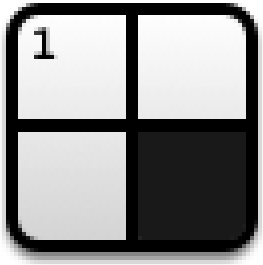
MOBSF

ANDROID STATIC ANALYSIS REPORT



Shortyz (3.2.10)

File Name:	installer324.apk
Package Name:	com.totsp.crossword.shortyz
Scan Date:	May 31, 2022, 11:17 a.m.
App Security Score:	47/100 (MEDIUM RISK)
Grade:	B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	7	1	1	1

FILE INFORMATION

File Name: installer324.apk
Size: 0.18MB
MD5: 7b821f74d9bafd51c7d9353dc5294512
SHA1: 011e71e5ac4a1dd55834fc96f328266efdcca570
SHA256: 6b4d29b9727089b8f71b8ca26cc5f832dbc61a0b7a33886493ec985e2ed790f8

APP INFORMATION

App Name: Shortyz
Package Name: com.totsp.crossword.shortyz
Main Activity: com.totsp.crossword.BrowseActivity
Target SDK: 11
Min SDK: 4
Max SDK:
Android Version Name: 3.2.10
Android Version Code: 30210

APP COMPONENTS

Activities: 8
Services: 0
Receivers: 1
Providers: 0
Exported Activities: 2
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.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.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: dx

BROWSABLE ACTIVITIES

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

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

MANIFEST ANALYSIS

NO	ISSUE	SEVERITY	DESCRIPTION
1	Application Data can be Backed up [android:allowBackup] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
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.

</> CODE ANALYSIS

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/totsp/crossword/ImaginaryTimer.java com/totsp/crossword/view/PlayboardRenderer.java com/totsp/crossword/net/NYTDownloader.java com/totsp/crossword/net/KFSDownloader.java com/totsp/crossword/ClueListActivity.java com/totsp/crossword/net/AbstractJPZDownloader.java com/totsp/crossword/versions/JellyBeanUtil.java com/totsp/crossword/versions/HoneycombUtil.java com/totsp/crossword/net/AbstractDownloader.java com/totsp/crossword/shortyz/ShortyzApplication.java com/totsp/crossword/net/Scrapers.java com/totsp/crossword/net/AVClubDownload

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/net/AVClubDownloader.java com/totsp/crossword/view/MultitouchHandler.java com/totsp/crossword/versions/AndroidVersionUtils.java com/totsp/crossword/BrowseActivity.java com/totsp/crossword/io/UclickXMLIO.java com/totsp/crossword/net/Downloaders.java com/totsp/crossword/io/JPZIO.java com/totsp/crossword/view/ScrollingImageView.java com/totsp/crossword/ShortyzActivity.java com/totsp/crossword/net/DownloadReceiverGinger.java com/totsp/crossword/versions/GingerbreadUtil.java com/totsp/crossword/net/AbstractPageScraper.java com/totsp/crossword/PlayActivity.java com/totsp/crossword/io/IO.java com/totsp/crossword/puz/Puzzle.java com/totsp/crossword/versions/DefaultUtil.java com/totsp/crossword/io/KingFeaturesPlaintextIO.java com/totsp/crossword/puz/Box.java
2	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/totsp/crossword/net/NYTDownloader.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
3	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/shortyz/ShortyzApplication.java com/totsp/crossword/BrowseActivity.java com/totsp/crossword/HttpDownloadActivity.java com/totsp/crossword/PuzzleDownloadListener.java com/totsp/crossword/net/Downloaders.java com/totsp/crossword/ShortyzActivity.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

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
2	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application generate no asymmetric cryptographic keys.
3	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity'].
4	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
5	FDP_NET_EXT.1.1	Security Functional Requirements	Network Communications	The application has user/application initiated network communications.
6	FDP_DAR_EXT.1.1	Security Functional Requirements	Encryption Of Sensitive Application Data	The application does not encrypt files in non-volatile memory.
7	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.
8	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.

🔍 DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
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
www.washingtonpost.com	ok	IP: 23.66.16.193 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 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

DOMAIN	STATUS	GEOLOCATION
thinks.com	ok	IP: 217.160.0.29 Country: Germany Region: Baden-Wurttemberg City: Karlsruhe Latitude: 49.004719 Longitude: 8.385830 View: Google Map
www.people.com	ok	IP: 108.156.60.77 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
cdn.games.arkadiumhosted.com	ok	IP: 23.62.99.89 Country: Netherlands Region: Noord-Holland City: Amsterdam Latitude: 52.374031 Longitude: 4.889690 View: Google Map

DOMAIN	STATUS	GEOLOCATION
www.fleetwoodwack.typepad.com	ok	**IP:** 104.18.137.190 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **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
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
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

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
select.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
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
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

DOMAIN	STATUS	GEOLOCATION
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

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.