Marvin User's Guide

Juan Heguiabehere

1 Who, Why, What, When (Introduction)

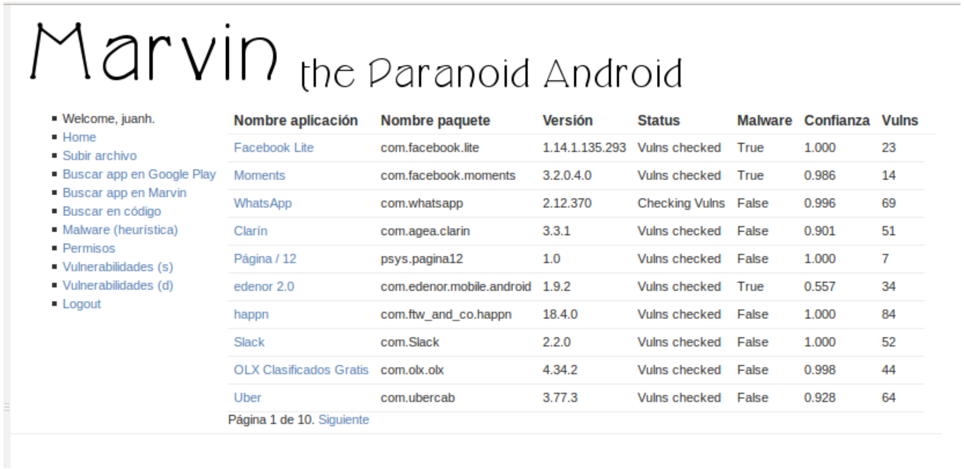
Marvin is a platform for analysis and tracking of Android applications. It can pick up apps from either .apk files or the Google Play Store, performs static and dynamic analysis on them, and keeps track of different versions on a GitLab instance. The main components of Marvin are:

- `marvin-frontend`: Takes care of the user interface, decompilation of apps, and interaction with databases, repositories and `marvin-static-analyzer`.
- `marvin-static-analyzer`: Looks for specific vulnerability types in an application.
- `marvin-dynamic-analyzer`: Takes care of running dynamic tests, some of them based on hints from `marvin-static-analyzer`, to see if it can trigger vulnerabilities.

In principle, `marvin-static-analyzer` and `marvin-dynamic-analyzer` run unassisted, so this is basically a use guide for `marvin-frontend`.

Marvin was developed by Juan Heguiabehere and Joaquín Rinaudo of the STIC team of Fundación Manuel Sadosky: `http://www.fundacionsadosky.org.ar/programas/seguridad-en-tic/`.

2 Home Screen



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

Figure 1: Marvin Home Screen

Marvin's Home Screen is split in two: to the left is the actions menu (which is always there) and to the right is a list of the last 10 uploaded apps. From left to right the list shows:

- The app's "fantasy" name.
- The app's package name, which functions as its identifier in the Google Play Store.
- The app's version number.
- App's process status (usually 'queued', 'checking vulns' or 'vulns checked').
- Whether the permissions heuristics determined that the app could be malware and with how much confidence.
- The number of potential vulnerabilities found for the app.

Clicking on the fantasy name brings us to the app's Information page. See Section 3.1.

3 Actions menu

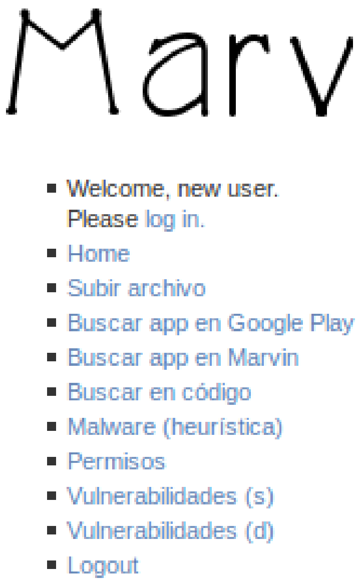


Figure 2: Actions menu

Actions menu is where all of Marvin's activities are started. From top to bottom, these are:

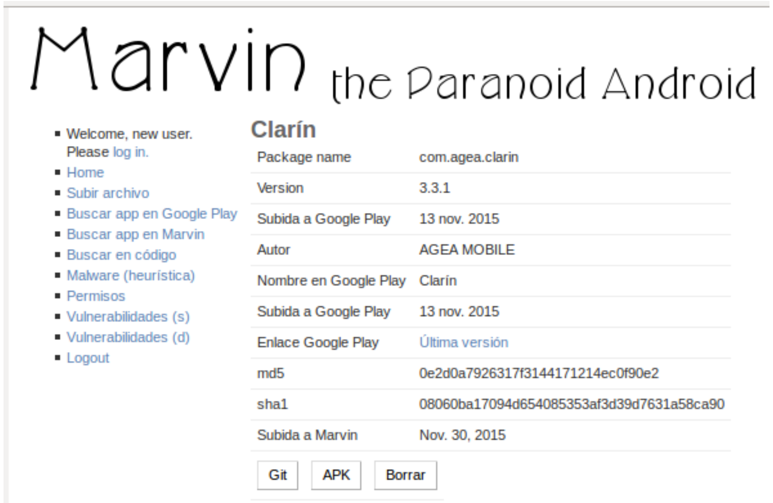
- Login (some actions require being logged in)
- Go to Home page.
- Upload a file: It allows uploading of `.apk` files.
- Search the Play Store: It allows searching and downloading of apps from the Google Play Store.
- Search Marvin: You can search for apps alredy uploaded, by app name or by package name.
- Search in the code: You can search the code for specific strings, such as library, class, or method names.

