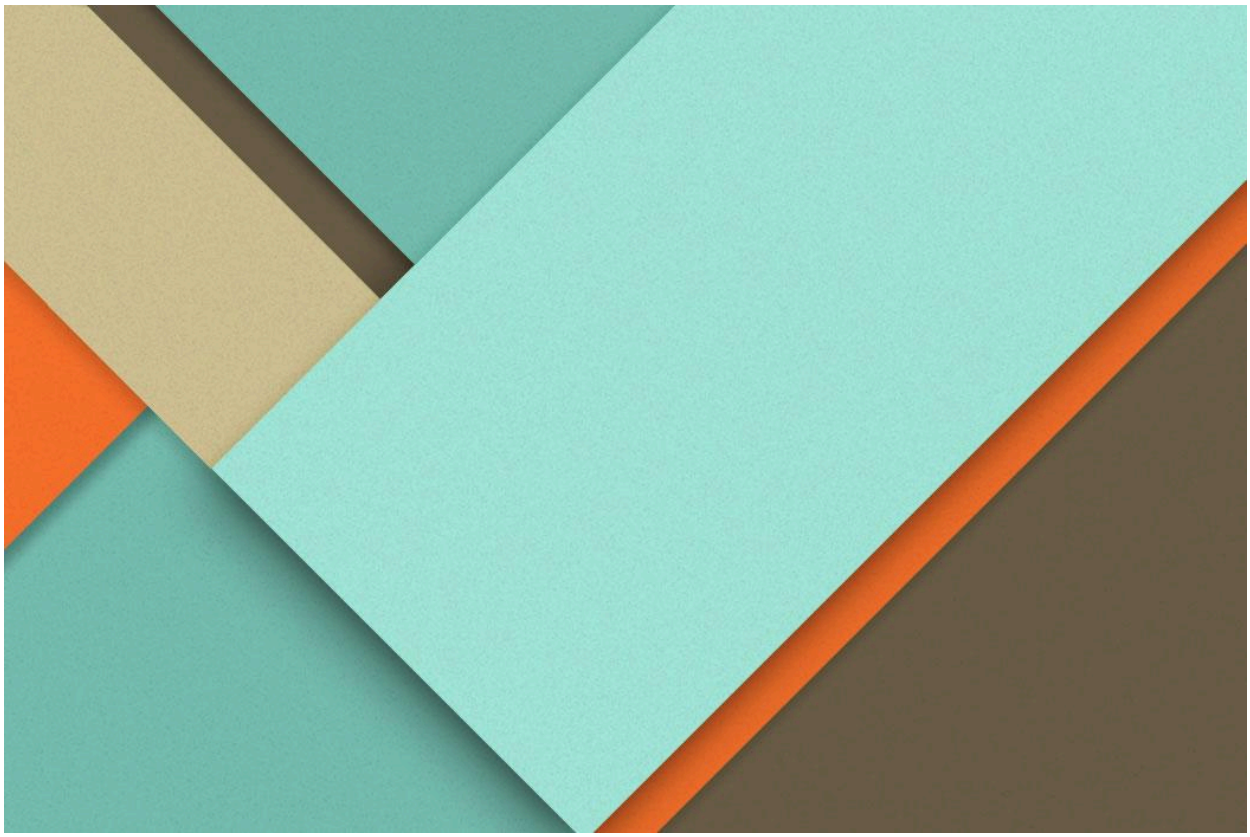
Tania Jaswal

CS 453

May 8, 2024



Mini For Facebook App Testing

Tania Jaswal

Table of Contents

Overview

The penetration testing of Mini for Facebook was conducted within the Android environment to comprehensively assess its security posture. Utilizing methodologies outlined in the OWASP Mobile Application Security Verification Standard (MASVS), our analysis aimed to identify vulnerabilities that could compromise user data and overall system integrity. The findings presented in this report offer a detailed examination of Mini for Facebook's security across various categories, revealing both strengths and weaknesses in its security measures. These insights provide valuable guidance for enhancing user privacy and data protection within the application.

What is Mini for Facebook?

Mini for Facebook is a lightweight mobile application designed to provide users with a streamlined and efficient way to access the Facebook platform on their mobile devices. Developed as a companion app to the full-fledged Facebook application, Mini for Facebook offers essential features for browsing the social media platform while consuming minimal system resources and data bandwidth.

