MOBILE APPLICATION ASSIGNMENT

IE3112

IT 19122410
W.P.T. Pamalka

PART 1

What is Static Analysis?

Static analysis is the method of debugging a source code without executing the code. This method helps to find errors, security vulnerabilities, violation of coding standards within the source code of an application. This analysis process is usually done in the early development of the application to offer a less error prone application.

Several advantages of static analysis are:

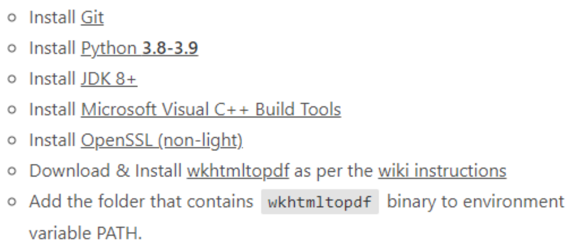
1. Fast process due to using automated tools
2. Automated tools increase the chance of lesser human errors
3. Automated tools increase the chances of finding more vulnerabilities which increases the application security
4. can evaluate all the code and as a result it increases the code quality

Performing Static Analysis

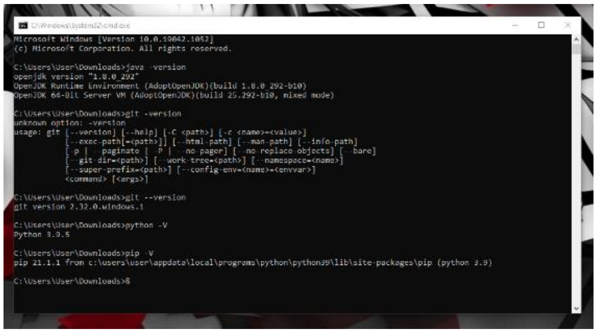
Installing ModSF

The static analysis was performed on windows OS due to an error within the kali OS.

First step was to install all the necessary tools needed. The tools were as follows:



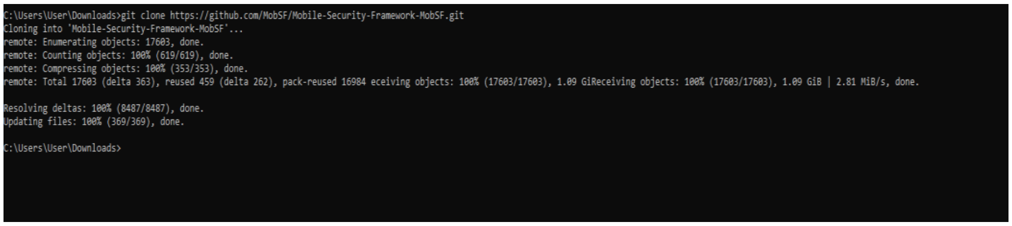
- Install Git
- Install Python **3.8-3.9**
- Install JDK 8+
- Install Microsoft Visual C++ Build Tools
- Install OpenSSL (non-light)
- Download & Install wkhtmltopdf as per the wiki instructions
- Add the folder that contains `wkhtmltopdf` binary to environment variable PATH.



```
Microsoft Windows [Version 10.0.19042.1052]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User\Downloads>java -version
openjdk version "1.8.0_292"
OpenJDK Runtime Environment (AdoptOpenJDK)(build 1.8.0_292-b10)
OpenJDK 64-Bit Server VM (AdoptOpenJDK)(build 25.292-b10, mixed mode)

C:\Users\User\Downloads>git -version
unknown option: -version
usage: git [--version] [--help] [-C <path>] [-c <name>=<value>]
           [--exec-path[=<path>]] [--html-path] [--man-path] [--info-path]
           [-p | --paginate | -P | --no-pager] [--no-replace-objects] [--bare]
           [--git-dir=<path>] [--work-tree=<path>] [--namespace=<name>]
           [--super-prefix=<path>] [--config-env=<name>=<envvar>]
           <command> [<args>]

C:\Users\User\Downloads>git --version
git version 2.32.0.windows.1

C:\Users\User\Downloads>python -V
Python 3.9.5

C:\Users\User\Downloads>pip -V
pip 21.1.1 from c:\users\user\appdata\local\programs\python\python39\lib\site-packages\pip (python 3.9)

C:\Users\User\Downloads>
```

The next step is to clone the GitHub repository and then to run the setup by using following commands:

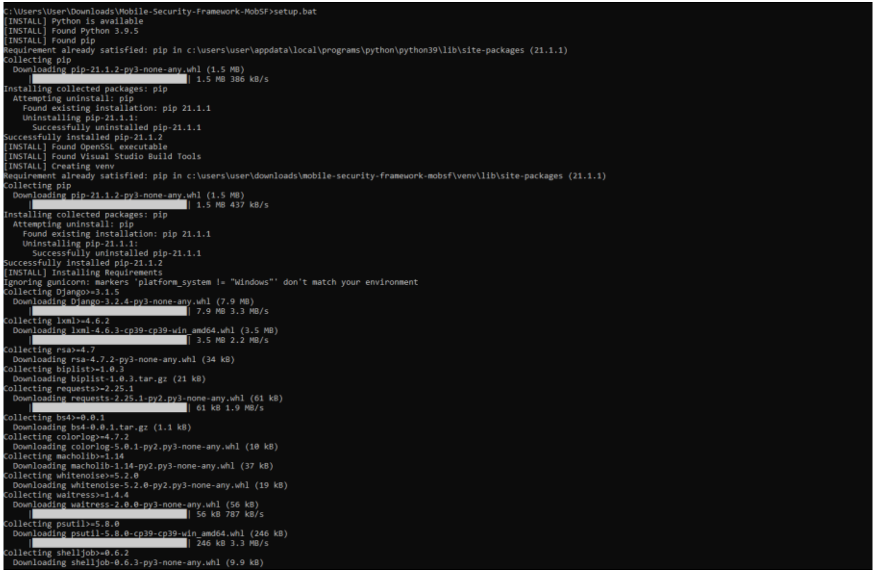
1. git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git



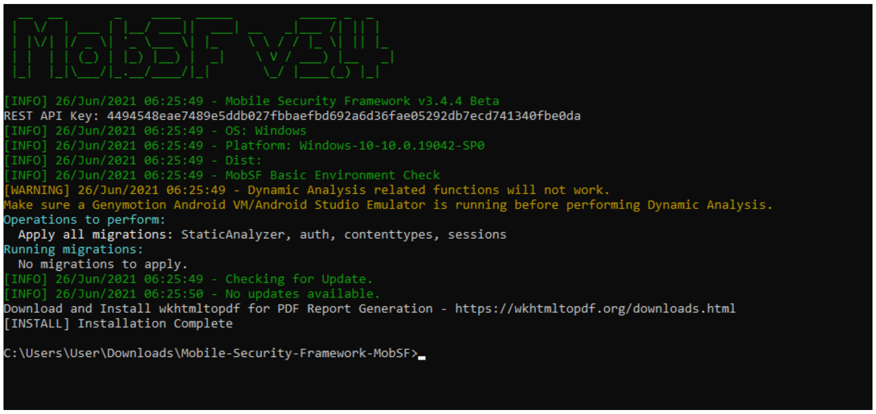
```
C:\Users\User\Downloads>git clone https://github.com/MobSF/Mobile-Security-Framework-MobSF.git
Cloning into 'Mobile-Security-Framework-MobSF'...
remote: Enumerating objects: 17603, done.
remote: Counting objects: 100% (619/619), done.
remote: Compressing objects: 100% (353/353), done.
remote: Total 17603 (delta 363), reused 459 (delta 262), pack-reused 16984 eceiving objects: 100% (17603/17603), 1.09 GiReceiving objects: 100% (17603/17603), 1.09 GiB | 2.81 MiB/s, done.

Resolving deltas: 100% (8487/8487), done.
Updating files: 100% (369/369), done.

C:\Users\User\Downloads>
```

2. cd Mobile-Security-Framework-MobSF

3. setup.bat

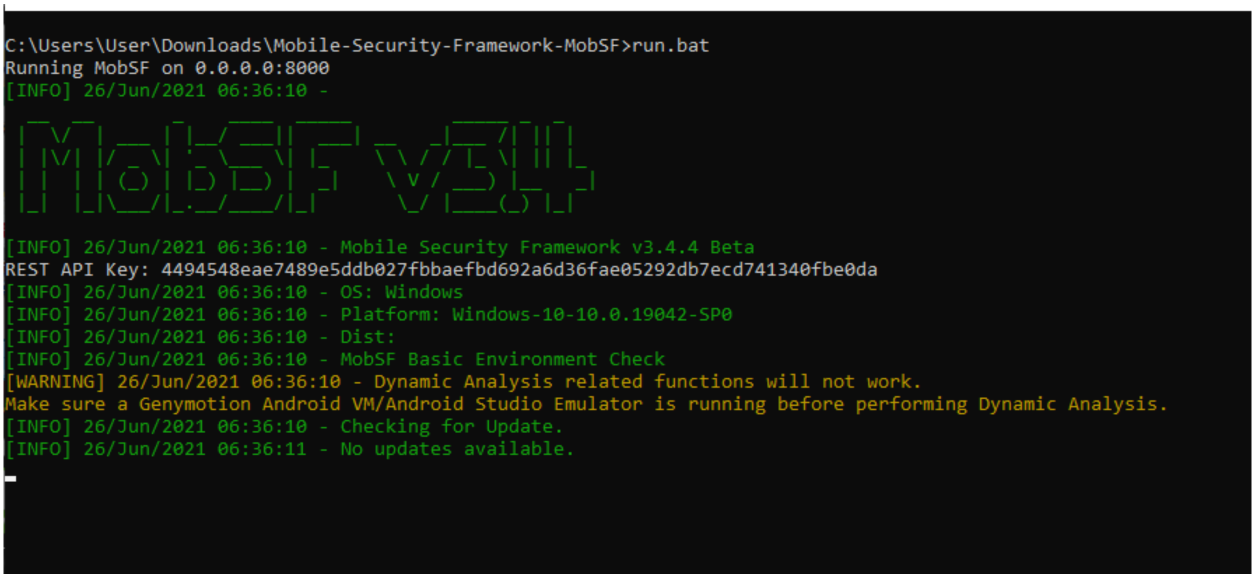


```
C:\Users\User\Downloads\Mobile-Security-Framework-MobSF>setup.bat
[INSTALL] Python is available
[INSTALL] Found Python 3.9.5
[INSTALL] Found pip
Requirement already satisfied: pip in c:\users\user\appdata\local\programs\python\python39\lib\site-packages (21.1.1)
Collecting pip
  Downloading pip-21.1.2-py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 386 kB/s
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 21.1.1
    Uninstalling pip-21.1.1:
      Successfully uninstalled pip-21.1.1
Successfully installed pip-21.1.2
[INSTALL] Found OpenSSL executable
[INSTALL] Found Visual Studio Build Tools
[INSTALL] Creating venv
Requirement already satisfied: pip in c:\users\user\downloads\mobile-security-framework-mobsf\venv\lib\site-packages (21.1.1)
Collecting pip
  Downloading pip-21.1.2-py3-none-any.whl (1.5 MB)
     |████████████████████████████████| 1.5 MB 437 kB/s
Installing collected packages: pip
  Attempting uninstall: pip
    Found existing installation: pip 21.1.1
    Uninstalling pip-21.1.1:
      Successfully uninstalled pip-21.1.1
Successfully installed pip-21.1.2
[INSTALL] Installing Requirements
Ignoring gunicorn: markers 'platform_system != "Windows"' don't match your environment
Collecting Django>=3.1.5
  Downloading Django-3.2.4-py3-none-any.whl (7.9 MB)
     |████████████████████████████████| 7.9 MB 3.3 MB/s
Collecting lxml>=4.6.2
  Downloading lxml-4.6.3-cp39-cp39-win_amd64.whl (3.5 MB)
     |████████████████████████████████| 3.5 MB 2.2 MB/s
Collecting rsa>=4.7
  Downloading rsa-4.7.2-py3-none-any.whl (34 kB)
Collecting biplist>=1.0.3
  Downloading biplist-1.0.3.tar.gz (21 kB)
Collecting requests>=2.25.1
  Downloading requests-2.25.1-py2.py3-none-any.whl (61 kB)
     |████████████████████████████████| 61 kB 1.9 MB/s
Collecting bs4>=0.0.1
  Downloading bs4-0.0.1.tar.gz (1.1 kB)
Collecting colorlog>=4.7.2
  Downloading colorlog-5.0.1-py2.py3-none-any.whl (10 kB)
Collecting macholib>=1.14
  Downloading macholib-1.14-py2.py3-none-any.whl (37 kB)
Collecting whitenoise>=5.2.0
  Downloading whitenoise-5.2.0-py2.py3-none-any.whl (19 kB)
Collecting waitress>=1.4.4
  Downloading waitress-2.0.0-py3-none-any.whl (56 kB)
     |████████████████████████████████| 56 kB 787 kB/s
Collecting psutil>=5.8.0
  Downloading psutil-5.8.0-cp39-cp39-win_amd64.whl (246 kB)
     |████████████████████████████████| 246 kB 3.3 MB/s
Collecting shelljob>=0.6.2
  Downloading shelljob-0.6.3-py3-none-any.whl (9.9 kB)
```



