ANDROID STATIC ANALYSIS REPORT

Pretend You're Xyzzy (3.0.0)

File Name:	installer297.apk
Package Name:	com.gianlu.pretendyourexyzzy
Scan Date:	May 31, 2022, 1:21 p.m.
App Security Score:	46/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	5	1	1	1

FILE INFORMATION

File Name: installer297.apk
Size: 3.2MB
MD5: 781af1f3ee4469192921b7acea23fcb9
SHA1: 0c6cb22cbb0ad9ec9bba54441efd6e3bb5b86f6b
SHA256: 67215384e04a56de23cc1d1fcbc96b2a0256e8abf6406c86cbd9869166d4a420

APP INFORMATION

App Name: Pretend You're Xyzzy
Package Name: com.gianlu.pretendyourexyzzy
Main Activity: com.gianlu.pretendyourexyzzy.LoadingActivity
Target SDK: 29
Min SDK: 21
Max SDK:
Android Version Name: 3.0.0
Android Version Code: 85

APP COMPONENTS

Activities: 12
Services: 0
Receivers: 0
Providers: 2
Exported Activities: 0
Exported Services: 0
Exported Receivers: 0
Exported Providers: 0

CERTIFICATE INFORMATION

```
APK is signed
v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2018-11-06 09:14:27+00:00
Valid To: 2046-03-24 09:14:27+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x239dc5a9
Hash Algorithm: sha256
md5: 470cee3d3f32da6e7c47182e4653a050
sha1: 2f3cc8683dfc7fcf38ce51699ece81af176f8887
sha256: 3c64db10a8348c0052e7423c2cbfdeebe3fc778f47b84223dff4c0b46a146076
sha512: f88fb0b06d55c41cf053c8761fd8875c285cd8af4e21b3629d427c2589f383b12d54d43b6aae59a5c39ff85c05a0a833fe8168a4f3b62d4c8e8bed930f521790
```