The app is optimized for performance, offering a simplified user interface that prioritizes essential functionalities such as news feed browsing, posting updates, messaging, and interacting with friends' content. Mini for Facebook aims to deliver a fast and responsive user experience, catering to users who seek a lightweight alternative to the resource-intensive official Facebook app.

Why OWASP Testing?

OWASP provides a standardized framework for evaluating the security of web applications, including mobile apps. By subjecting Mini for Facebook to OWASP testing, we aim to achieve several objectives:

1. **Identifying Vulnerabilities:** OWASP testing helps uncover security vulnerabilities or weaknesses present in the Mini for Facebook app. This includes vulnerabilities related to data storage, cryptography, authentication, network communication, platform interaction, code quality, and resilience requirements.
2. **Mitigating Risks:** By identifying vulnerabilities early, we can proactively mitigate security risks associated with Mini for Facebook. This involves implementing necessary security controls, patches, and fixes to address identified vulnerabilities and strengthen the overall security posture of the application.
3. **Protecting User Data:** Mini for Facebook likely handles sensitive user data, including personal information, login credentials, and communication data. Ensuring the security of this data is crucial to protecting user privacy and preventing data breaches. OWASP testing helps identify and address vulnerabilities that could compromise the confidentiality, integrity, or availability of user data.
4. **Enhancing Trust and Confidence:** A secure application fosters trust and confidence among users, demonstrating a commitment to protecting their privacy and security. By subjecting Mini for Facebook to rigorous security testing and implementing necessary security measures, we can instill trust in users and reassure them that their data is being handled securely.
5. **Compliance Requirements:** Compliance with industry regulations and standards is essential for organizations handling user data. OWASP testing helps ensure that Mini for Facebook complies with relevant security standards and regulations, reducing the risk of non-compliance penalties and legal repercussions.

Overview of OWASP Testing

OWASP (Open Web Application Security Project) testing refers to a comprehensive assessment of web applications to identify and mitigate potential security vulnerabilities. The OWASP project provides a standardized methodology and checklist for evaluating the security posture of web applications, ensuring they adhere to best practices and guidelines for secure development.

The testing process involves examining various aspects of the web application, including its storage mechanisms, cryptography implementations, authentication mechanisms, network communication protocols, platform interactions, code quality, build settings, and resilience to common security threats. Each aspect is evaluated against the requirements outlined in the OWASP Mobile Application Security Verification Standard (MASVS), which provides a set of criteria for assessing the security of mobile applications.

The key components of OWASP testing:

1. **Storage Testing:** Evaluates how the application handles sensitive data storage, including proper encryption, secure storage mechanisms, and protection against unauthorized access.
2. **Cryptography Testing:** Assesses the implementation of cryptographic algorithms and protocols within the application to ensure the confidentiality, integrity, and authenticity of data.
3. **Authentication Testing:** Verifies the effectiveness of the application's authentication mechanisms in preventing unauthorized access to sensitive resources and user accounts.
4. **Network Communication Testing:** Examines the security of network communication protocols used by the application to transmit data, ensuring encryption, integrity protection, and protection against common network-based attacks.
5. **Platform Interaction Testing:** Reviews how the application interacts with the underlying mobile platform, including permissions, data sharing, and integration with device features such as GPS, camera, and contacts.
6. **Code Quality and Build Settings Testing:** Analyzes the source code of the application for security vulnerabilities, coding errors, and misconfigurations, as well as ensuring secure build settings to prevent potential exploitation.
7. **Resilience Requirements Testing:** Tests the application's resilience to common security threats such as injection attacks, cross-site scripting (XSS), cross-site request forgery (CSRF), and insecure direct object references (IDOR).
8. **App Privacy Testing:** App privacy testing assesses how the application collects, uses, and protects user data, ensuring compliance with privacy regulations and best practices. It involves evaluating privacy policies, data collection practices, user controls, and security measures to safeguard user privacy and prevent unauthorized access or misuse of personal information.

MASVS Storage Testing

MASVS-STORAGE-1

MASVS-STORAGE-1 stipulates that the app securely stores sensitive data, protecting against unauthorized access or tampering. This criterion underscores the need for robust security measures to maintain the confidentiality and integrity of user information, both locally and remotely. The app demonstrates a commitment to data security and user privacy by complying with this standard.

Testing Conducted for the Storage Testing:

1. These are the internal and external local storage created by the application-

```
[emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cd ..
[emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook # ls
 app_textures  app_webview  cache  databases  files  shared_prefs
```

Shared_prefs- This directory is used to store application preference information in Android ASCII or binary XML files.

Files- The files directory is used by the app to store arbitrary file data used for the application.