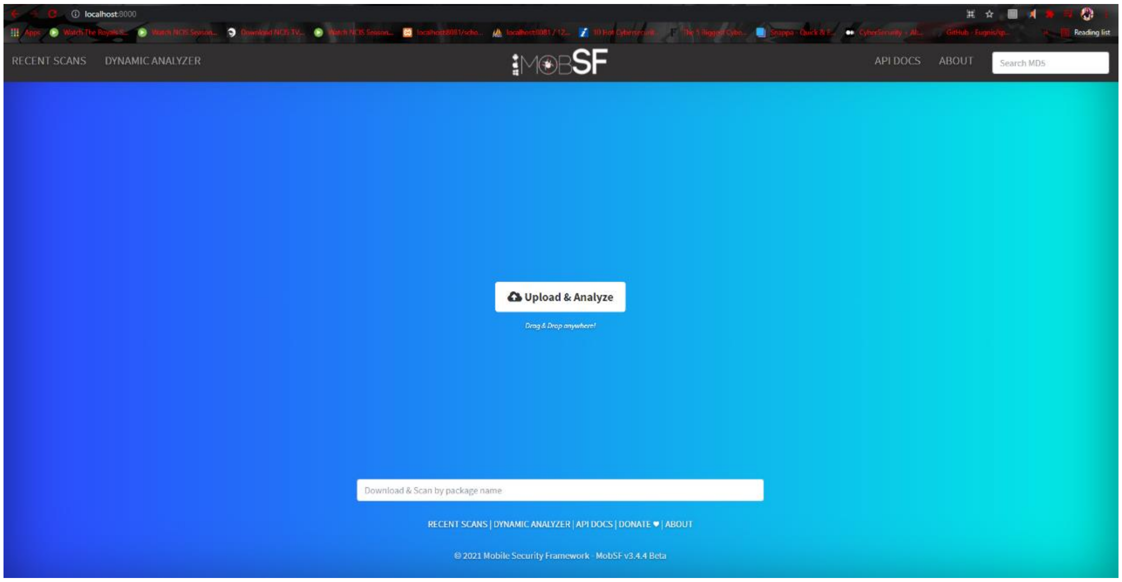
```
 __  __       _     ____  _____         _____ _  _
|  \/  | ___ | |__ / ___||  ___| __   _|___ /| || |
| |\/| |/ _ \| '_ \\___ \| |_    \ \ / / |_ \| || |_
| |  | | (_) | |_) |___) |  _|    \ V / ___) |__   _|
|_|  |_|\___/|_.__/|____/|_|       \_/ |____(_) |_|

[INFO] 26/Jun/2021 06:25:49 - Mobile Security Framework v3.4.4 Beta
REST API Key: 4494548eae7489e5ddb027fbbaefbd692a6d36fae05292db7ecd741340fbe0da
[INFO] 26/Jun/2021 06:25:49 - OS: Windows
[INFO] 26/Jun/2021 06:25:49 - Platform: Windows-10-10.0.19042-SP0
[INFO] 26/Jun/2021 06:25:49 - Dist:
[INFO] 26/Jun/2021 06:25:49 - MobSF Basic Environment Check
[WARNING] 26/Jun/2021 06:25:49 - Dynamic Analysis related functions will not work.
Make sure a Genymotion Android VM/Android Studio Emulator is running before performing Dynamic Analysis.
Operations to perform:
  Apply all migrations: StaticAnalyzer, auth, contenttypes, sessions
Running migrations:
  No migrations to apply.
[INFO] 26/Jun/2021 06:25:49 - Checking for Update.
[INFO] 26/Jun/2021 06:25:50 - No updates available.
Download and Install wkhtmltopdf for PDF Report Generation - https://wkhtmltopdf.org/downloads.html
[INSTALL] Installation Complete

C:\Users\User\Downloads\Mobile-Security-Framework-MobSF>
```

Once the setup is installed successfully, run it by run.bat command.

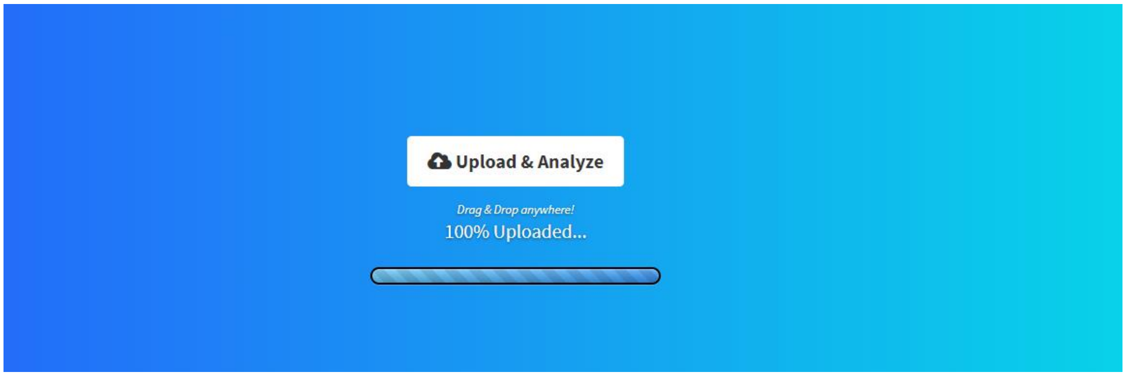


```
C:\Users\User\Downloads\Mobile-Security-Framework-MobSF>run.bat
Running MobSF on 0.0.0.0:8000
[INFO] 26/Jun/2021 06:36:10 -
  __  __       _    ____  _____       _____ _  _
 |  \/  | ___ | |__/ ___||  ___|_   _|___ /| || |
 | |\/| |/ _ \| '_ \___ \| |_  \ \ / / |_ \| || |_
 | |  | | (_) | |_) |__) |  _|  \ V / ___) |__   _|
 |_|  |_|\___/|_.__/____/|_|     \_/ |____(_) |_|

[INFO] 26/Jun/2021 06:36:10 - Mobile Security Framework v3.4.4 Beta
REST API Key: 4494548eae7489e5ddb027fbbaefbd692a6d36fae05292db7ecd741340fbe0da
[INFO] 26/Jun/2021 06:36:10 - OS: Windows
[INFO] 26/Jun/2021 06:36:10 - Platform: Windows-10-10.0.19042-SP0
[INFO] 26/Jun/2021 06:36:10 - Dist:
[INFO] 26/Jun/2021 06:36:10 - MobSF Basic Environment Check
[WARNING] 26/Jun/2021 06:36:10 - Dynamic Analysis related functions will not work.
Make sure a Genymotion Android VM/Android Studio Emulator is running before performing Dynamic Analysis.
[INFO] 26/Jun/2021 06:36:10 - Checking for Update.
[INFO] 26/Jun/2021 06:36:11 - No updates available.
```

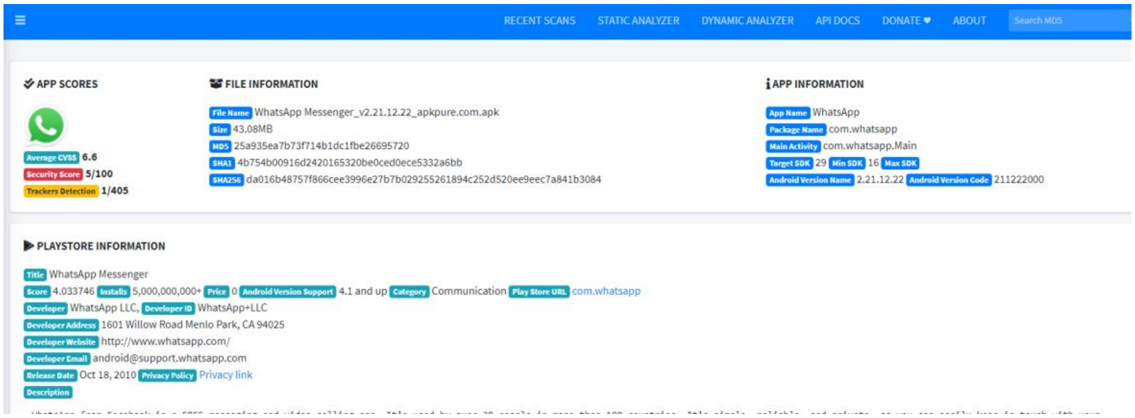
MobSF is opened through Google chrome at http://localhost:8000/


localhost:8000
RECENT SCANS
DYNAMIC ANALYZER
MobSF
API DOCS
ABOUT
Search MDS
Upload & Analyze
Drag & Drop anywhere!
Download & Scan by package name
RECENT SCANS | DYNAMIC ANALYZER | API DOCS | DONATE ♥ | ABOUT
© 2021 Mobile Security Framework - MobSF v3.4.4 Beta

WhatsApp Messenger v2.21.12.22 was used for the static analysis. First, The APK is uploaded for analysis.



Once the APK is uploaded and analyzed, it displays file information and app information of the APK as given below. It also gives out scores based on the source code structure.



APP SCORES

Average CVSS 6.6
Security Score 5/100
Trackers Detection 1/405

FILE INFORMATION

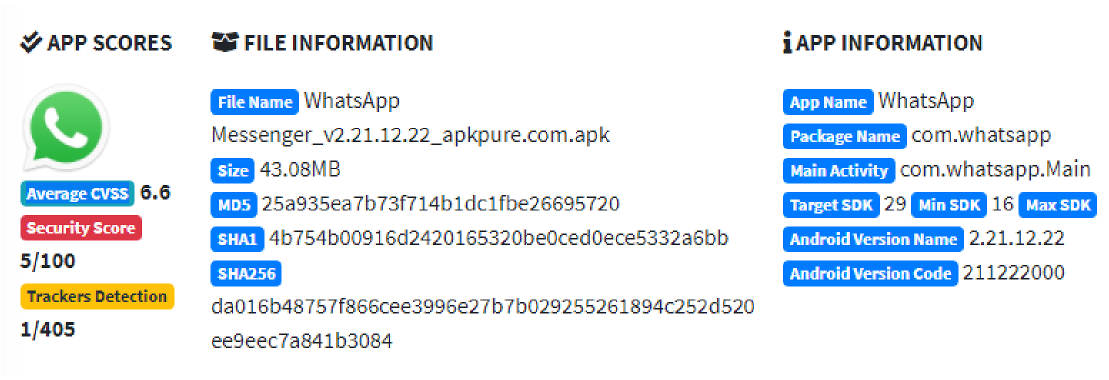
File Name WhatsApp Messenger_v2.21.12.22_apkpure.com.apk
Size 43.08MB
MD5 25a935ea7b73f714b1dc1fbe26695720
SHA1 4b754b00916d2420165320be0ced0ece5332a6bb
SHA256 da016b48757f866cee3996e27b7b029255261894c252d520ee9eec7a841b3084

APP INFORMATION

App Name WhatsApp
Package Name com.whatsapp
Main Activity com.whatsapp.Main
Target SDK 29 Min SDK 16 Max SDK
Android Version Name 2.21.12.22 Android Version Code 211222000

PLAYSTORE INFORMATION

Title WhatsApp Messenger
Score 4.033746 Installs 5,000,000,000+ Price 0 Android Version Support 4.1 and up Category Communication Play Store URL com.whatsapp
Developer WhatsApp LLC, Developer ID WhatsApp+LLC
Developer Address 1601 Willow Road Menlo Park, CA 94025
Developer Website http://www.whatsapp.com/
Developer Email android@support.whatsapp.com
Release Date Oct 18, 2010 Privacy Policy Privacy link
Description



✔ APP SCORES

Average CVSS 6.6

Security Score 5/100

Trackers Detection 1/405

FILE INFORMATION

File Name WhatsApp Messenger_v2.21.12.22_apkpure.com.apk

Size 43.08MB

MD5 25a935ea7b73f714b1dc1fbe26695720

SHA1 4b754b00916d2420165320be0ced0ece5332a6bb

SHA256 da016b48757f866cee3996e27b7b029255261894c252d520ee9eec7a841b3084

APP INFORMATION

App Name WhatsApp

Package Name com.whatsapp

Main Activity com.whatsapp.Main

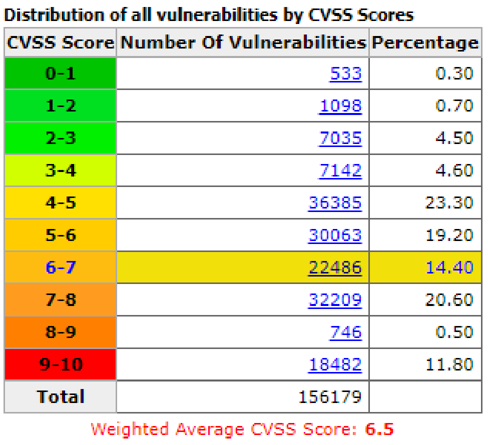
Target SDK 29 Min SDK 16 Max SDK

Android Version Name 2.21.12.22

Android Version Code 211222000

APP Scores

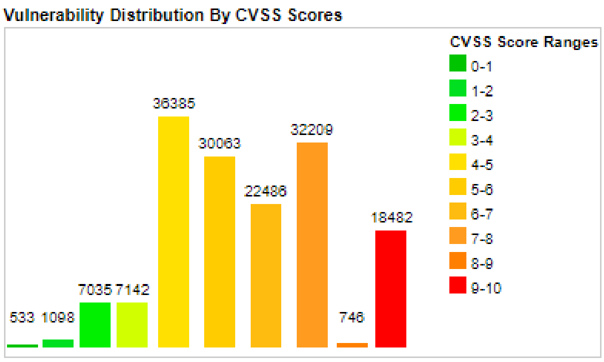
CVSS which stands for Common Vulnerability Scoring System, is a scoring system that provides a number value (0-10) representing the severity of the vulnerability. Here, the given score is 6.6 which gives out a medium rating. CVSS scores are calculated by a formulation that depends on how easy it is to exploit the vulnerability and the impact value when it is exploited.