- Malware (heuristics): It gives an ordered list of apps for which the permissions list gave the impression that it could be malware, ordered by how strong the impression was.
- Permissions: Gives a list of the permissions Marvin found, together with the number of apps requesting each one.
- Vulnerabilities(s): Gives a list of the vulnerabilities that Marvin seeks via static analysis, ordered by the number of found instances.
- Vulnerabilities(d): Gives a list of the vulnerabilities that Marvin seeks via dynamic analysis, ordered by the number of found instances.
- Logout

3.1 App information

In any application list, clicking the name of the app brings us to the app information page. This page has three sections:

- Metadata and repository access
- Heuristics, permissions and components
- Vulnerabilities

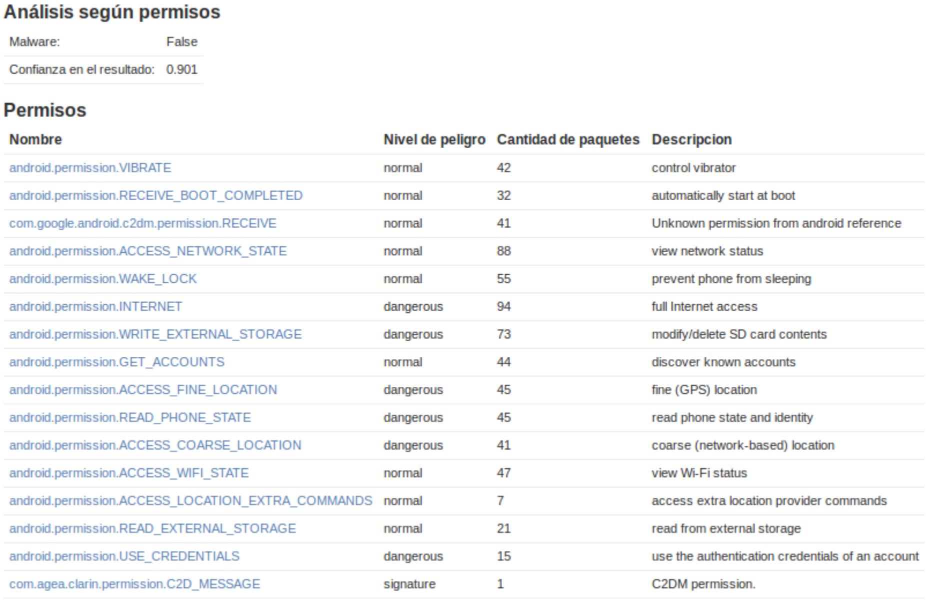


Clarín

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

Figure 3: Metadata and repository access

In the metadata and repository access section we can see data such as the date an app was uploaded to Google Play, its version number, or the app file checksums, as well as access the Git repository for the app, the APK file itself, or the Google Play page for it (although in this case we are brought to the page for the last uploaded version). We can also delete an app from Marvin here.



Análisis según permisos

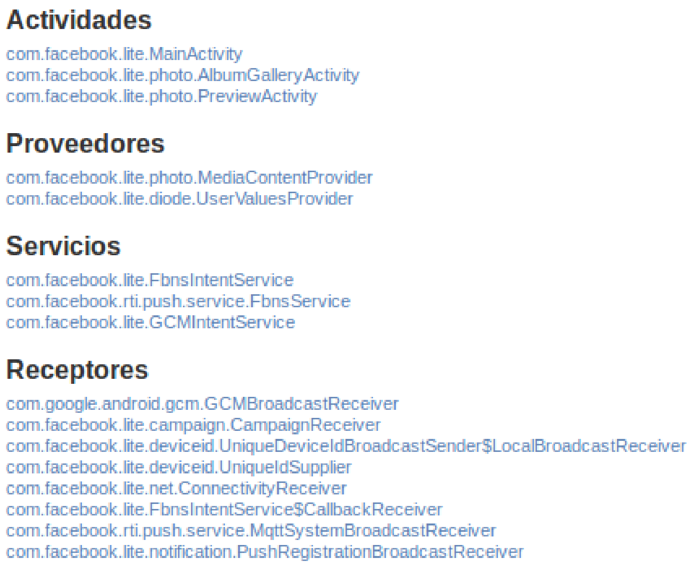
Malware:	False
Confianza en el resultado:	0.901

Permisos

Nombre	Nivel de peligro	Cantidad de paquetes	Descripcion
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.

Figure 4: Heuristics and permissions

The heuristics and permissions section shows the result of the Bayesian analysis of the permissions requested by the app, as well as the list of said permissions. The permissions list gives for each permission its name, its danger level, the number of packages that request it, and a succint description of what granting it implies. Clicking on a permission name brings us to a page with stats for the permission (see Section 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

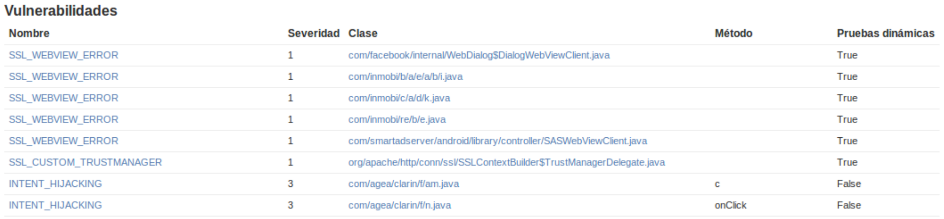
com.facebook.lite.FbnsIntentService
com.facebook.rti.push.service.FbnsService
com.facebook.lite.GCMIntentService

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

Figure 5: Components section

The components section shows us the activities, providers, services and event receivers of an application. If the decompilation process has finished, clicking on any of these will bring up a new browser tab with the GitLab page for its source code.



