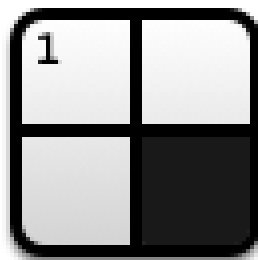




ANDROID STATIC ANALYSIS REPORT



 Shortyz (4.4.0)

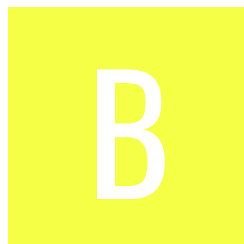
File Name: installer360.apk

Package Name: com.totsp.crossword.shortyz






Scan Date: May 31, 2022, 7:34 a.m.

App Security Score: 40/100 (MEDIUM RISK)

Grade:



FINDINGS SEVERITY

 HIGH	 MEDIUM	 INFO	 SECURE	 HOTSPOT
4	8	1	1	1

FILE INFORMATION

File Name: installer360.apk

Size: 4.91MB

MD5: 4d80ef12787796769349145bcce2969b

SHA1: 447dc2904538e9cd33517b8245bba059b1ea4420

SHA256: 8ed6f6d7c3f3aaf490a74f454eaffbfae68f41b8acf93a94084e42c9a50e9823

APP INFORMATION

App Name: Shortyz

Package Name: com.totsp.crossword.shortyz

Main Activity: com.totsp.crossword.BrowseActivity

Target SDK: 25

Min SDK: 9

Max SDK:

Android Version Name: 4.4.0

Android Version Code: 40400

APP COMPONENTS

Activities: 12
Services: 0
Receivers: 1
Providers: 0
Exported Activities: 4
Exported Services: 0
Exported Receivers: 1
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: 2012-01-08 14:51:45+00:00
Valid To: 2039-05-26 14:51:45+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x4f09ad81
Hash Algorithm: sha1
md5: ada7b23081fa6376c39dbf2d022c36ec
sha1: 9fce777611ac315f8a4a9ccc62b46bc3d025a9f5
sha256: abcd4ab97eca7a3ce7454f2c3a728b91940360d67f63c5822c61e74613cb7589
sha512: 7674b4e6a2816711d1a7a710bac31bbfe0e52ff62da88df86351055396dd6a6efcd21d798005969c71664b147f1f0a00413be488edd94177589a36063f1ef6f1

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.
Certificate algorithm might be vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

≡ APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.MANAGE_ACCOUNTS	dangerous	manage the accounts list	Allows an application to perform operations like adding and removing accounts and deleting their password.
android.permission.USE_CREDENTIALS	dangerous	use the authentication credentials of an account	Allows an application to request authentication tokens.

APKID ANALYSIS

FILE	DETAILS	
classes.dex	FINDINGS	DETAILS
	Anti-VM Code	Build.MANUFACTURER check Build.BOARD check
	Compiler	dx (possible dexmerge)
	Manipulator Found	dexmerge

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.totsp.crossword.HttpDownloadActivity	Schemes: http://, Hosts: *, Path Patterns: /\.*\puz,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION
----	-------	----------	-------------

Q MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	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.
2	Activity (com.totsp.crossword.HttpDownloadActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
3	Activity (com.totsp.crossword.PlayActivity) is not Protected. An intent-filter exists.	warning	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Activity is explicitly exported.
4	Broadcast Receiver (com.totsp.crossword.net.DownloadReceiver) is not Protected. An intent-filter exists.	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the Broadcast Receiver is explicitly exported.
5	Activity (com.totsp.crossword.firstrun.FirstrunActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
6	Activity (com.totsp.crossword.nyt.LoginActivity) is not Protected. [android:exported=true]	high	An Activity is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
----	-------	----------	-----------	-------

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	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/totsp/crossword/PuzzleFinishedActivity.java com/totsp/crossword/PlayActivity.java com/totsp/crossword/io/BrainsOnlyIO.java com/nineoldandroids/animation/PropertyValuesHolder.java com/totsp/crossword/ClueListActivity.java com/totsp/crossword/io/IO.java com/totsp/crossword/net/Downloaders.java com/totsp/crossword/io/KingFeaturesPlaintextIO.java com/totsp/crossword/net/DownloadReceiverGinger.java com/totsp/crossword/net/AbstractPageScraper.java com/totsp/crossword/ImaginaryTimer.java com/totsp/crossword/view/SeparatedListAdapter.java com/totsp/crossword/puz/Puzzle.java com/fasterxml/jackson/core/util/VersionUtil.java com/totsp/crossword/net/AbstractDownloader.java com/totsp/crossword/versions/HoneycombUtil.java com/totsp/crossword/firstrun/Slide1.java com/totsp/crossword/BrowseActivity.java com/totsp/crossword/net/Scrapers.java com/totsp/crossword/io/JPZIO.java com/totsp/crossword/net/AVClubDownloader.java com/totsp/crossword/versions/AndroidVersionUtils.java com/totsp/crossword/io/UclickXMLIO.java com/totsp/crossword/io/XTEA.java com/totsp/crossword/GameHelper.java com/franmontiel/persistentcookiejar/persistence/SerializableCookie.java com/jenzz/materialpreference/Typefaces.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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/totsp/crossword/versions/GingerbreadUtil.java com/totsp/crossword/gmail/GmailDownloader.java com/totsp/crossword/BrowseActivity.java com/totsp/crossword/HttpDownloadActivity.java com/totsp/crossword/shortyz/ShortyzApplication.java com/totsp/crossword/PuzzleDownloadListener.java com/totsp/crossword/ShortyzActivity.java
3	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	okio/Buffer.java
4	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/totsp/crossword/shortyz/BackupAgent.java
5	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	com/totsp/crossword/GameHelper.java

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.
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 implement functionality to encrypt sensitive data 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.