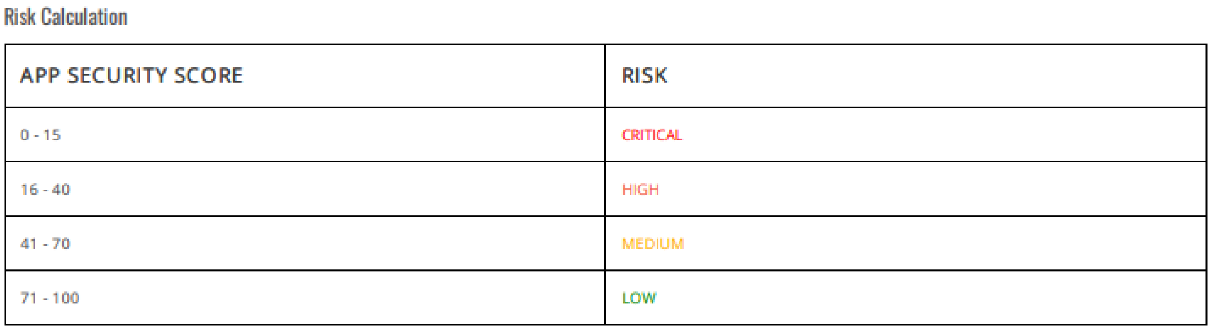
Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	533	0.30
1-2	1098	0.70
2-3	7035	4.50
3-4	7142	4.60
4-5	36385	23.30
5-6	30063	19.20
6-7	22486	14.40
7-8	32209	20.60
8-9	746	0.50
9-10	18482	11.80
Total	156179	

Weighted Average CVSS Score: 6.5



The security score is the overall score given for the APK by the MobSF. The security score given is 5/100 and as a result, this APK cannot be recommend for customer use due to safety issues.



Risk Calculation

APP SECURITY SCORE	RISK
0 - 15	CRITICAL
16 - 40	HIGH
41 - 70	MEDIUM
71 - 100	LOW

The tracker detection score follows any tracking agents that could be hidden within the source code or APK.

File Information

MD5 Hash - commonly used for validating data integrity

SHA1 Hash – often used to verify the file is not altered.

SHA256 Hash – used for secure password hashing.

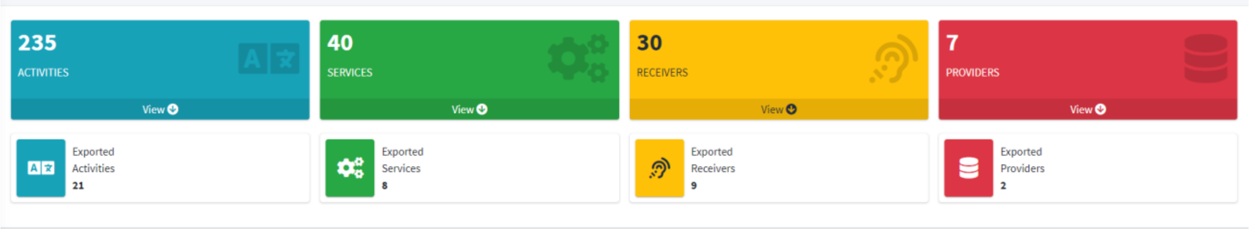
App Information

Target SDK – version of android that the app was created to run

Min SDK – the minimum version of android that is required to run the app

Max SDK – has no effect on NDK builds

4 Components of APK



235
ACTIVITIES
View

40
SERVICES
View

30
RECEIVERS
View

7
PROVIDERS
View

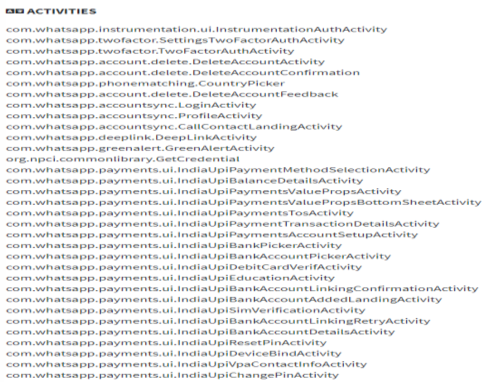
Exported Activities
21

Exported Services
8

Exported Receivers
9

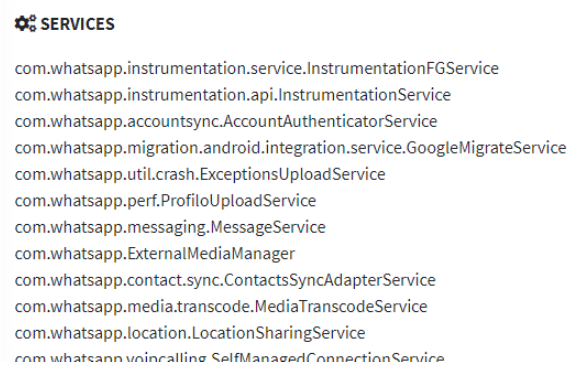
Exported Providers
2

Activities – user interfaces of the app and activities that user interacts with.



```
ACTIVITIES
com.whatsapp.instrumentation.ui.InstrumentationAuthActivity
com.whatsapp.twofactor.SettingsTwoFactorAuthActivity
com.whatsapp.twofactor.TwoFactorAuthActivity
com.whatsapp.account.delete.DeleteAccountActivity
com.whatsapp.account.delete.DeleteAccountConfirmation
com.whatsapp.phonematching.CountryPicker
com.whatsapp.account.delete.DeleteAccountFeedback
com.whatsapp.accountsync.LoginActivity
com.whatsapp.accountsync.ProfileActivity
com.whatsapp.accountsync.CallContactLandingActivity
com.whatsapp.deeplink.DeepLinkActivity
com.whatsapp.greenalert.GreenAlertActivity
org.npci.commonlibrary.GetCredential
com.whatsapp.payments.ui.IndiaUpiPaymentMethodSelectionActivity
com.whatsapp.payments.ui.IndiaUpiBalanceDetailsActivity
com.whatsapp.payments.ui.IndiaUpiPaymentsValuePropsActivity
com.whatsapp.payments.ui.IndiaUpiPaymentsValuePropsBottomSheetActivity
com.whatsapp.payments.ui.IndiaUpiPaymentsTosActivity
com.whatsapp.payments.ui.IndiaUpiPaymentTransactionDetailsActivity
com.whatsapp.payments.ui.IndiaUpiPaymentsAccountSetupActivity
com.whatsapp.payments.ui.IndiaUpiBankPickerActivity
com.whatsapp.payments.ui.IndiaUpiBankAccountPickerActivity
com.whatsapp.payments.ui.IndiaUpiDebitCardVerifActivity
com.whatsapp.payments.ui.IndiaUpiEducationActivity
com.whatsapp.payments.ui.IndiaUpiBankAccountLinkingConfirmationActivity
com.whatsapp.payments.ui.IndiaUpiBankAccountAddedLandingActivity
com.whatsapp.payments.ui.IndiaUpiSimVerificationActivity
com.whatsapp.payments.ui.IndiaUpiBankAccountLinkingRetryActivity
com.whatsapp.payments.ui.IndiaUpiBankAccountDetailsActivity
com.whatsapp.payments.ui.IndiaUpiResetPinActivity
com.whatsapp.payments.ui.IndiaUpiDeviceBindActivity
com.whatsapp.payments.ui.IndiaUpiVpaContactInfoActivity
com.whatsapp.payments.ui.IndiaUpiChangePinActivity
```

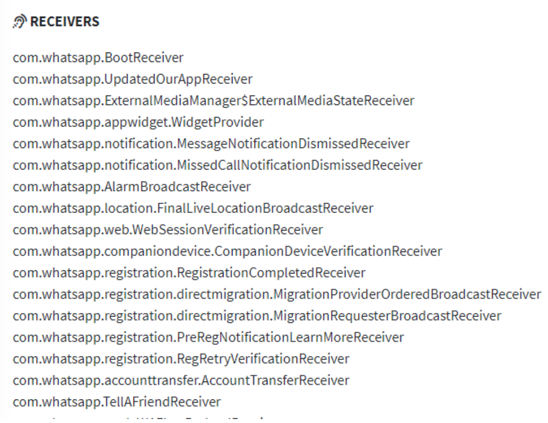
Services – Services that keeps the app running in the background



SERVICES

com.whatsapp.instrumentation.service.InstrumentationFGService
com.whatsapp.instrumentation.api.InstrumentationService
com.whatsapp.accountsync.AccountAuthenticatorService
com.whatsapp.migration.android.integration.service.GoogleMigrateService
com.whatsapp.util.crash.ExceptionsUploadService
com.whatsapp.perf.ProfiloUploadService
com.whatsapp.messaging.MessageService
com.whatsapp.ExternalMediaManager
com.whatsapp.contact.sync.ContactsSyncAdapterService
com.whatsapp.media.transcode.MediaTranscodeService
com.whatsapp.location.LocationSharingService
com.whatsapp.voipcalling.SelfManagedConnectionService

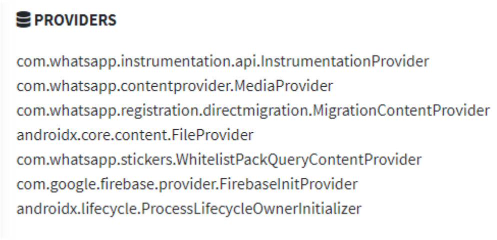
Receivers – enables the system to deliver functions to the app outside the regular uses allowing the app to response to wider broadcast announcements.



RECEIVERS

com.whatsapp.BootReceiver
com.whatsapp.UpdatedOurAppReceiver
com.whatsapp.ExternalMediaManager$ExternalMediaStateReceiver
com.whatsapp.appwidget.WidgetProvider
com.whatsapp.notification.MessageNotificationDismissedReceiver
com.whatsapp.notification.MissedCallNotificationDismissedReceiver
com.whatsapp.AlarmBroadcastReceiver
com.whatsapp.location.FinalLiveLocationBroadcastReceiver
com.whatsapp.web.WebSessionVerificationReceiver
com.whatsapp.companiondevice.CompanionDeviceVerificationReceiver
com.whatsapp.registration.RegistrationCompletedReceiver
com.whatsapp.registration.directmigration.MigrationProviderOrderedBroadcastReceiver
com.whatsapp.registration.directmigration.MigrationRequesterBroadcastReceiver
com.whatsapp.registration.PreRegNotificationLearnMoreReceiver
com.whatsapp.registration.RegRetryVerificationReceiver
com.whatsapp.accounttransfer.AccountTransferReceiver
com.whatsapp.TellAFriendReceiver

Providers - share app data that are stored in the file systems in the database on the web or other storage location the app can access.



PROVIDERS

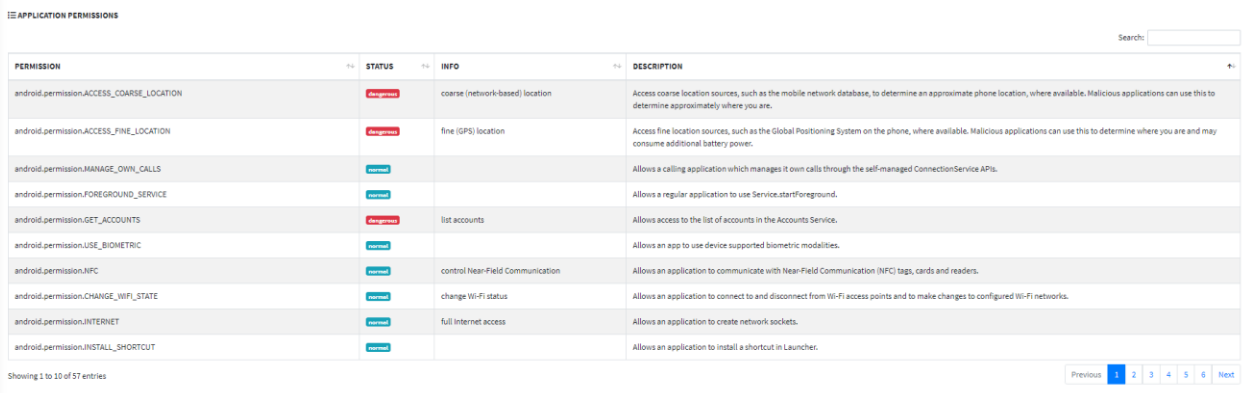
com.whatsapp.instrumentation.api.InstrumentationProvider
com.whatsapp.contentprovider.MediaProvider
com.whatsapp.registration.directmigration.MigrationContentProvider
androidx.core.content.FileProvider
com.whatsapp.stickers.WhitelistPackQueryContentProvider
com.google.firebase.provider.FirebaseInitProvider
androidx.lifecycle.ProcessLifecycleOwnerInitializer

Application Permissions

Application permission regulates access and functions of the software. This category is divided into 2: normal and dangerous.