Vulnerabilidades

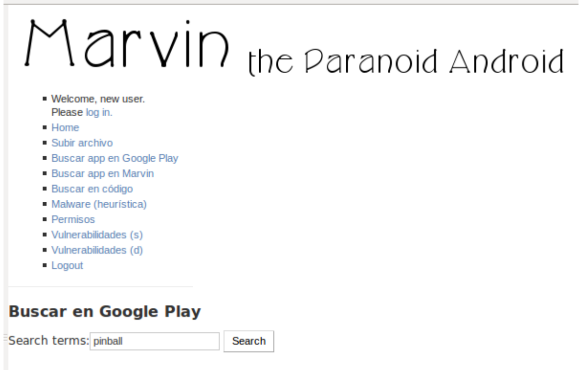
Nombre	Severidad	Clase	Método	Pruebas dinámicas
SSL_WEBVIEW_ERROR	1	com/facebook/internal/WebDialog$DialogWebViewClient.java		True
SSL_WEBVIEW_ERROR	1	com/inmobi/b/a/e/a/b/i.java		True
SSL_WEBVIEW_ERROR	1	com/inmobi/c/a/d/k.java		True
SSL_WEBVIEW_ERROR	1	com/inmobi/re/b/e.java		True
SSL_WEBVIEW_ERROR	1	com/smartadserver/android/library/controller/SASWebViewClient.java		True
SSL_CUSTOM_TRUSTMANAGER	1	org/apache/http/conn/ssl/SSLContextBuilder$TrustManagerDelegate.java		True
INTENT_HIJACKING	3	com/agea/clarin/f/am.java	c	False
INTENT_HIJACKING	3	com/agea/clarin/f/n.java	onClick	False

Figure 6: Vulnerabilities

The Vulnerabilities section shows us a list of the vulnerabilities found by `marvin-static-analyzer`; for each vulnerability found, we can see its type, its severity, the class where it was found, the method if applicable, and whether it can be verified by dynamic analysis. Clicking on the vulnerability type gives us information about the type, while clicking on the class name brings up a new tab with the GitLab page for its source code.

3.2 Search the Google Play Store

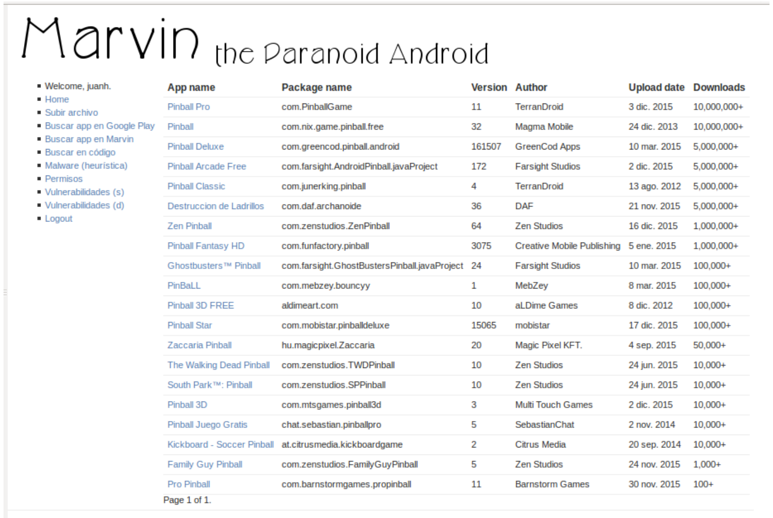
Marvin can search and download apps from Google Play Store. For this, select “Search Google Play” in the Actions menu, enter the search terms, and press Enter.



Buscar en Google Play

Search terms: pinball

Figure 7: Google Play Search - Search terms



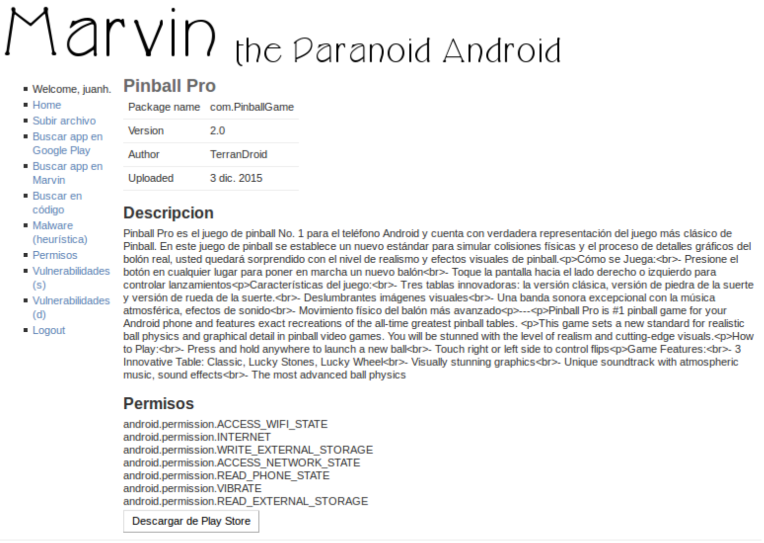
App name	Package name	Version	Author	Upload date	Downloads
Pinball Pro	com.PinballGame	11	TerranDroid	3 dic. 2015	10,000,000+
Pinball	com.nix.game.pinball.free	32	Magma Mobile	24 dic. 2013	10,000,000+
Pinball Deluxe	com.greencod.pinball.android	161507	GreenCod Apps	10 mar. 2015	5,000,000+
Pinball Arcade Free	com.farsight.AndroidPinball.javaProject	172	Farsight Studios	2 dic. 2015	5,000,000+
Pinball Classic	com.junerking.pinball	4	TerranDroid	13 ago. 2012	5,000,000+
Destruccion 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	com.mebzey.bouncyy	1	MebZey	8 mar. 2015	100,000+
Pinball 3D FREE	aldimeart.com	10	aLDime 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.mtsgames.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.