Cache- This temporary storage location is used by the app within the sandbox.

Databases- This is used for storage of most local app data in SQLite databases.

Findings under Cache directory-

The cache directory of the app reveals a typical structure with WebView, afwad, and picasso-cache folders. The Picasso-cache folder stores HTTP responses, suggesting the caching of fetched URLs, while the WebView folder seems to contain various cache data related to the web view, including crash reports, safe browsing data, and font information.

```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/cache # ls
WebView  afwad  picasso-cache
```

```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/cache/picasso-cache # ls
2646f0ed0f2d404742f20510bdab8192.0  a00a684f37a62b6e153d2e9aeceb37e5.1
2646f0ed0f2d404742f20510bdab8192.1  journal
a00a684f37a62b6e153d2e9aeceb37e5.0
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/cache/picasso-cache # cat 2646f0ed0f2d404742f20510bdab8192.0
http://crl3.digicert.com/CloudflareIncECCCA-3.crl
GET
0
HTTP/1.1 200 OK
13
Accept-Ranges: bytes
Age: 3590
Cache-Control: max-age=7200, public
Content-Type: application/pkix-crl
Date: Sun, 21 Apr 2024 21:53:04 GMT
Etag: "6624cb07-173"
Expires: Sun, 21 Apr 2024 23:53:04 GMT
Last-Modified: Sun, 21 Apr 2024 08:15:03 GMT
Server: ECAcc (sac/255C)
X-Cache: HIT
Content-Length: 371
X-Android-Sent-Millis: 1712279196800
X-Android-Received-Millis: 1712279196827
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/cache/picasso-cache # cat journal
libcore.io.DiskLruCache
1
201105
2

DIRTY 2646f0ed0f2d404742f20510bdab8192
CLEAN 2646f0ed0f2d404742f20510bdab8192 454 371
DIRTY a00a684f37a62b6e153d2e9aeceb37e5
CLEAN a00a684f37a62b6e153d2e9aeceb37e5 453 371
```