Normal – safe, default without asking for user permission

Dangerous – risk to user privacy.



APPLICATION PERMISSIONS

Search:

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.
android.permission.MANAGE_OWN_CALLS	normal		Allows a calling application which manages it own calls through the self-managed ConnectionService APIs.
android.permission.FOREGROUND_SERVICE	normal		Allows a regular application to use Service.startForeground.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.USE_BIOMETRIC	normal		Allows an app to use device supported biometric modalities.
android.permission.NFC	normal	control Near-Field Communication	Allows an application to communicate with Near-Field Communication (NFC) tags, cards and readers.
android.permission.CHANGE_WIFI_STATE	normal	change Wi-Fi status	Allows an application to connect to and disconnect from Wi-Fi access points and to make changes to configured Wi-Fi networks.
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.INSTALL_SHORTCUT	normal		Allows an application to install a shortcut in Launcher.

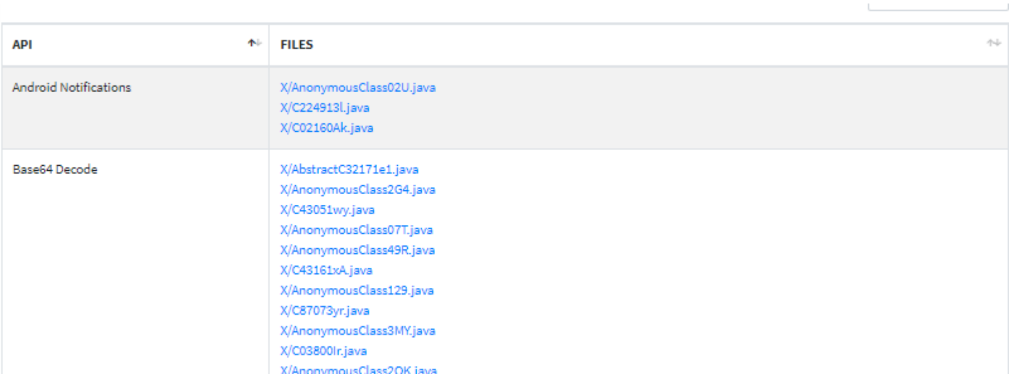
Showing 1 to 10 of 57 entries

Android API

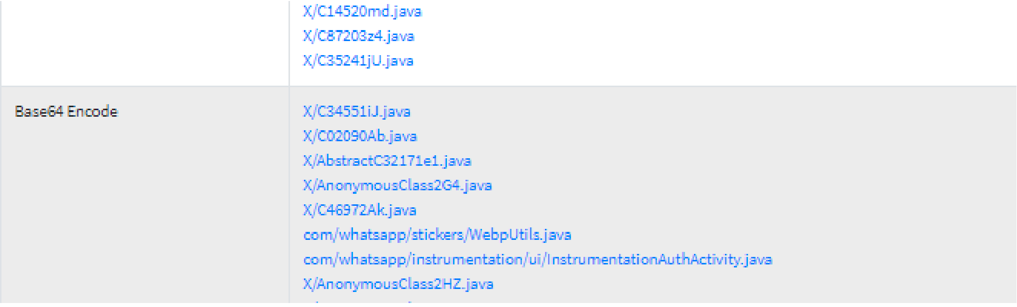
API (Application Program Interface) is the framework the application uses to interact with the fundamental android system.

APIs available within this APK are:

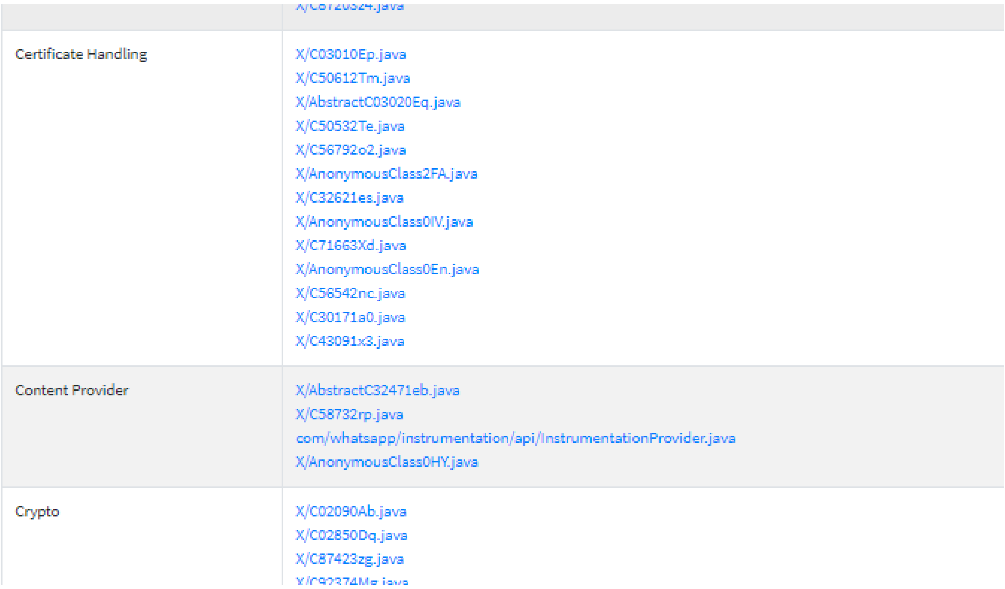
- Android notifications
- Base64 decode
- Base64 encoder
- Certificate handling
- Content provider
- Crypto
- Execute OS command
- Get installed application
- Get phone numbers
- Get SIM operator name and more…



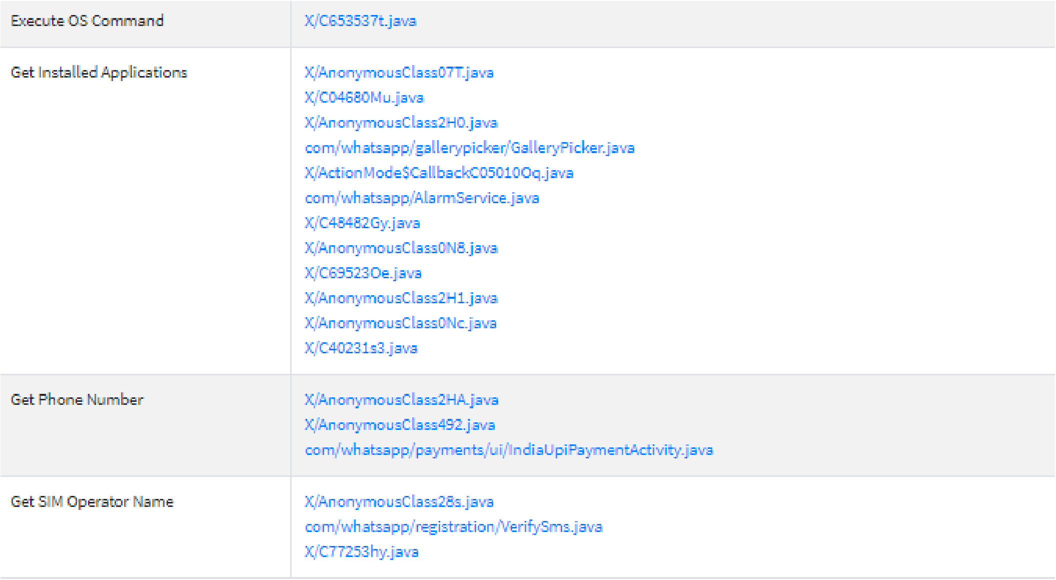
API	FILES
Android Notifications	X/AnonymousClass02U.java X/C224913l.java X/C02160Ak.java
Base64 Decode	X/AbstractC32171e1.java X/AnonymousClass2G4.java X/C43051wy.java X/AnonymousClass07T.java X/AnonymousClass49R.java X/C43161xA.java X/AnonymousClass129.java X/C87073yr.java X/AnonymousClass3MY.java X/C03800Ir.java X/AnonymousClass2OK.java



	X/C14520md.java X/C87203z4.java X/C35241jU.java
Base64 Encode	X/C34551iJ.java X/C02090Ab.java X/AbstractC32171e1.java X/AnonymousClass2G4.java X/C46972Ak.java com/whatsapp/stickers/WebpUtils.java com/whatsapp/instrumentation/ui/InstrumentationAuthActivity.java X/AnonymousClass2HZ.java



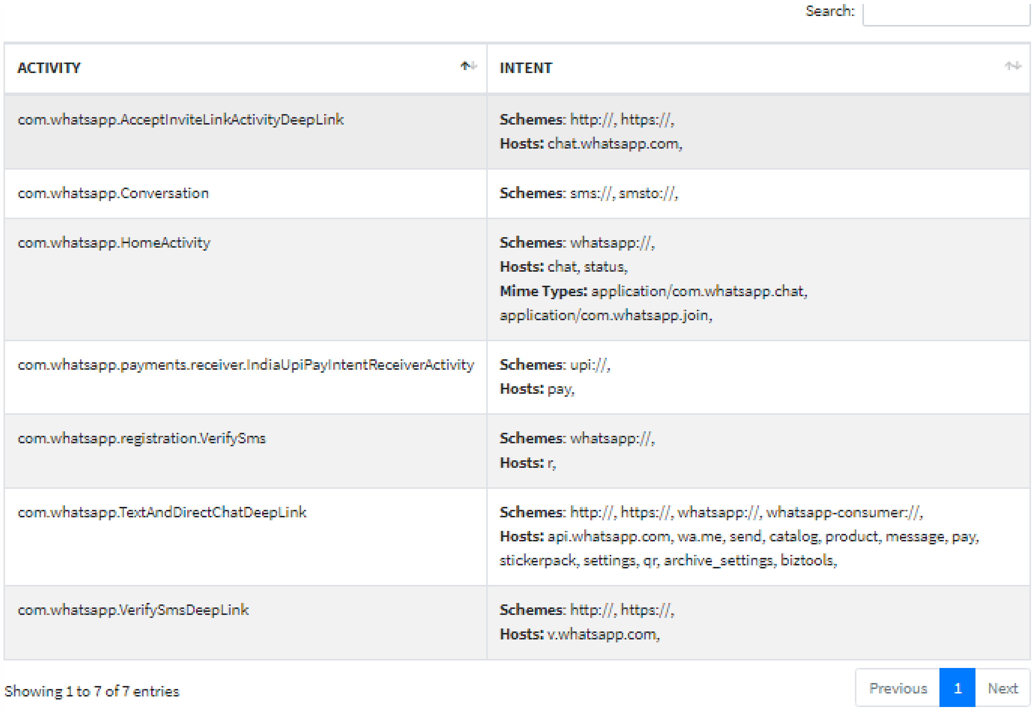
	X/C87203z4.java
Certificate Handling	X/C03010Ep.java X/C50612Tm.java X/AbstractC03020Eq.java X/C50532Te.java X/C56792o2.java X/AnonymousClass2FA.java X/C32621es.java X/AnonymousClass0IV.java X/C71663Xd.java X/AnonymousClass0En.java X/C56542nc.java X/C30171a0.java X/C43091x3.java
Content Provider	X/AbstractC32471eb.java X/C58732rp.java com/whatsapp/instrumentation/api/InstrumentationProvider.java X/AnonymousClass0HY.java
Crypto	X/C02090Ab.java X/C02850Dq.java X/C87423zg.java X/C92374Mg.java



Execute OS Command	X/C653537t.java
Get Installed Applications	X/AnonymousClass07T.java X/C04680Mu.java X/AnonymousClass2H0.java com/whatsapp/gallerypicker/GalleryPicker.java X/ActionMode$CallbackC05010Oq.java com/whatsapp/AlarmService.java X/C48482Gy.java X/AnonymousClass0N8.java X/C69523Oe.java X/AnonymousClass2H1.java X/AnonymousClass0Nc.java X/C40231s3.java
Get Phone Number	X/AnonymousClass2HA.java X/AnonymousClass492.java com/whatsapp/payments/ui/IndiaUpiPaymentActivity.java
Get SIM Operator Name	X/AnonymousClass28s.java com/whatsapp/registration/VerifySms.java X/C77253hy.java

Browsable Activities

The user can control how the application should react when user clicks on an activity.