Figure 8: Google Play Search - Results

The results page is as seen in Figure 8: it has some basic data for each app, plus the upload date to Google Play and the number of downloads. If we click on any of the apps, we are brought to a page like the one in Figure 9, where some more information is shown such as the description and the permissions it requests, and finally there's a button for downloading the app to Marvin and starting analysis.

The analysis: First the app is decompiled, then static analysis is performed on it. Nevertheless, uploading of sources to the repositories takes a long time, so it's common for the results of static analysis (and with them links to the sources in the App info page) to be there before the Gitlab page for them is ready.



Marvin the Paranoid Android

Pinball Pro

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

Descripcion

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 bolón real, usted quedará sorprendido con el nivel de realismo y efectos visuales de pinball.<p>Cómo 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>---<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

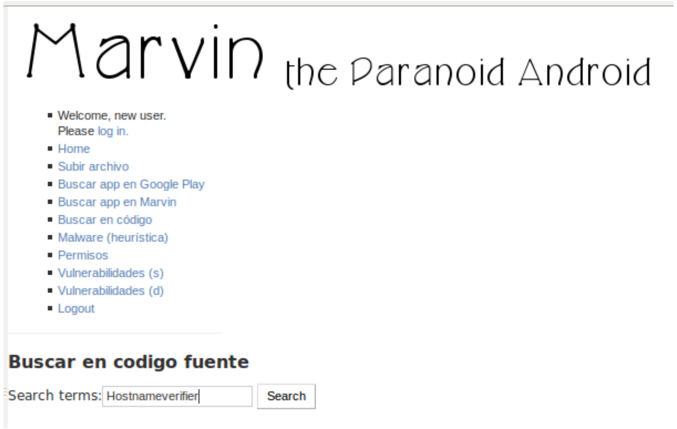
Permisos

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

Figure 9: Google Play Search- Description

3.3 Code Search

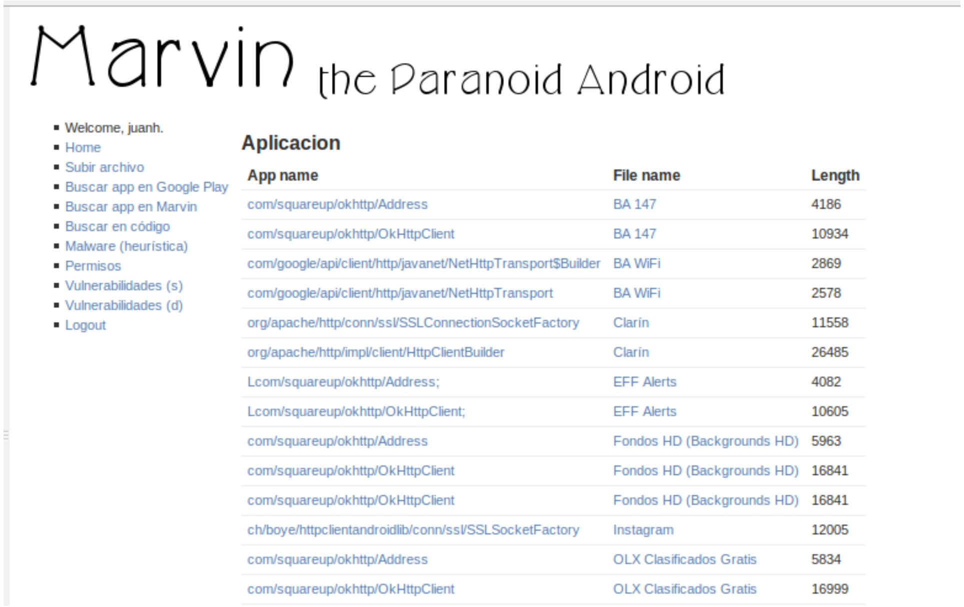
The "Search Code" option allows us to search for specific strings in the code, for example to search for use of specific libraries or Android services. After writing the search terms and pressing Enter, the results will show as in Figure 11: for each match, there's the class name, the app it belongs to, and the length of the source file. Clicking on the file name brings us to the GitLab page for its source code.