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

TITLE	SEVERITY	DESCRIPTION
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.android.vending.BILLING	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td><table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8</td></tr>
</table></td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.gianlu.pretendyourexyzzy.LoadingActivity	Schemes: http://, https://, Hosts: *.pretendyoure.xyz,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high	The app intends to use cleartext network traffic, such as cleartext HTTP, FTP stacks, DownloadManager, and MediaPlayer. The default value for apps that target API level 27 or lower is "true". Apps that target API level 28 or higher default to "false". The key reason for avoiding cleartext traffic is the lack of confidentiality, authenticity, and protections against tampering; a network attacker can eavesdrop on transmitted data and also modify it without being detected.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	com/gianlu/pretendyourexyzzy/cards/GameRoundSummary.java com/gianlu/pretendyourexyzzy/adapters/CardcastDecksAdapter.java com/gianlu/commonutils/CommonUtils.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/bumptech/glide/load/engine/DataCacheKey.java com/bumptech/glide/load/Option.java com/bumptech/glide/load/engine/ResourceCacheKey.java com/bumptech/glide/load/engine/EngineResource.java
				com/bumptech/glide/load/resource/bitmap/TransformationUtils.java com/bumptech/glide/load/engine/bitmap_recycle/LruArrayPool.java com/bumptech/glide/manager/RequestManagerRetriever.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/bumptech/glide/manager/RequestManagerFragment.java com/bumptech/glide/load/engine/bitmap_recycle/LruBitmapPool.java com/github/paolorotolo/appintro/AppIntroBase.java com/bumptech/glide/gifdecoder/StandardGifDecoder.java com/bumptech/glide/manager/SupportRequestManagerFragment.java com/bumptech/glide/request/SingleRequest.java com/bumptech/glide/load/engine/SourceGenerator.java com/bumptech/glide/load/engine/DecodePath.java com/bumptech/glide/load/resource/ImageDecoderResourceDecoder.java com/bumptech/glide/load/resource/bitmap/DrawableToBitmapConverter.java com/bumptech/glide/load/resource/gif/GifDrawableEncoder.java com/bumptech/glide/load/resource/bitmap/BitmapImageDecoderResourceDecoder.java com/bumptech/glide/load/engine/executor/GlideExecutor.java com/bumptech/glide/manager/RequestTracker.java com/bumptech/glide/load/engine/cache/DiskLruCacheWrapper.java com/bumptech/glide/load/resource/bitmap/BitmapEncoder.java com/bumptech/glide/load/model/ByteBufferEncoder.java com/bumptech/glide/gifdecoder/GifHeaderParser.java com/bumptech/glide/load/resource/bitmap/HardwareConfigState.java com/bumptech/glide/manager/DefaultConnectivityMonitor.java com/bumptech/glide/load/model/FileLoader.java com/bumptech/glide/load/model/ResourceLoader.java com/bumptech/glide/load/resource/gif/ByteBufferGifDecoder.java com/bumptech/glide/load/engine/Engine.java com/bumptech/glide/load/model/StreamEncoder.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/bumptech/glide/util/pool/FactoryPools.java com/bumptech/glide/load/resource/bitmap/Downsampler.java com/bumptech/glide/load/resource/bitmap/DefaultImageHeaderParser.java com/bumptech/glide/Glide.java com/gianlu/commonutils/ui/Toaster.java com/bumptech/glide/load/resource/gif/StreamGifDecoder.java com/bumptech/glide/load/data/LocalUriFetcher.java com/bumptech/glide/load/data/AssetPathFetcher.java me/zhanghai/android/materialratingbar/ClipDrawableCompat.java com/bumptech/glide/load/model/ByteBufferFileLoader.java com/bumptech/glide/load/engine/DecodeJob.java com/bumptech/glide/load/data/mediastore/ThumbnailStreamOpener.java com/bumptech/glide/load/engine/GlideException.java com/gianlu/commonutils/logging/Logging.java com/bumptech/glide/load/resource/bitmap/VideoDecoder.java me/zhanghai/android/materialratingbar/MaterialRatingBar.java com/bumptech/glide/load/engine/executor/RuntimeCompat.java com/bumptech/glide/load/engine/cache/MemorySizeCalculator.java com/bumptech/glide/manager/DefaultConnectivityMonitorFactory.java com/bumptech/glide/load/data/mediastore/ThumbFetcher.java com/bumptech/glide/load/data/HttpUrlFetcher.java com/bumptech/glide/request/target/ViewTarget.java com/bumptech/glide/module/ManifestParser.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
4	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/gianlu/pretendyourexyzzy/dialogs/GameRoundDialog.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application invoke platform-provided DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to no sensitive information repositories.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
6	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
7	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
8	FMT_MEC_EXT.1.1	Security Functional Requirements	Supported Configuration Mechanism	The application invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.
9	FTP_DIT_EXT.1.1	Security Functional Requirements	Protection of Data in Transit	The application does encrypt some transmitted data with HTTPS/TLS/SSH between itself and another trusted IT product.
10	FCS_RBG_EXT.2.1,FCS_RBG_EXT.2.2	Selection-Based Security Functional Requirements	Random Bit Generation from Application	The application perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using Hash_DRBG. The deterministic RBG is seeded by an entropy source that accumulates entropy from a platform-based DRBG and a software-based noise source, with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.
11	FCS_COP.1.1(2)	Selection-Based Security Functional Requirements	Cryptographic Operation - Hashing	The application perform cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1/SHA-256/SHA-384/SHA-512 and message digest sizes 160/256/384/512 bits.
12	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
13	FCS_HTTPS_EXT.1.3	Selection-Based Security Functional Requirements	HTTPS Protocol	The application notify the user and not establish the connection or request application authorization to establish the connection if the peer certificate is deemed invalid.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
14	FIA_X509_EXT.2.1	Selection-Based Security Functional Requirements	X.509 Certificate Authentication	The application use X.509v3 certificates as defined by RFC 5280 to support authentication for HTTPS , TLS.

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
api.cardcastgame.com	ok	No Geolocation information available.
play.google.com	ok	**IP:** 142.251.36.46 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
api.urbandictionary.com	ok	**IP:** 142.251.39.115 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.gnu.org	ok	**IP:** 209.51.188.116 **Country:** United States of America **Region:** Massachusetts **City:** Boston **Latitude:** 42.358429 **Longitude:** -71.059769 **View:** Google Map
gianlu.xyz	ok	**IP:** 104.21.74.162 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
www.apache.org	ok	**IP:** 151.101.2.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
pyx-discovery.gianlu.xyz	ok	**IP:** 104.21.74.162 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
github.com	ok	**IP:** 140.82.121.4 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
paolorotolo.github.io	ok	**IP:** 185.199.108.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
altomanigianluca@gmail.com 电邮地址altomanigianluca@gmail.com	Android String Resource

HARDCODED SECRETS

POSSIBLE SECRETS
"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"
"library_appintro_authorWebsite" : "http://paolorotolo.github.io/"

Report Generated by - MobSF v3.5.2 Beta

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.