Search:

ACTIVITY	INTENT
com.whatsapp.AcceptInviteLinkActivityDeepLink	**Schemes**: http://, https://, **Hosts:** chat.whatsapp.com,
com.whatsapp.Conversation	**Schemes**: sms://, smsto://,
com.whatsapp.HomeActivity	**Schemes**: whatsapp://, **Hosts:** chat, status, **Mime Types:** application/com.whatsapp.chat, application/com.whatsapp.join,
com.whatsapp.payments.receiver.IndiaUpiPayIntentReceiverActivity	**Schemes**: upi://, **Hosts:** pay,
com.whatsapp.registration.VerifySms	**Schemes**: whatsapp://, **Hosts:** r,
com.whatsapp.TextAndDirectChatDeepLink	**Schemes**: http://, https://, whatsapp://, whatsapp-consumer://, **Hosts:** api.whatsapp.com, wa.me, send, catalog, product, message, pay, stickerpack, settings, qr, archive_settings, biztools,
com.whatsapp.VerifySmsDeepLink	**Schemes**: http://, https://, **Hosts:** v.whatsapp.com,

Showing 1 to 7 of 7 entries

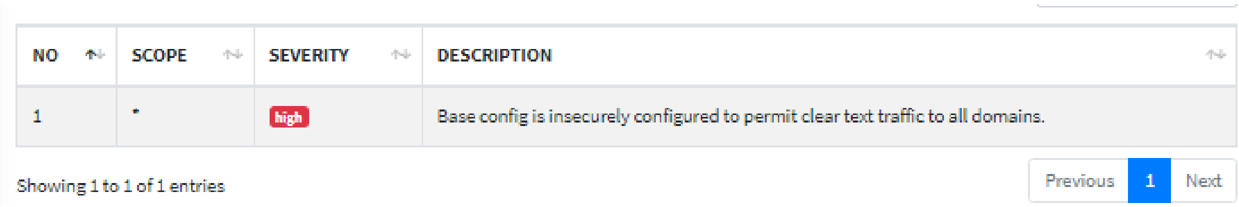
Security Analysis

Security analysis has 6 categories:

1. Network Security
2. Manifest Analysis
3. Code Analysis
4. Binary Analysis
5. NIAP Analysis
6. File Analysis

Network Security

Network security is present to protect the devices from threats and vulnerabilities.



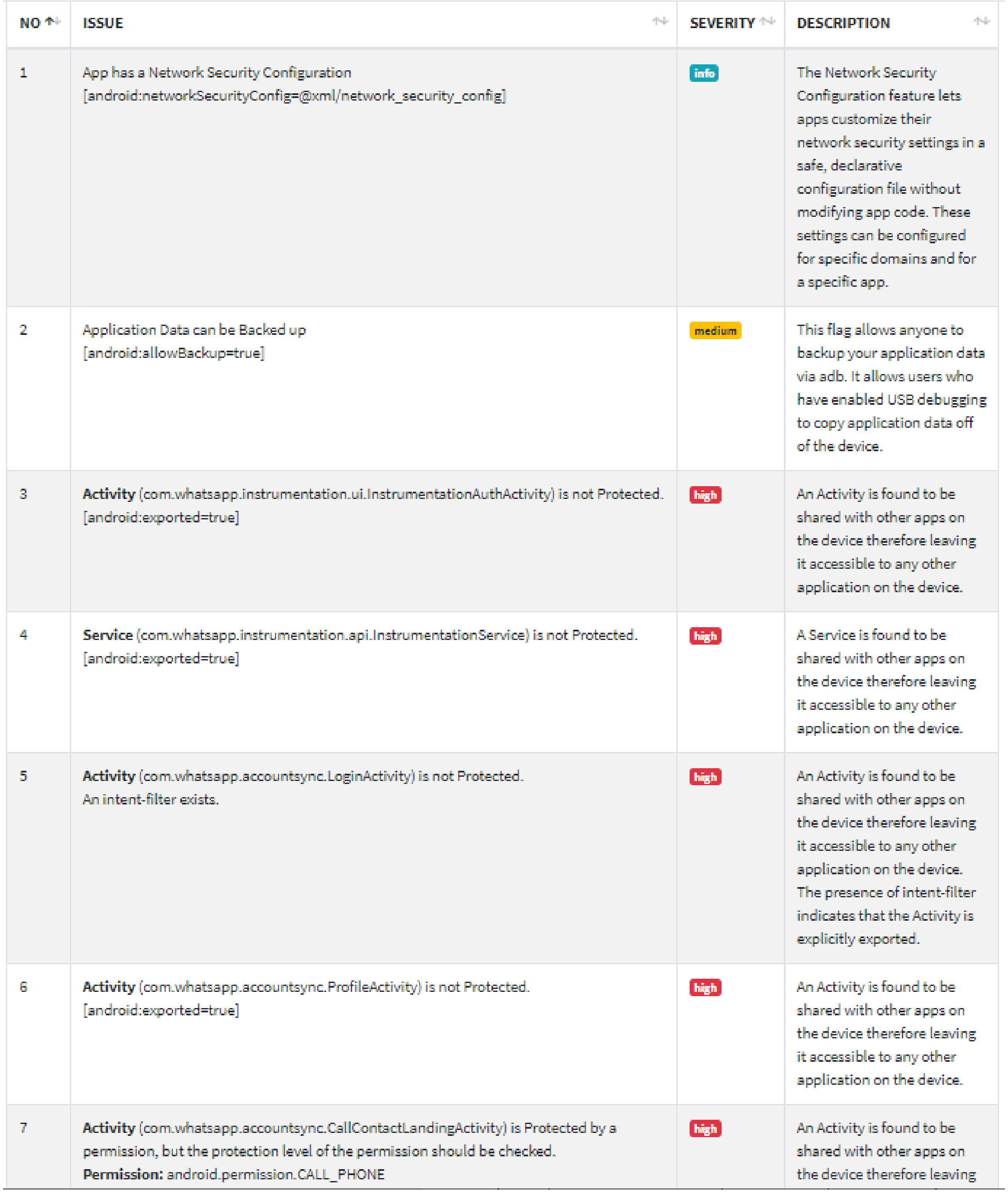
NO	SCOPE	SEVERITY	DESCRIPTION
1	*	high	Base config is insecurely configured to permit clear text traffic to all domains.

Showing 1 to 1 of 1 entries

Clear text is transmission of information that is not encrypted but should be encrypted. This could raise the risk of modification or eavesdropping.

Manifest Analysis

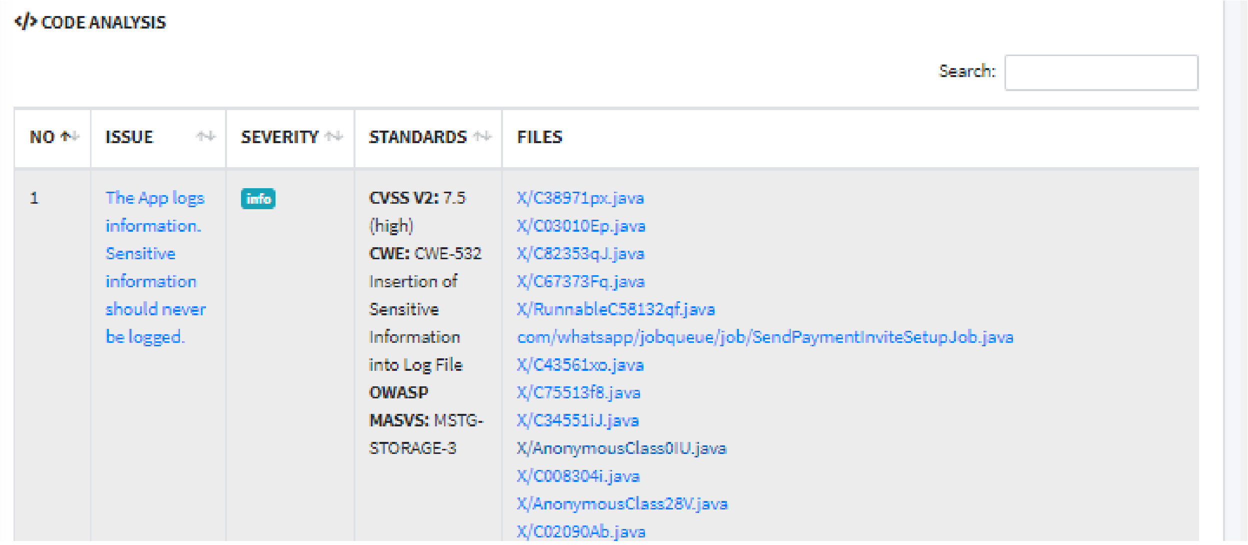
Manifest analysis is used for detecting malware in android by extracting features from the android manifest to create machine learning classifiers and malware detection.



NO	ISSUE	SEVERITY	DESCRIPTION
1	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
2	Application Data can be Backed up [android:allowBackup=true]	medium	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.
3	**Activity** (com.whatsapp.instrumentation.ui.InstrumentationAuthActivity) 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.
4	**Service** (com.whatsapp.instrumentation.api.InstrumentationService) is not Protected. [android:exported=true]	high	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	**Activity** (com.whatsapp.accountsync.LoginActivity) is not Protected. An intent-filter exists.	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. The presence of intent-filter indicates that the Activity is explicitly exported.
6	**Activity** (com.whatsapp.accountsync.ProfileActivity) 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.
7	**Activity** (com.whatsapp.accountsync.CallContactLandingActivity) is Protected by a permission, but the protection level of the permission should be checked. **Permission:** android.permission.CALL_PHONE	high	An Activity is found to be shared with other apps on the device therefore leaving

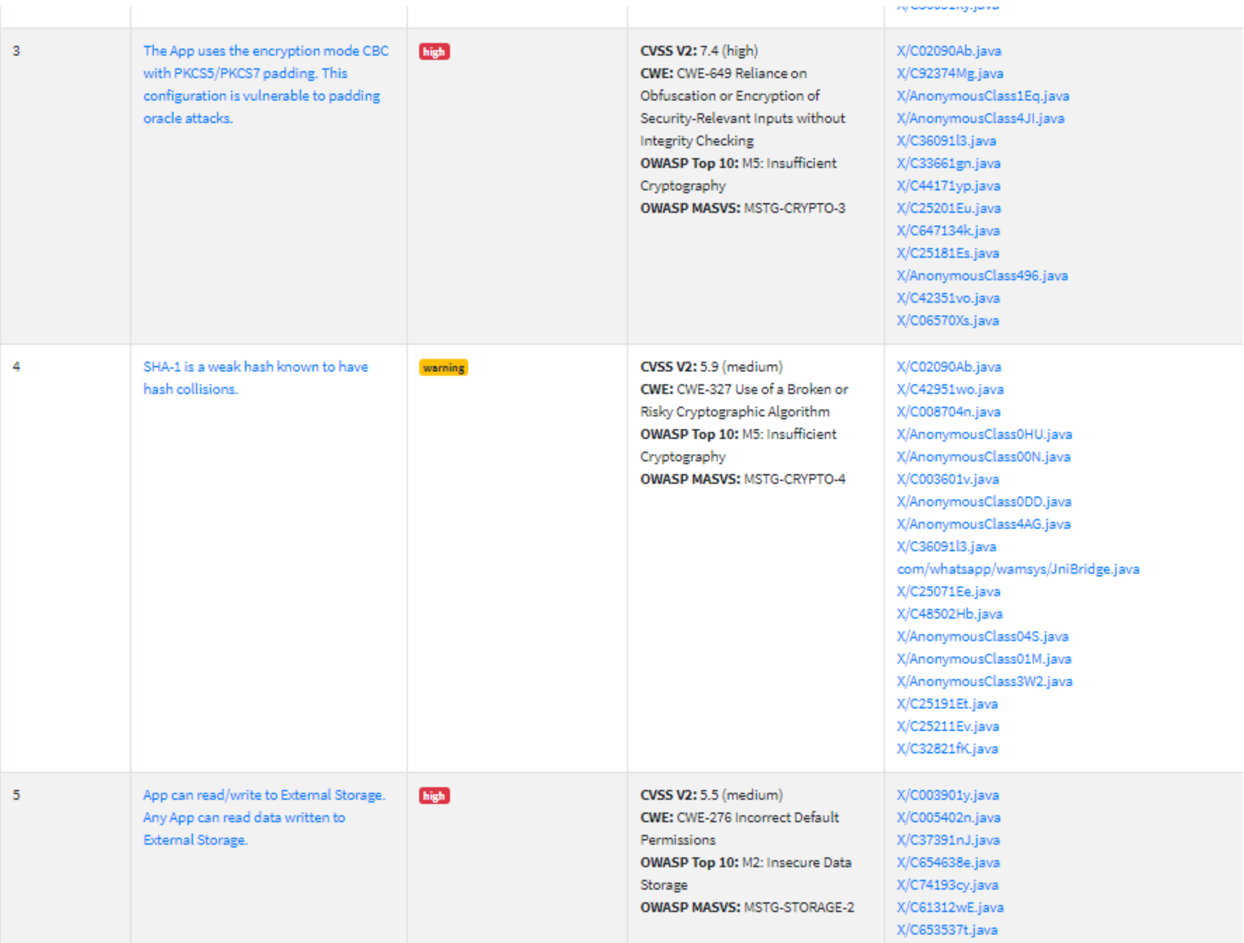
Code Analysis

Code analysis is the analyzation of the code without executing it. The analysis includes vulnerability detection, errors within the code.