Buscar en codigo fuente

Search terms: Hostnameverifier

Figure 10: Code search



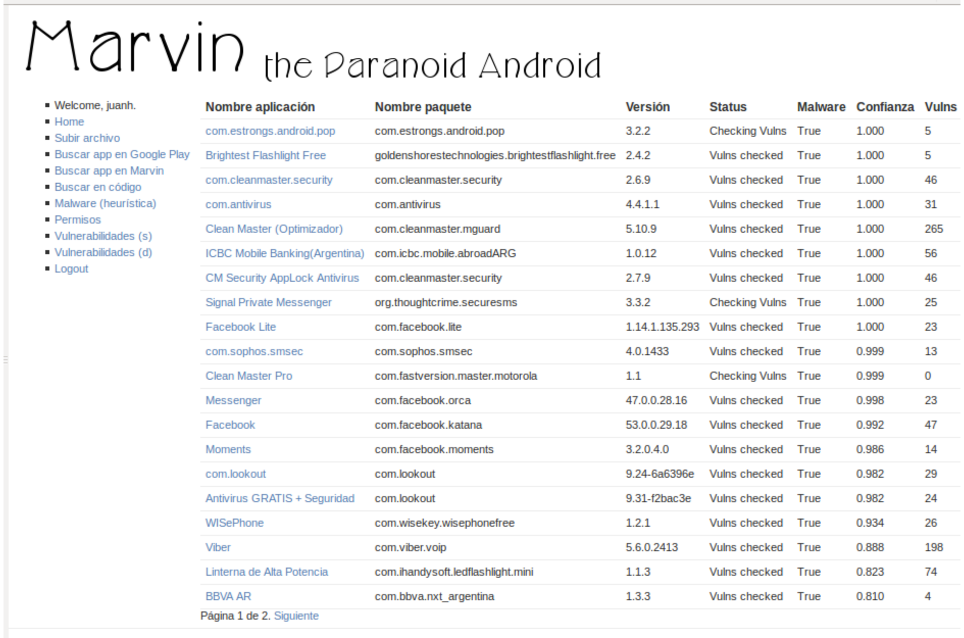
Aplicacion

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/NetHttpTransport$Builder	BA WiFi	2869
com/google/api/client/http/javanet/NetHttpTransport	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

Figure 11: Code search - Results

3.4 Malware (heuristics)

This option shows an ordered list of the apps that according to the heuristics are most likely to be malware. Together with version information, we can see a score that marks the confidence in the result, and the amount of vulnerabilities Marvin found in the app.



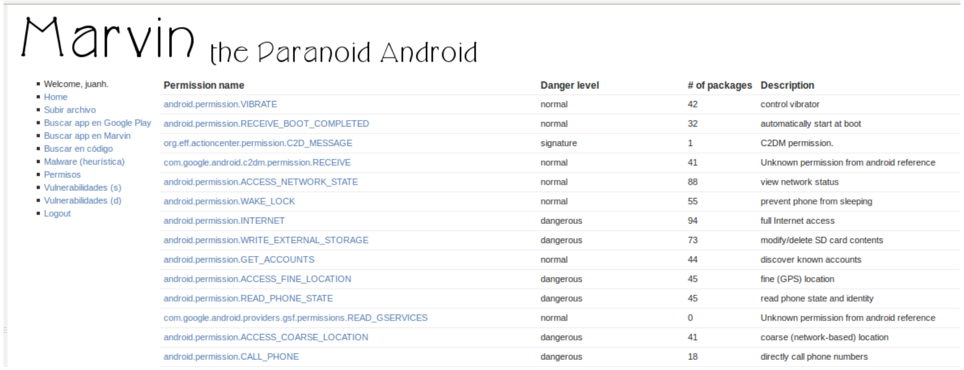
Nombre aplicación	Nombre paquete	Versión	Status	Malware	Confianza	Vulns
com.estrongs.android.pop	com.estrongs.android.pop	3.2.2	Checking Vulns	True	1.000	5
Brightest Flashlight Free	goldenshorestechnologies.brightestflashlight.free	2.4.2	Vulns checked	True	1.000	5
com.cleanmaster.security	com.cleanmaster.security	2.6.9	Vulns checked	True	1.000	46
com.antivirus	com.antivirus	4.4.1.1	Vulns checked	True	1.000	31
Clean Master (Optimizador)	com.cleanmaster.mguard	5.10.9	Vulns checked	True	1.000	265
ICBC Mobile Banking(Argentina)	com.icbc.mobile.abroadARG	1.0.12	Vulns checked	True	1.000	56
CM Security AppLock Antivirus	com.cleanmaster.security	2.7.9	Vulns checked	True	1.000	46
Signal Private Messenger	org.thoughtcrime.securesms	3.3.2	Checking Vulns	True	1.000	25
Facebook Lite	com.facebook.lite	1.14.1.135.293	Vulns checked	True	1.000	23
com.sophos.smsec	com.sophos.smsec	4.0.1433	Vulns checked	True	0.999	13
Clean Master Pro	com.fastversion.master.motorola	1.1	Checking Vulns	True	0.999	0
Messenger	com.facebook.orca	47.0.0.28.16	Vulns checked	True	0.998	23
Facebook	com.facebook.katana	53.0.0.29.18	Vulns checked	True	0.992	47
Moments	com.facebook.moments	3.2.0.4.0	Vulns checked	True	0.986	14
com.lookout	com.lookout	9.24-6a6396e	Vulns checked	True	0.982	29
Antivirus GRATIS + Seguridad	com.lookout	9.31-f2bac3e	Vulns checked	True	0.982	24
WISePhone	com.wisekey.wisephonefree	1.2.1	Vulns checked	True	0.934	26
Viber	com.viber.voip	5.6.0.2413	Vulns checked	True	0.888	198
Linterna de Alta Potencia	com.ihandysoft.ledflashlight.mini	1.1.3	Vulns checked	True	0.823	74
BBVA AR	com.bbva.nxt_argentina	1.3.3	Vulns checked	True	0.810	4

