>1</td><td>Vulns checked</td><td>False</td><td>0.992</td><td>10</td></tr><tr><td>AFIP Móvil</td><td>com.afip.mobile</td><td>3</td><td>Vulns checked</td><td>False</td><td>0.978</td><td>14</td></tr><tr><td>edenor 2.0</td><td>com.edenor.mobile.android</td><td>1.9.2</td><td>Vulns checked</td><td>True</td><td>0.557</td><td>34</td></tr><tr><td>BA 147</td><td>ar.gob.buenosaires.reclamos</td><td>1.4</td><td>Vulns checked</td><td>False</td><td>0.982</td><td>11</td></tr><tr><td>Fiscalizando Argentina</td><td>org.fiscalizando</td><td>2.0.19</td><td>Vulns checked</td><td>False</td><td>0.997</td><td>35</td></tr></table> <div>Página 1 de 1.</div> | Nombre aplicación | Nombre paquete | Versión | Status | Malware | Confianza | Vulns | BA Como Llego | ar.gob.buenosaires.comollego | 1 | Vulns checked | False | 0.992 | 10 | AFIP Móvil | com.afip.mobile | 3 | Vulns checked | False | 0.978 | 14 | edenor 2.0 | com.edenor.mobile.android | 1.9.2 | Vulns checked | True | 0.557 | 34 | BA 147 | ar.gob.buenosaires.reclamos | 1.4 | Vulns checked | False | 0.982 | 11 | Fiscalizando Argentina | org.fiscalizando | 2.0.19 | Vulns checked | False | 0.997 | 35 |
|--|--|-------------------|----------------|---------|-----------|---------|-----------|-------|---------------|------------------------------|---|---------------|-------|-------|----|------------|-----------------|---|---------------|-------|-------|----|------------|---------------------------|-------|---------------|------|-------|----|--------|-----------------------------|-----|---------------|-------|-------|----|------------------------|------------------|--------|---------------|-------|-------|----|
| Nombre aplicación | Nombre paquete | Versión | Status | Malware | Confianza | Vulns | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| BA Como Llego | ar.gob.buenosaires.comollego | 1 | Vulns checked | False | 0.992 | 10 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| AFIP Móvil | com.afip.mobile | 3 | Vulns checked | False | 0.978 | 14 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| edenor 2.0 | com.edenor.mobile.android | 1.9.2 | Vulns checked | True | 0.557 | 34 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| BA 147 | ar.gob.buenosaires.reclamos | 1.4 | Vulns checked | False | 0.982 | 11 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Fiscalizando Argentina | org.fiscalizando | 2.0.19 | Vulns checked | False | 0.997 | 35 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Figura 16: Lista de aplicaciones con una vulnerabilidad determinada

4. Administración

En la sección de Administración se manejan las cuentas de usuario de Marvin y la cuenta de acceso al Play Store. Se accede a esta sección por `http://{url_marvin}/admin`.

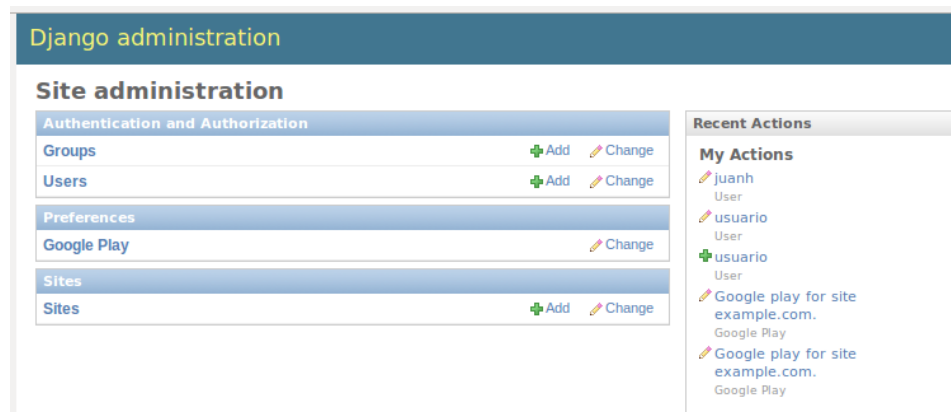


Figura 17: Sección de administración

4.1. Cuentas de usuario

Clickeando en “Users” ingresamos a la administración de usuarios:

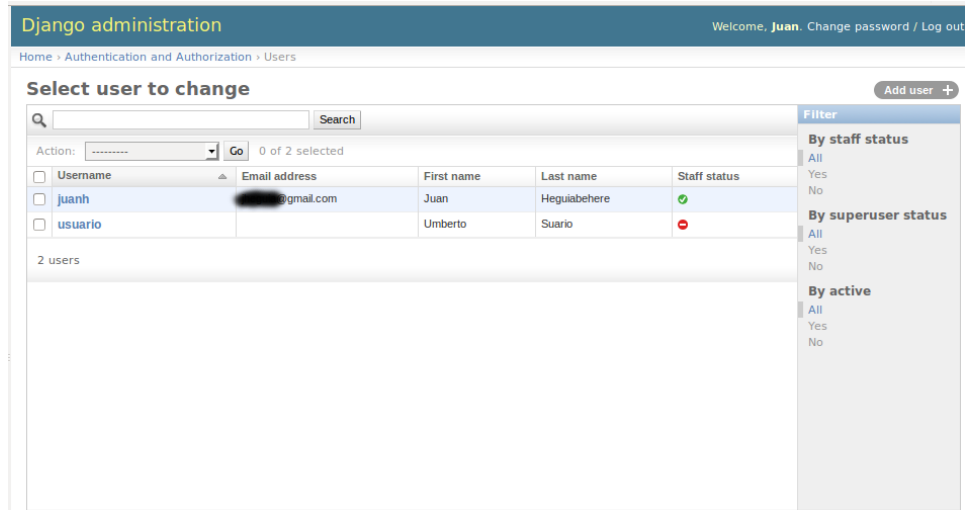


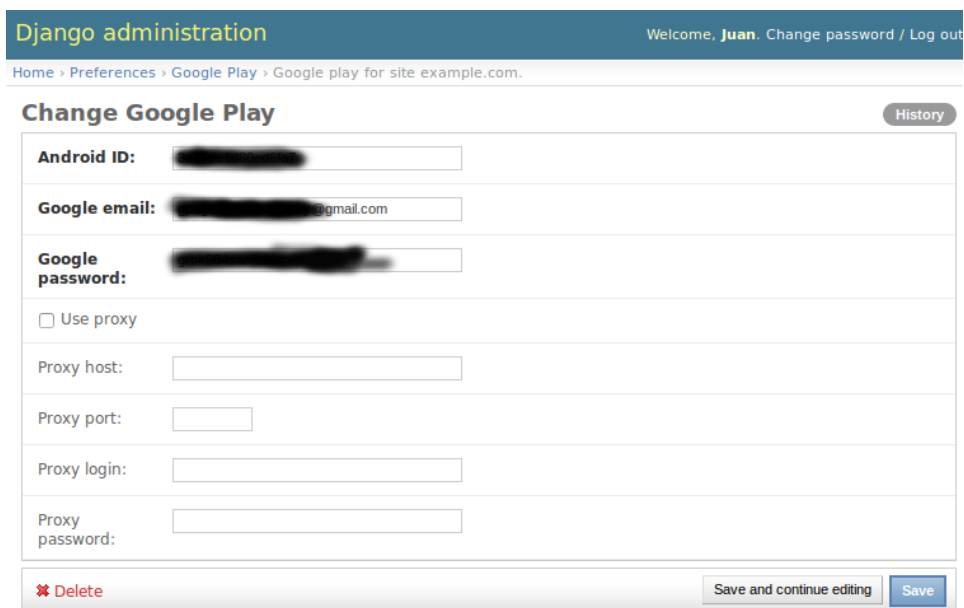
Figura 18: Sección de administración - Usuarios

En esta sección se pueden dar de alta o baja cuentas, necesarias para modificar el estado de una aplicación en Marvin (léase dar de alta aplicaciones desde Google Play o archivo, borrar aplicaciones). De momento todos los usuarios no-administradores tienen permisos completos sobre todo el repositorio.

El alta de un usuario es trivial:

Figura 19: Sección de administración - Alta de usuario

4.2. Cuenta de Google Play



The screenshot shows the Django administration interface for managing Google Play account settings. The header includes the Django logo and the text 'Django administration'. The user is logged in as 'Juan' and can click on 'Welcome, Juan.', 'Change password', or 'Log out'. The breadcrumb trail is 'Home > Preferences > Google Play > Google play for site example.com.'. The main heading is 'Change Google Play', with a 'History' button to its right. The form contains several fields: 'Android ID' (redacted), 'Google email' (redacted, with '@gmail.com' visible), 'Google password' (redacted), a checkbox for 'Use proxy' (unchecked), 'Proxy host' (empty), 'Proxy port' (empty), 'Proxy login' (empty), and 'Proxy password' (empty). At the bottom, there is a red 'Delete' button with a trash icon, and two buttons: 'Save and continue editing' and 'Save'.

Figura 20: Sección de administración - Usuario Google Play

La sección de Cuenta de Google Play nos permite ingresar los datos de una cuenta habilitada para acceder al Play Store. Para habilitar una cuenta de Google ya existente, se puede utilizar el programa `android-checkin` de Nicolas Viennot: <https://github.com/nviennot/android-checkin>, o por supuesto haber usado esa cuenta en un teléfono Android.