</> CODE ANALYSIS

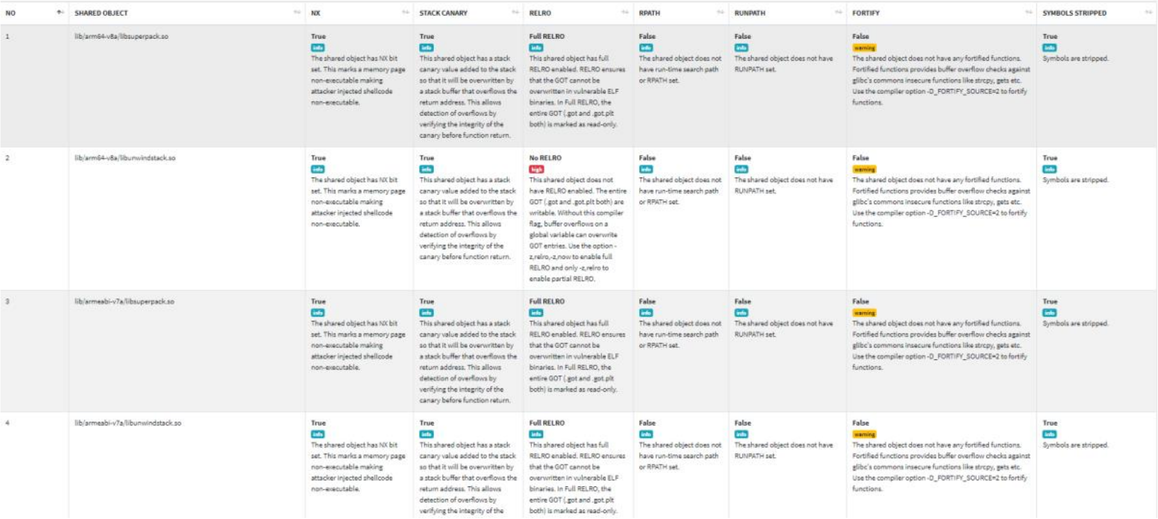
Search:



NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	**CVSS V2:** 7.5 (high) **CWE:** CWE-532 Insertion of Sensitive Information into Log File **OWASP MASVS:** MSTG-STORAGE-3	X/C38971px.java X/C03010Ep.java X/C82353qJ.java X/C67373Fq.java X/RunnableC58132qf.java com/whatsapp/jobqueue/job/SendPaymentInviteSetupJob.java X/C43561xo.java X/C75513f8.java X/C34551iJ.java X/AnonymousClass0IU.java X/C008304i.java X/AnonymousClass28V.java X/C02090Ab.java
3	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	**CVSS V2:** 7.4 (high) **CWE:** CWE-649 Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-3	X/C02090Ab.java X/C92374Mg.java X/AnonymousClass1Eq.java X/AnonymousClass4JI.java X/C36091l3.java X/C33661gn.java X/C44171yp.java X/C25201Eu.java X/C647134k.java X/C25181Es.java X/AnonymousClass496.java X/C42351vo.java X/C06570Xs.java
4	SHA-1 is a weak hash known to have hash collisions.	warning	**CVSS V2:** 5.9 (medium) **CWE:** CWE-327 Use of a Broken or Risky Cryptographic Algorithm **OWASP Top 10:** M5: Insufficient Cryptography **OWASP MASVS:** MSTG-CRYPTO-4	X/C02090Ab.java X/C42951wo.java X/C008704n.java X/AnonymousClass0HU.java X/AnonymousClass00N.java X/C003601v.java X/AnonymousClass0DD.java X/AnonymousClass4AG.java X/C36091l3.java com/whatsapp/wamsys/JniBridge.java X/C25071Ee.java X/C48502Hb.java X/AnonymousClass04S.java X/AnonymousClass01M.java X/AnonymousClass3W2.java X/C25191Et.java X/C25211Ev.java X/C32821fK.java
5	App can read/write to External Storage. Any App can read data written to External Storage.	high	**CVSS V2:** 5.5 (medium) **CWE:** CWE-276 Incorrect Default Permissions **OWASP Top 10:** M2: Insecure Data Storage **OWASP MASVS:** MSTG-STORAGE-2	X/C003901y.java X/C005402n.java X/C37391nJ.java X/C654638e.java X/C74193cy.java X/C61312wE.java X/C653537t.java

Binary Analysis

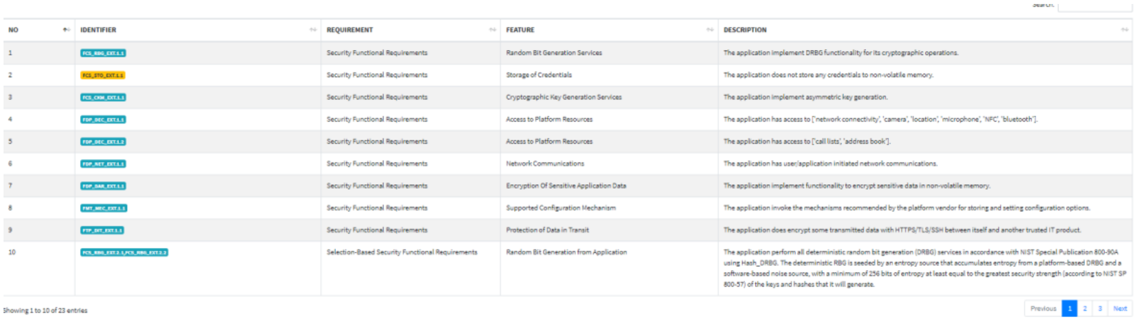
Binary analysis is reviewing codes that are composed of binary code and evaluate the content and structure without accessing the source code. It is used to assess possible vulnerabilities and to perform security audits.



NO	SHARED OBJECT	NX	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	lib/arm64-v8a/libsuperpack.so	**True** info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**True** info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**False** info The shared object does not have run-time search path or RPATH set.	**False** info The shared object does not have RUNPATH set.	**False** warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	**True** info Symbols are stripped.
2	lib/arm64-v8a/libunwindstack.so	**True** info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**True** info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**No RELRO** high This shared object does not have RELRO enabled. The entire GOT (.got and .got.plt both) are writable. Without this compiler flag, buffer overflows on a global variable can overwrite GOT entries. Use the option -z,relro,-z,now to enable full RELRO and only -z,relro to enable partial RELRO.	**False** info The shared object does not have run-time search path or RPATH set.	**False** info The shared object does not have RUNPATH set.	**False** warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	**True** info Symbols are stripped.
3	lib/armeabi-v7a/libsuperpack.so	**True** info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**True** info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**False** info The shared object does not have run-time search path or RPATH set.	**False** info The shared object does not have RUNPATH set.	**False** warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	**True** info Symbols are stripped.
4	lib/armeabi-v7a/libunwindstack.so	**True** info The shared object has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	**True** info This shared object has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the	**Full RELRO** info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	**False** info The shared object does not have run-time search path or RPATH set.	**False** info The shared object does not have RUNPATH set.	**False** warning The shared object does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions.	**True** info Symbols are stripped.

NIAP Analysis

Analyze whether IT products such as mobile applications and software meets the security and guild line standards.

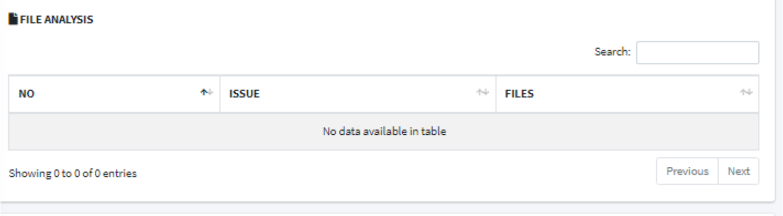


NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION
1	FCS_RBG_EXT.1.1	Security Functional Requirements	Random Bit Generation Services	The application implement DRBG functionality for its cryptographic operations.
2	FCS_STO_EXT.1.1	Security Functional Requirements	Storage of Credentials	The application does not store any credentials to non-volatile memory.
3	FCS_CKM_EXT.1.1	Security Functional Requirements	Cryptographic Key Generation Services	The application implement asymmetric key generation.
4	FDP_DEC_EXT.1.1	Security Functional Requirements	Access to Platform Resources	The application has access to ['network connectivity', 'camera', 'location', 'microphone', 'NFC', 'bluetooth'].
5	FDP_DEC_EXT.1.2	Security Functional Requirements	Access to Platform Resources	The application has access to ['call lists', 'address book'].
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.
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.

Showing 1 to 10 of 23 entries

File Analysis

File analysis: analyze, search, track and report of file metadata and content and enables the organizations to take actions on what files discovered.



FILE ANALYSIS

NO	ISSUE	FILES
No data available in table		

Showing 0 to 0 of 0 entries

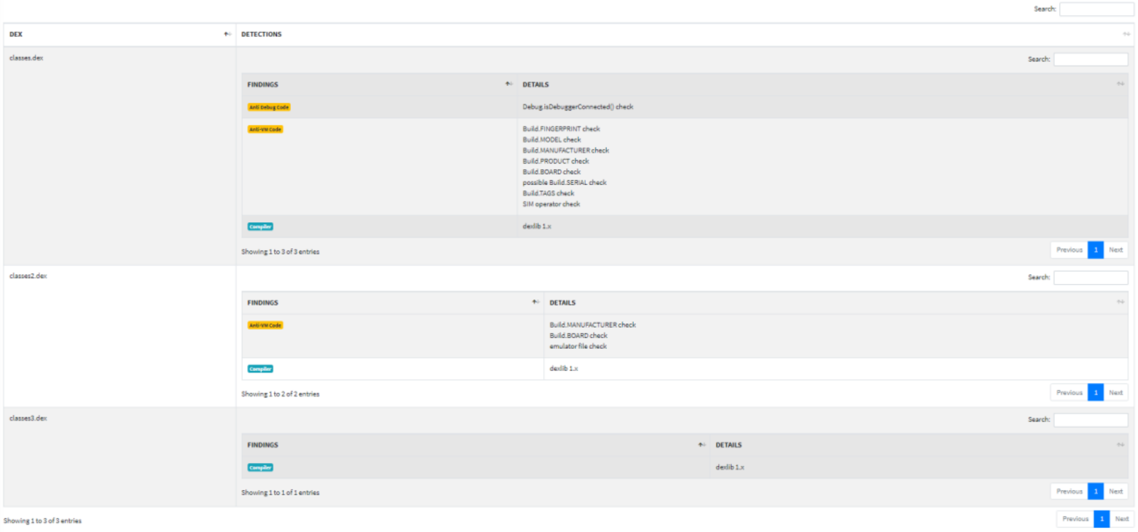
Malware Analysis

Malware analysis have 3 categories:

1. APKiD Analysis
2. Server locations
3. Domain malware check

APKiD Analysis

APKiD gives information regarding how the APK was created. It also identifies compliers, packers and obfuscators.