Página 1 de 2. Siguiente

Figure 12: Malware according to the permissions heuristics

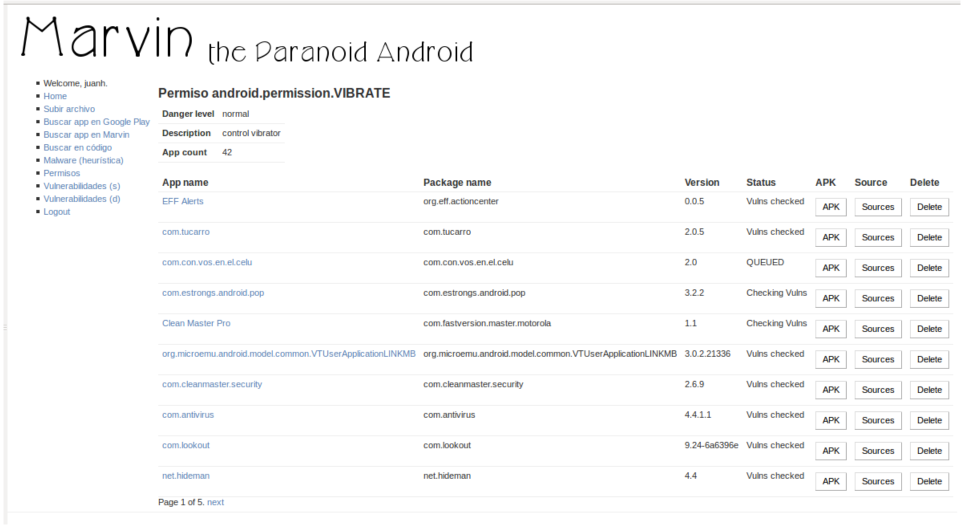
3.5 Permissions

This option shows us the permissions seen by Marvin among all the applications, together with their respective descriptions, danger levels and the number of applications that request them (see Figure 13). Clicking on a permission's name brings us to a page with the list of applications that request it (see Figure 14).



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.C2D_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

Figure 13: Permissions seen by Marvin



Permiso android.permission.VIBRATE

Danger level	normal
Description	control vibrator
App count	42

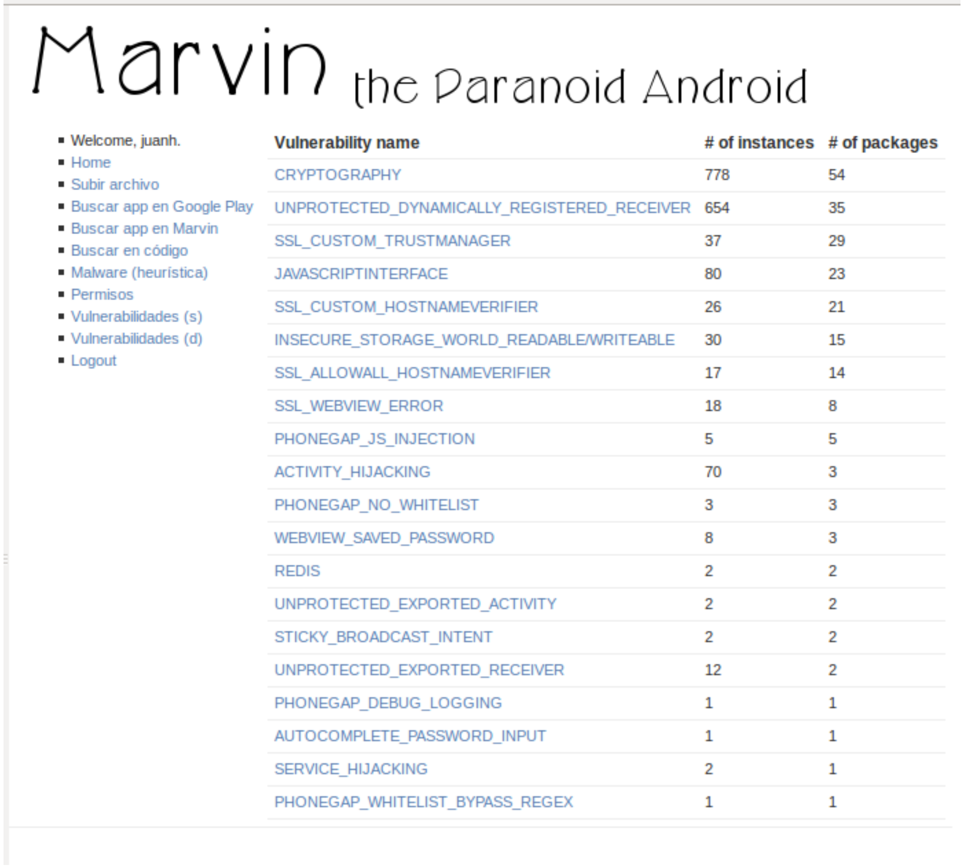
App name	Package name	Version	Status	APK	Source	Delete
EFF Alerts	org.eff.actioncenter	0.0.5	Vulns checked	APK	Sources	Delete
com.tucarro	com.tucarro	2.0.5	Vulns checked	APK	Sources	Delete
com.con.vos.en.el.celu	com.con.vos.en.el.celu	2.0	QUEUED	APK	Sources	Delete
com.estrongs.android.pop	com.estrongs.android.pop	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.cleanmaster.security	com.cleanmaster.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