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
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 not in accordance with FCS_COP.1.1(2) and uses the cryptographic algorithm RC2/RC4/MD4/MD5.
12	FCS_COP.1.1(3)	Selection-Based Security Functional Requirements	Cryptographic Operation - Signing	The application perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm RSA schemes using cryptographic key sizes of 2048-bit or greater.
13	FCS_COP.1.1(4)	Selection-Based Security Functional Requirements	Cryptographic Operation - Keyed-Hash Message Authentication	The application perform keyed-hash message authentication with cryptographic algorithm ['HMAC-SHA1'] .
14	FCS_HTTPS_EXT.1.1	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement the HTTPS protocol that complies with RFC 2818.
15	FCS_HTTPS_EXT.1.2	Selection-Based Security Functional Requirements	HTTPS Protocol	The application implement HTTPS using TLS.
16	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
17	FIA_X509_EXT.1.1	Selection-Based Security Functional Requirements	X.509 Certificate Validation	The application invoked platform-provided functionality to validate certificates in accordance with the following rules: ['The certificate path must terminate with a trusted CA certificate'].
18	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
developers.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
world.std.com	ok	IP: 192.74.137.5 Country: United States of America Region: Massachusetts City: Boston Latitude: 42.350819 Longitude: -71.118423 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.nytimes.com	ok	IP: 151.101.37.164 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
myaccount.nytimes.com	ok	IP: 151.101.37.164 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
washingtonpost.as.arkadiumhosted.com	ok	IP: 174.143.221.176 Country: United States of America Region: Texas City: Dallas Latitude: 32.783058 Longitude: -96.806671 View: Google Map
cdn.games.arkadiumhosted.com	ok	IP: 2.23.6.199 Country: France Region: Ile-de-France City: Paris Latitude: 48.853409 Longitude: 2.348800 View: Google Map

DOMAIN	STATUS	GEOLOCATION
crosswords.washingtonpost.com	ok	IP: 52.207.98.240 Country: United States of America Region: Virginia City: Ashburn Latitude: 39.043720 Longitude: -77.487488 View: Google Map
brainsonly.com	ok	IP: 216.154.208.173 Country: United States of America Region: Georgia City: Norcross Latitude: 33.974335 Longitude: -84.238441 View: Google Map
www.cruciverb.com	ok	IP: 159.89.118.99 Country: Canada Region: Ontario City: Toronto Latitude: 43.700111 Longitude: -79.416298 View: Google Map
wij.theworld.com	ok	IP: 69.38.147.200 Country: United States of America Region: Massachusetts City: Brighton Latitude: 42.350819 Longitude: -71.118423 View: Google Map

DOMAIN	STATUS	GEOLOCATION
mazerlm.home.comcast.net	ok	IP: 96.99.227.255 Country: United States of America Region: New Jersey City: Mount Laurel Latitude: 39.947819 Longitude: -74.911682 View: Google Map
chronicle.com	ok	IP: 108.156.60.7 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map
herbach.dnsalias.com	ok	IP: 104.57.229.132 Country: United States of America Region: Connecticut City: Wallingford Latitude: 41.457039 Longitude: -72.823158 View: Google Map
www.lafn.org	ok	IP: 208.91.197.27 Country: United States of America Region: Texas City: Austin Latitude: 30.267151 Longitude: -97.743057 View: Google Map

DOMAIN	STATUS	GEOLOCATION
picayune.uclick.com	ok	IP: 66.6.101.188 Country: United States of America Region: Iowa City: Des Moines Latitude: 41.585686 Longitude: -93.618919 View: Google Map
thinks.com	ok	IP: 217.160.0.29 Country: Germany Region: Baden-Wurttemberg City: Karlsruhe Latitude: 49.004719 Longitude: 8.385830 View: Google Map
puzzles.kingdigital.com	ok	IP: 52.191.222.170 Country: United States of America Region: Virginia City: Washington Latitude: 38.713451 Longitude: -78.159439 View: Google Map
www.people.com	ok	IP: 108.156.60.60 Country: United States of America Region: Washington City: Redmond Latitude: 47.682899 Longitude: -122.120903 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.fleetwoodwack.typepad.com	ok	IP: 104.18.140.190 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map
standalone.com	ok	IP: 45.79.187.215 Country: United States of America Region: New Jersey City: Cedar Knolls Latitude: 40.821945 Longitude: -74.448891 View: Google Map
github.com	ok	IP: 140.82.121.3 Country: United States of America Region: California City: San Francisco Latitude: 37.775700 Longitude: -122.395203 View: Google Map

EMAILS

EMAIL	FILE
kebernet@gmail.com	com/totsp/crossword/shortyz/ShortyzApplication.java

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.

© 2022 Mobile Security Framework - MobSF | [Ajin Abraham](#) | [OpenSecurity](#).