Search:

DEX | DETECTIONS

classes.dex

Search:

FINDINGS	DETAILS
Anti Debug Code	Debug.isDebuggerConnected() check
Anti-VM Code	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check
Compiler	dexlib 1.x

Showing 1 to 3 of 3 entries

classes2.dex

Search:

FINDINGS	DETAILS
Anti-VM Code	Build.MANUFACTURER check Build.BOARD check emulator file check
Compiler	dexlib 1.x

Showing 1 to 2 of 2 entries

classes3.dex

Search:

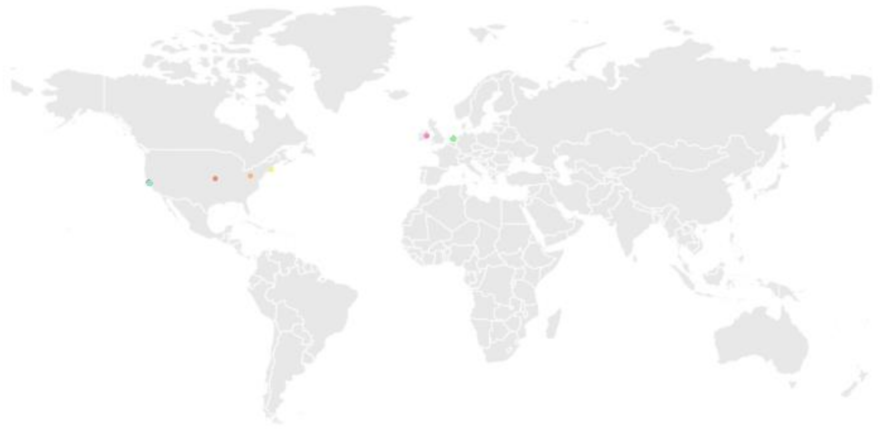
FINDINGS	DETAILS
Compiler	dexlib 1.x

Showing 1 to 1 of 1 entries

Showing 1 to 3 of 3 entries

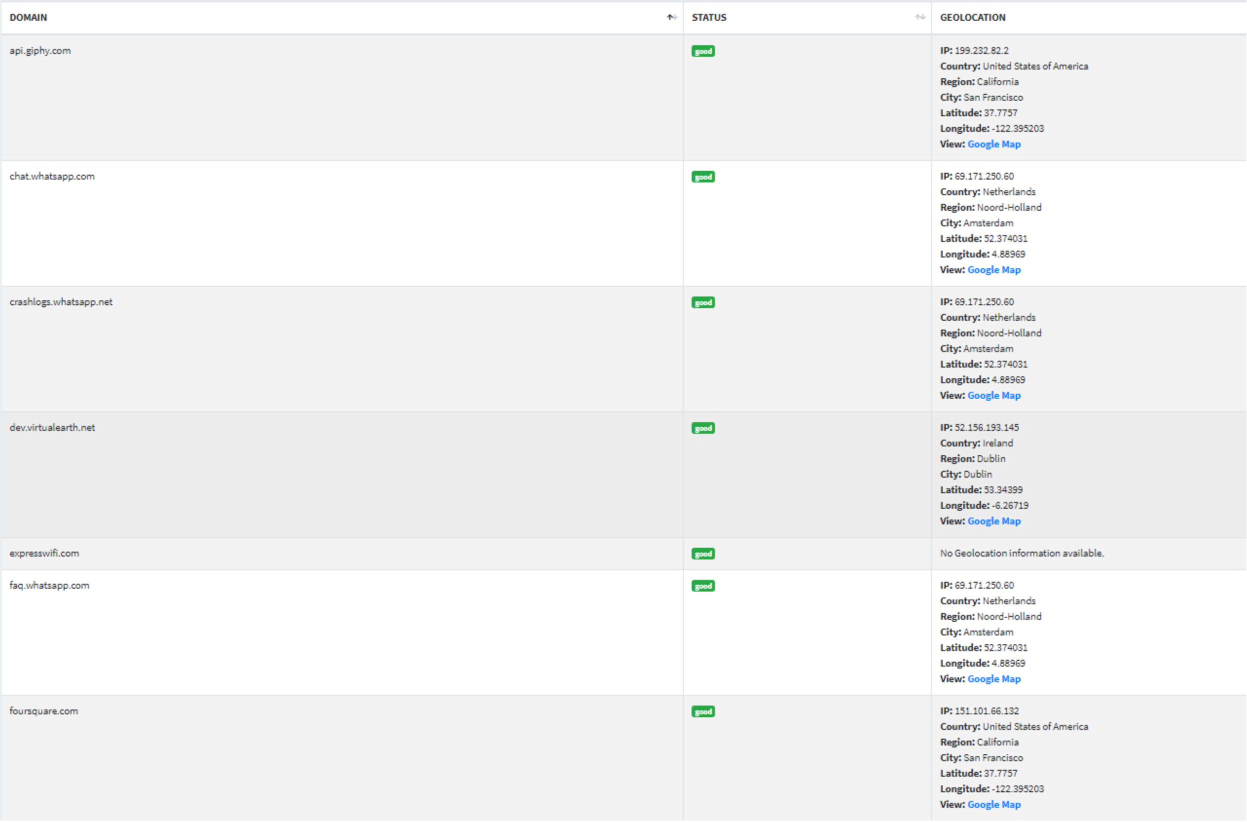
Server Locations

Server locations is whether the data is hosted.

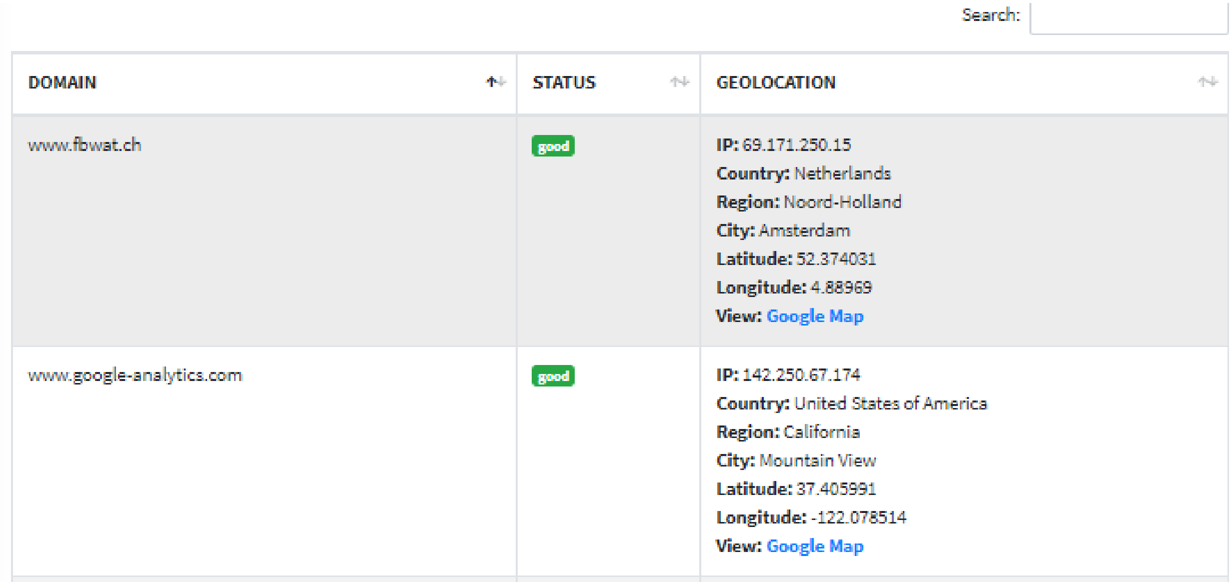


Domain Malware Check

Scan domain names to check any presence of malware recoded on connected security databases.



DOMAIN	STATUS	GEOLOCATION
api.giphy.com	good	**IP:** 199.232.82.2 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map
chat.whatsapp.com	good	**IP:** 69.171.250.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.88969 **View:** Google Map
crashlogs.whatsapp.net	good	**IP:** 69.171.250.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.88969 **View:** Google Map
dev.virtualearth.net	good	**IP:** 52.156.193.145 **Country:** Ireland **Region:** Dublin **City:** Dublin **Latitude:** 53.34399 **Longitude:** -6.26719 **View:** Google Map
expresswifi.com	good	No Geolocation information available.
faq.whatsapp.com	good	**IP:** 69.171.250.60 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.88969 **View:** Google Map
foursquare.com	good	**IP:** 151.101.66.132 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.7757 **Longitude:** -122.395203 **View:** Google Map



Search:

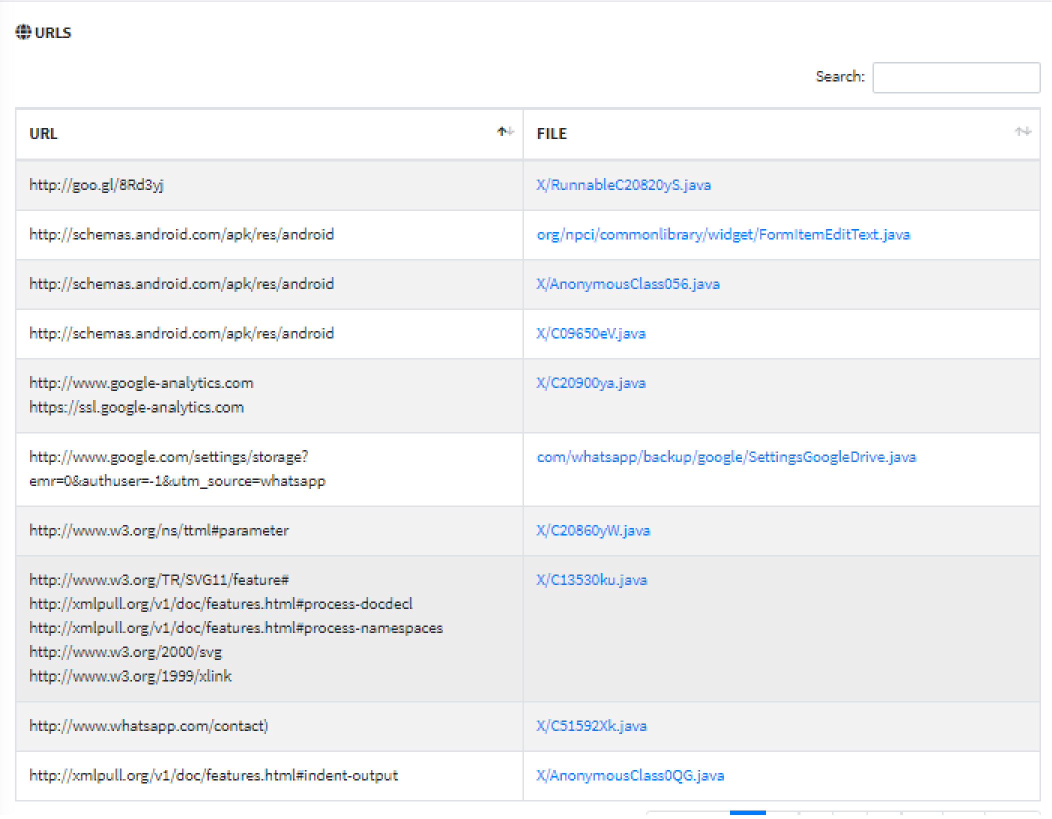
DOMAIN	STATUS	GEOLOCATION
www.fbwat.ch	good	**IP:** 69.171.250.15 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.88969 **View:** Google Map
www.google-analytics.com	good	**IP:** 142.250.67.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

Reconnaissance

Reconnaissance is the gathering of information of the targeted software. The found information will be used to determine weaknesses and security vulnerabilities of the software.

MobSF uses 5 ways to perform reconnaissance:

1. URLs

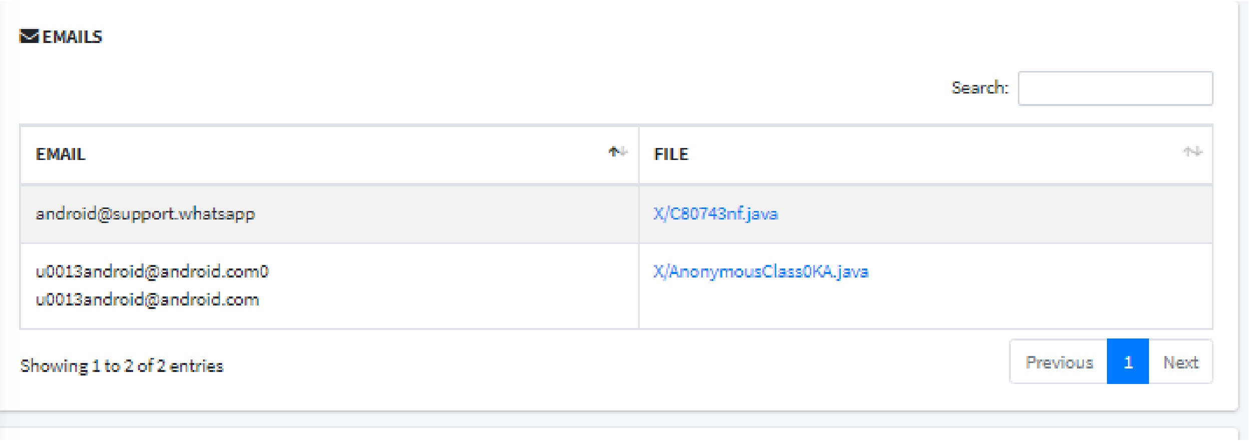


URLS

Search:

URL	FILE
http://goo.gl/8Rd3yj	X/RunnableC20820yS.java
http://schemas.android.com/apk/res/android	org/npci/commonlibrary/widget/FormItemEditText.java
http://schemas.android.com/apk/res/android	X/AnonymousClass056.java
http://schemas.android.com/apk/res/android	X/C09650eV.java
http://www.google-analytics.com https://ssl.google-analytics.com	X/C20900ya.java
http://www.google.com/settings/storage?emr=0&authuser=-1&utm_source=whatsapp	com/whatsapp/backup/google/SettingsGoogleDrive.java
http://www.w3.org/ns/ttml#parameter	X/C20860yW.java
http://www.w3.org/TR/SVG11/feature# http://xmlpull.org/v1/doc/features.html#process-docdecl http://xmlpull.org/v1/doc/features.html#process-namespaces http://www.w3.org/2000/svg http://www.w3.org/1999/xlink	X/C13530ku.java
http://www.whatsapp.com/contact)	X/C51592Xk.java
http://xmlpull.org/v1/doc/features.html#indent-output	X/AnonymousClass0QG.java