Figure 14: Apps requesting a given permission

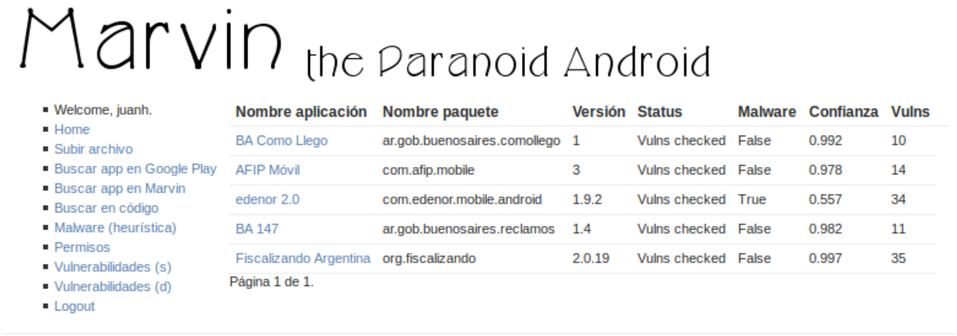
3.6 Vulnerabilities

In this section we can see the vulnerability types that Marvin knows about and can find, statically as well as dynamically. Some of the vulnerabilities it finds via static analysis can be verified by dynamic analysis, and some are directly searched for via dynamic analysis. For each vulnerability type, Marvin shows a list ordered by the number of applications where it is found (see Figure 15). If we click on the vulnerability type name, Marvin shows us the list of apps where it was found (see Figure 16).



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_READABLE/WRITEABLE	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

Figure 15: List of vulnerability types known to 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

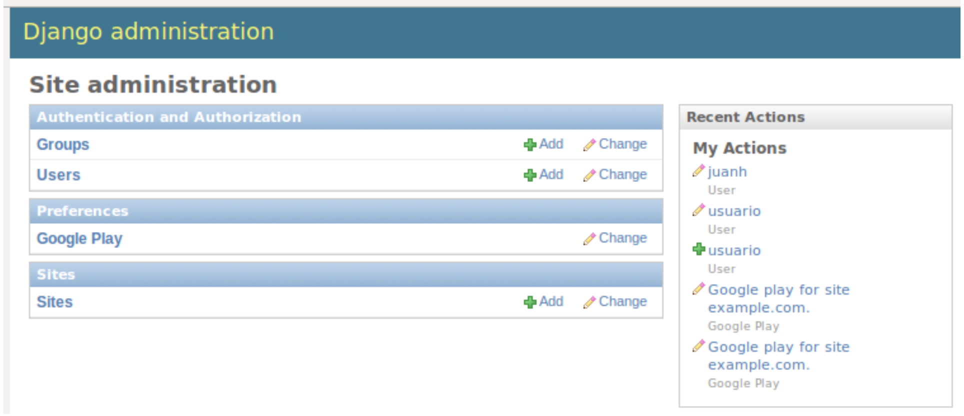
Nombre aplicación	Nombre paquete	Versión	Status	Malware	Confianza	Vulns
BA Como Llego	ar.gob.buenosaires.comollego	1	Vulns checked	False	0.992	10
AFIP Móvil	com.afip.mobile	3	Vulns checked	False	0.978	14
edenor 2.0	com.edenor.mobile.android	1.9.2	Vulns checked	True	0.557	34
BA 147	ar.gob.buenosaires.reclamos	1.4	Vulns checked	False	0.982	11
Fiscalizando Argentina	org.fiscalizando	2.0.19	Vulns checked	False	0.997	35

Página 1 de 1.

Figure 16: List of apps with a given vulnerability

4 Administration

In the Administration section we can manage user accounts for Marvin and the access data for the Play Store. This section can be accessed at `http://url_marvin/admin`.



Django administration

Site administration

Authentication and Authorization

Groups ✚Add ✎Change

Users ✚Add ✎Change

Preferences

Google Play ✎Change

Sites

Sites ✚Add ✎Change

Recent Actions

My Actions

✎juanh
User

✎usuario
User

✚usuario
User

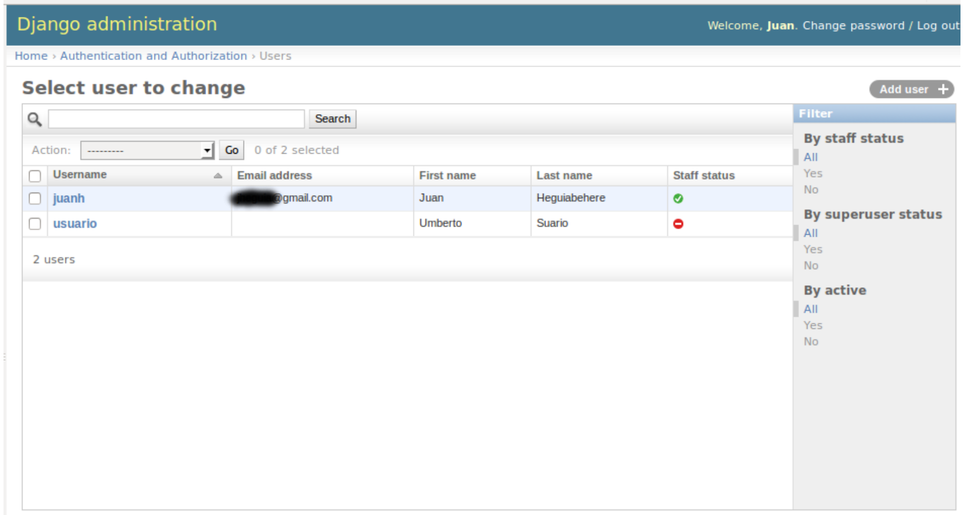
✎Google play for site example.com.
Google Play

✎Google play for site example.com.
Google Play

Figure 17: Administration

4.1 User accounts

Clicking 'Users' we enter the Marvin user administration proper:



Django administration

Welcome, **Juan**. Change password / Log out

Home › Authentication and Authorization › Users

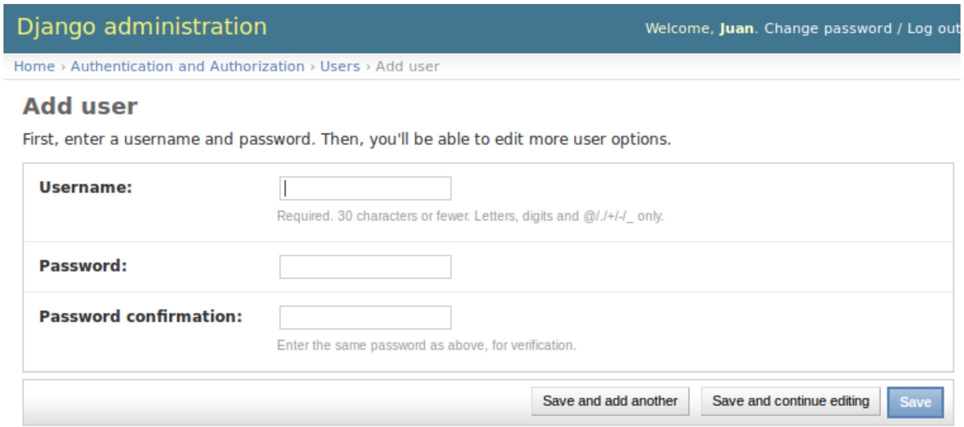
Select user to change

□	Username	Email address	First name	Last name	Staff status
□	juanh	[redacted]@gmail.com	Juan	Heguiabehere	✓
□	usuario		Umberto	Suario	⊖

2 users

Figure 18: Administration - Users

In this section we can create, update and delete Marvin user accounts (so far all users have the same access to all data, but still we want to make sure only logged in users can do some things). User management is straightforward:



Django administration

Welcome, **Juan**. Change password / Log out

Home › Authentication and Authorization › Users › Add user

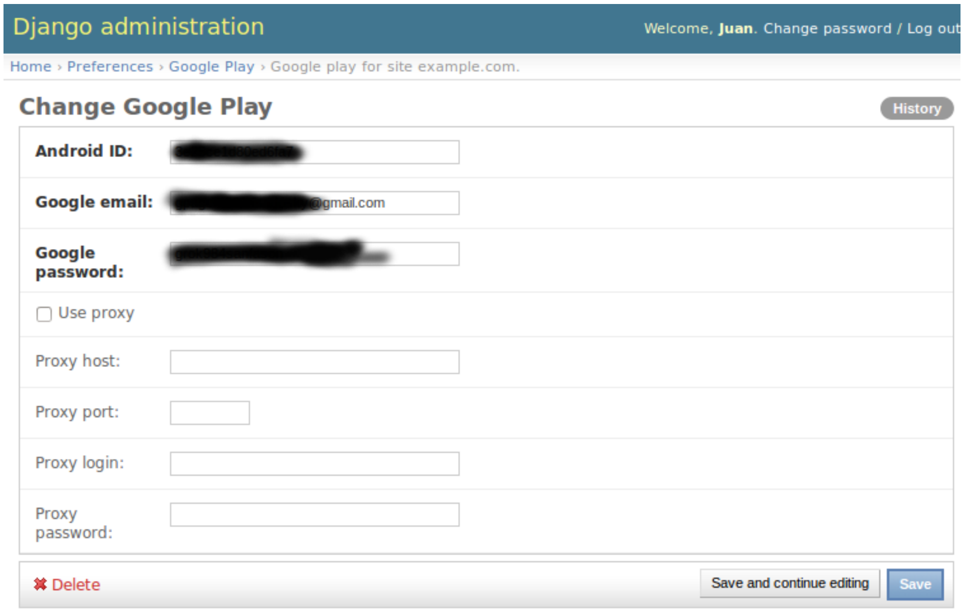
Add user

First, enter a username and password. Then, you'll be able to edit more user options.

Username:	Required. 30 characters or fewer. Letters, digits and @/./+/-/_ only.
Password:	
Password confirmation:	Enter the same password as above, for verification.

Figure 19: Administration - New User

4.2 Google Play account


Django administration
Welcome, Juan. Change password / Log out
Home › Preferences › Google Play › Google play for site example.com.
History
✖ Delete
Save and continue editing
Save

Change Google Play

Android ID: [redacted]

Google email: [redacted]@gmail.com

Google password: [redacted]

□ Use proxy

Proxy host:

Proxy port:

Proxy login:

Proxy password:

Figure 20: Administration - Google Play account

The Google Play section lets us input the credentials of a Gmail account to access the Play Store. Of course, such account should be 'checked in' the Play Store. This can be an account used on a phone, or (better) one checked in via the `android-checkin` program, written by Nicolas Viennot: `https://github.com/nviennot/android-checkin`