2. Emails



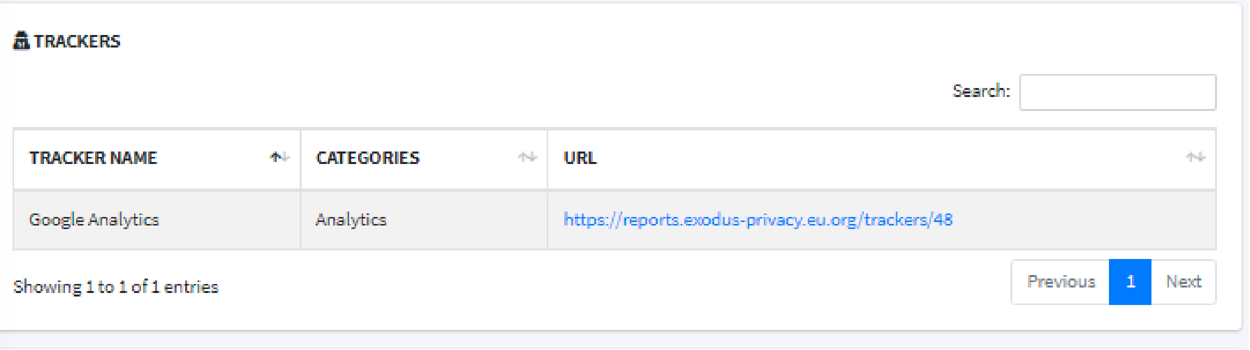
EMAILS

Search:

EMAIL	FILE
android@support.whatsapp	X/C80743nf.java
u0013android@android.com0 u0013android@android.com	X/AnonymousClass0KA.java

Showing 1 to 2 of 2 entries

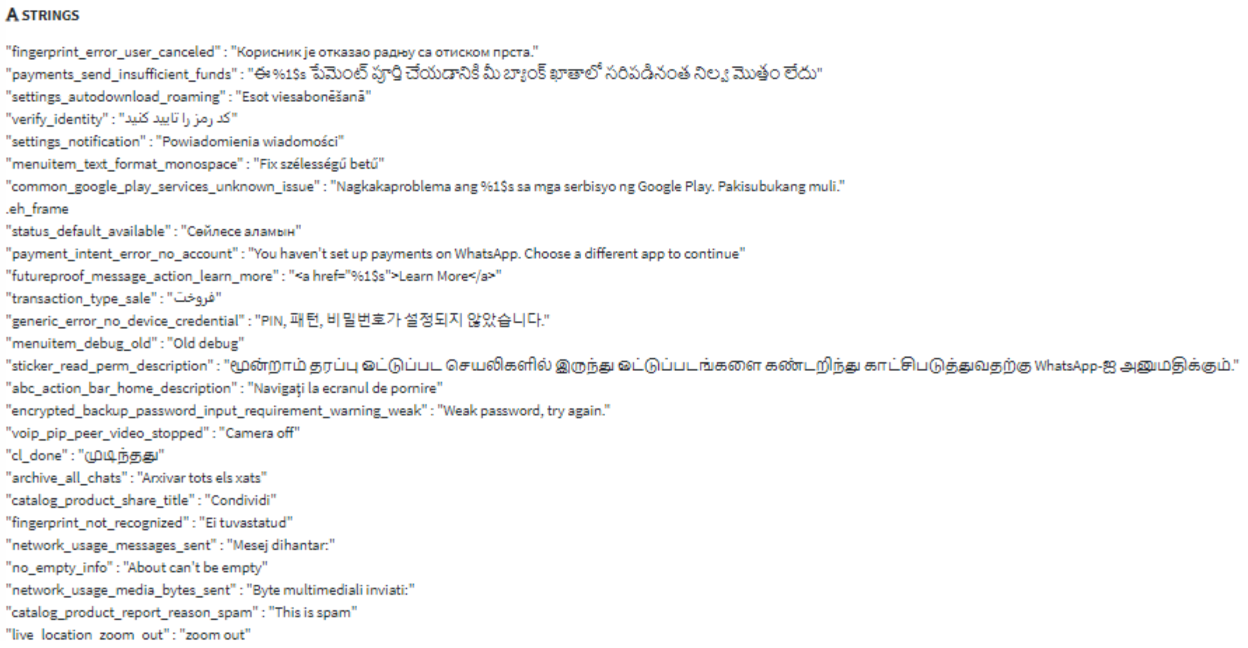
3. Trackers



TRACKER NAME	CATEGORIES	URL
Google Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/48

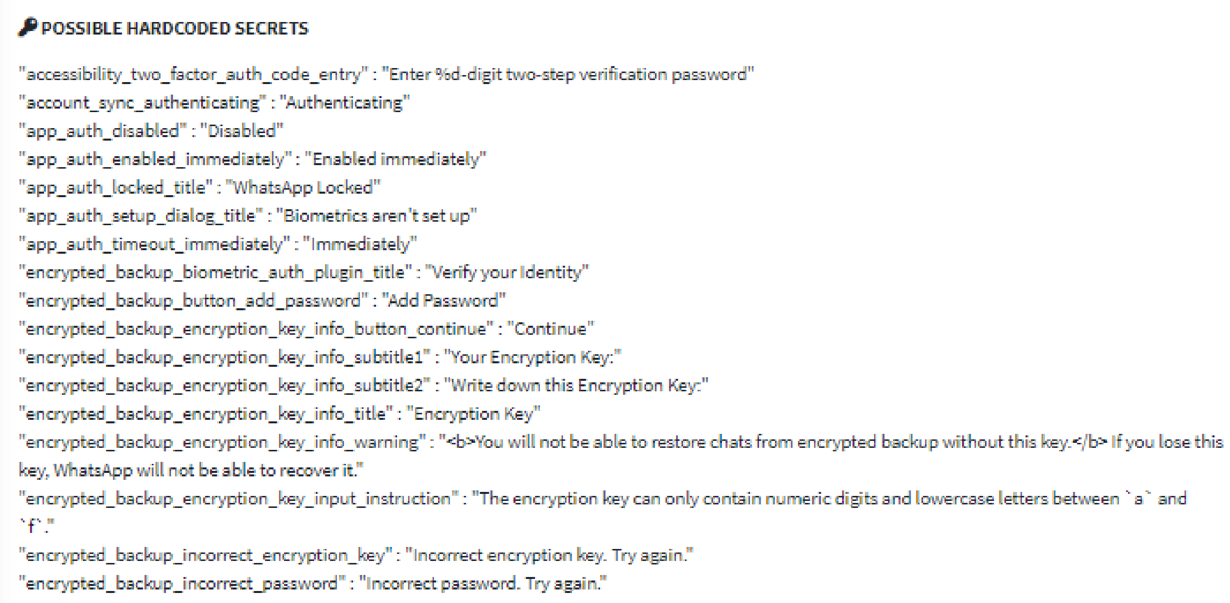
Showing 1 to 1 of 1 entries

4. Strings



"fingerprint_error_user_canceled" : "Корисник је отказао радњу са отиском прста."
"payments_send_insufficient_funds" : "ఈ %1$s పేమెంట్ పూర్తి చేయడానికి మీ బ్యాంక్ ఖాతాలో సరిపడినంత నిల్వ మొత్తం లేదు"
"settings_autodownload_roaming" : "Esot viesabonēšanā"
"verify_identity" : "کد رمز را تایید کنید"
"settings_notification" : "Powiadomienia wiadomości"
"menuitem_text_format_monospace" : "Fix szélességű betű"
"common_google_play_services_unknown_issue" : "Nagkakaproblema ang %1$s sa mga serbisyo ng Google Play. Pakisubukang muli."
.eh_frame
"status_default_available" : "Сөйлесе аламын"
"payment_intent_error_no_account" : "You haven't set up payments on WhatsApp. Choose a different app to continue"
"futureproof_message_action_learn_more" : "<a href="%1$s">Learn More</a>"
"transaction_type_sale" : "فروخت"
"generic_error_no_device_credential" : "PIN, 패턴, 비밀번호가 설정되지 않았습니다."
"menuitem_debug_old" : "Old debug"
"sticker_read_perm_description" : "மூன்றாம் தரப்பு ஒட்டுப்பட செயலிகளில் இருந்து ஒட்டுப்படங்களை கண்டறிந்து காட்சிபடுத்துவதற்கு WhatsApp-ஐ அனுமதிக்கும்."
"abc_action_bar_home_description" : "Navigaţi la ecranul de pornire"
"encrypted_backup_password_input_requirement_warning_weak" : "Weak password, try again."
"voip_pip_peer_video_stopped" : "Camera off"
"cl_done" : "முடிந்தது"
"archive_all_chats" : "Arxivar tots els xats"
"catalog_product_share_title" : "Condividi"
"fingerprint_not_recognized" : "Ei tuvastatud"
"network_usage_messages_sent" : "Mesej dihantar:"
"no_empty_info" : "About can't be empty"
"network_usage_media_bytes_sent" : "Byte multimediali inviati:"
"catalog_product_report_reason_spam" : "This is spam"
"live location zoom out" : "zoom out"

5. Hardcoded Secrets



POSSIBLE HARDCODED SECRETS

```
"accessibility_two_factor_auth_code_entry" : "Enter %d-digit two-step verification password"
"account_sync_authenticating" : "Authenticating"
"app_auth_disabled" : "Disabled"
"app_auth_enabled_immediately" : "Enabled immediately"
"app_auth_locked_title" : "WhatsApp Locked"
"app_auth_setup_dialog_title" : "Biometrics aren't set up"
"app_auth_timeout_immediately" : "Immediately"
"encrypted_backup_biometric_auth_plugin_title" : "Verify your Identity"
"encrypted_backup_button_add_password" : "Add Password"
"encrypted_backup_encryption_key_info_button_continue" : "Continue"
"encrypted_backup_encryption_key_info_subtitle1" : "Your Encryption Key:"
"encrypted_backup_encryption_key_info_subtitle2" : "Write down this Encryption Key:"
"encrypted_backup_encryption_key_info_title" : "Encryption Key"
"encrypted_backup_encryption_key_info_warning" : "<b>You will not be able to restore chats from encrypted backup without this key.</b> If you lose this key, WhatsApp will not be able to recover it."
"encrypted_backup_encryption_key_input_instruction" : "The encryption key can only contain numeric digits and lowercase letters between `a` and `f`."
"encrypted_backup_incorrect_encryption_key" : "Incorrect encryption key. Try again."
"encrypted_backup_incorrect_password" : "Incorrect password. Try again."
```

Part 2

Decentralized Application

The world that we live in has become a massive connection of networks. Everyone is interconnected with anyone and all these connections are connected to a single center, the server. Facebook and google are great examples of a centralized system. Nevertheless, if one connection fails, the entire network breaks and malfunction. However, this was not always a problem. During the early development stage of world wide web or the internet, the implemented concept known as decentralized systems where there is no central point of authority and as a result even if one node fails, the connection still stands. Bitcoin, Ethereum are the best sample to take into consideration (which is also a distributed system) where each user holds a copy of the data and if one node goes down, the network will be able to operate due to its decentralized nature.

A Dapp must have the following characteristics:

1. Open-source – The source code should be available to all and it must run autonomously and there must be no controlling of tokens by a single entity and adapt fast to feedback and system responses.

2. Decentralized – use cryptography to record and store data and utilize a decentralized blockchain to avoid a node becoming centralized.

3. Incentivize – the users of the application should be rewarded using a cryptographic currency such as bitcoins.

4. Protocol – the users must agree on an algorithm to show the proof of value, bitcoin – proof of work algorithm.

Therefore, it can be seen that a Dapp is an open-source software that utilizes a decentralized blockchain that rewards and energize themselves by a currency that is produced using an algorithm.

IPFS (Inter Planetary File System) is a hypermedia distribution protocol that uses peer to peer method to store and generates content-addresses instead of IP addresses and uses. The content is constantly being copied with the network which makes it harder to take down. Unlike in HTTP the applications/systems are not centralized and as a result cyber attacks such as DDos attacks will not be able take down the network.

The future of decentralized applications is based on more autonomously operating systems where human vulnerability is completely eliminated from the network. The applications will be fast adaptive to the changes due to its artificial intelligence sector and be more reliable with human entity is gone from monitoring edge to the consumer edge completely.

Case Scenario

Election Dapp for Presidential Election Voting System

The traditional voting method is slowly becoming incompatible with today's day and age. The reasons are that:

1. Voters can not go to voting centers due to personal issues (transportation, illness, etc.)
2. Global pandemics
3. The current voting systems could easily be rigged due to intentional human intervention or human error

As a result of the above reasons, the future of the election system should be adapted to the current situations of the world. An Election Dapp is a great step to start this process. The voters have to pre-register through the open-source app using information such as full name, date of birth, Social Security/National ID Number, permanent address and current living address and will face a biometric scan through their smart phone. Once the data is process at the Election Commission, the eligible voters would receive a verification message with details regarding the election. All voters' data will be stored in a cryptographic manner.

The voters biometrics will be scanned and they will have to input Social Security Number and full name at the security check in order or them to go to the voting page and voters are only allowed to choose one representative and if they wish to not choose any, they can select the check box that states "I do not wish to use my vote" and once the check box is ticked the Dapp will automatically close. The voters who participated will receive a bitcoin value as a reward for voting and all the election votes will go to a safe storage where it is analyzed by an AI interface. The results can not be viewed until all the votes are calculated and displayed by the AI.

(Assumption: no errors will occur during the time)