Findings under Database directory-

The examination of SQLite databases extracted from "Gold_Finger.V.X.your_Facebook" reveals a structured schema comprising tables like alarms, composite_measurement_sessions, measurements, reports, routines, sending, and speed. Each table appears to house diverse datasets, encompassing alarm configurations, composite measurement sessions, network measurements, sentiment analysis reports, event routines, sending-related activities, and speed measurements. However, due to the app's non-debuggable nature, extraction into a SQLite database viewer is unfeasible. Despite this, no sensitive information appears to be stored within the tables. It's noteworthy that the SQLite database lacks encryption, as evidenced by its accessibility through cat commands.

```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/databases # cat composite_measurement_sessions
SQLite format 3@  .(h.4
??

?P++Ytablesqlite_sequencesqlite_sequenceCREATE TABLE sqlite_sequence(name,seq)II??tablecomposite_measurement_sessionscomposite_measurement_sessionsCREATE TAB
LE composite_measurement_sessions (_id INTEGER PRIMARY KEY AUTOINCREMENT,APP_VRS_CODE TEXT,DC_VRS_CODE TEXT,DB_VRS_CODE TEXT,ANDROID_VRS TEXT,ANDROID_SDK INT
EGER,NAME TEXT,SESSION_INTERRUPTED NUMERIC, TIME_a INTEGER,TIME_b INTEGER,LOC_ACCURACY_a REAL,LOC_ACCURACY_b REAL,LOC_AGE_a INTEGER,LOC_AGE_b INTEGER,ALTITUD
E_a REAL,ALTITUDE_b REAL,LOC_BEARING_a REAL,LOC_BEARING_b REAL,LOC_SPEED_a REAL,LOC_SPEED_b REAL,LATITUDE_a REAL,LATITUDE_b REAL,LONGITUDE_a REAL,LONGITUDE_b
 REAL,LOC_PROVIDER_a TEXT,LOC_PROVIDER_b TEXT,LOC_SAT_a INTEGER,LOC_SAT_b INTEGER,LOC_ENABLED_a NUMERIC,LOC_ENABLED_b NUMERIC,LOC_MOCKING_ENABLED_a NUMERIC,L
OC_MOCKING_ENABLED_b NUMERIC,SCREEN_ON_a NUMERIC,SCREEN_ON_b NUMERIC,SCREEN_LOCKED_a NUMERIC,SCREEN_LOCKED_b NUMERIC,CDMA_DBM_a INTEGER,CDMA_DBM_b INTEGER,CD
MA_ECIO_a INTEGER,CDMA_ECIO_b INTEGER,EVDO_DBM_a INTEGER,EVDO_DBM_b INTEGER,EVDO_ECIO_a INTEGER,EVDO_ECIO_b INTEGER,EVDO_SNR_a INTEGER,EVDO_SNR_b INTEGER,GSM
_BIT_ERROR_RATE_a INTEGER,GSM_BIT_ERROR_RATE_b INTEGER,GSM_SIGNAL_STRENGTH_a INTEGER,GSM_SIGNAL_STRENGTH_b INTEGER,LTE_RSRP_a INTEGER,LTE_RW--ctableandroid_m
_CENTER_FQ_0_a INTEGER,WF_CENTER_FQ_0_b INTEGER,WF_CENTER_FQ_1_a INTEGER,WF_CENTER_FQ_1_b INTEGER,WF_CHANNEL_WD_a INTEGER,WF_CHANNEL_WD_b INTEGER,WF_FQ_a INT
EGER,WF_FQ_b INTEGER,WF_80211MC_a NUMERIC,WF_80211MC_b NUMERIC,WF_PASSPOINT_a NUMERIC,WF_PASSPOINT_b NUMERIC,WF_LEVEL_a INTEGER,WF_LEVEL_b INTEGER,WF_OPERATO
R_NAME_a TEXT,WF_OPERATOR_NAME_b TEXT,WF_VENUE_NAME_a TEXT,WF_VENUE_NAME_b TEXT,WF_SCAN_AGE_a INTEGER,WF_SCAN_AGE_b INTEGER,NETWORK_CONNECTION_TYPE_a INTEGER
,NETWORK_CONNECTION_TYPE_b INTEGER,WIFI_ON_a NUMERIC,WIFI_ON_b NUMERIC,PRESSURE_a REAL,PRESSURE_b REAL,PRESSURE_ACC_a INTEGER,PRESSURE_ACC_b INTEGER,LIGHT_a
REAL,LIGHT_b REAL,LIGHT_ACC_a INTEGER,LIGHT_ACC_b INTEGER,HUMIDITY_a REAL,HUMIDITY_b REAL,HUMIDITY_ACC_a INTEGER,HUMIDITY_ACC_b INTEGER,TEMPERATURE_a REAL,TE
MPERATURE_b REAL,TEMPERATURE_ACC_a INTEGER,TEMPERATURE_ACC_b INTEGER,BT_LEVEL_a INTEGER,BT_LEVEL_b INTEGER,BT_SCALE_a INTEGER,BT_SCALE_b INTEGER,BT_HEALTH_a
INTEGER,BT_HEALTH_b INTEGER,BT_PLUGGED_a INTEGER,BT_PLUGGED_b INTEGER,BT_STATUS_a INTEGER,BT_STATUS_b INTEGER,BT_TECH_a TEXT,BT_TECH_b TEXT,BT_TEMP_a INTEGER
,BT_TEMP_b INTEGER,BT_VOLT_a INTEGER,BT_VOLT_b INTEGER,BT_PRESENT_a NUMERIC,BT_PRESENT_b NUMERIC,SIG_MOTION_OCC_a NUMERIC,SIG_MOTION_OCC_b NUMERIC,SIG_MOTION
_DETECT_DUR_a INTEGER,SIG_MOTION_DETECT_DUR_b INTEGER,STEP_OCC_a NUMERIC,STEP_OCC_b NUMERIC,STEP_DETECT_DUR_a INTEGER,STEP_DETECT_DUR_b INTEGER,AZIMUTH_a REA
L,AZIMUTH_b REAL,PITCH_a REAL,PITCH_b REAL,ROLL_a REAL,ROLL_b REAL,DT_DELTA_TX_BYTES_WIFI_a INTEGER,DT_DELTA_TX_BYTES_WIFI_b INTEGER,DT_DELTA_RX_BYTES_WIFI_a
 INTEGER,DT_DELTA_RX_BYTES_WIFI_b INTEGER,DT_DELTA_TX_BYTES_CELL_a INTEGER,DT_DELTA_TX_BYTES_CELL_b INTEGER,DT_DELTA_RX_BYTES_CELL_a INTEGER,DT_DELTA_RX_BYTE
S_CELL_b INTEGER,DT_TOT_TX_BYTES_WIFI_a INTEGER,DT_TOT_TX_BYTES_WIFI_b INTEGER,DT_TOT_RX_BYTES_WIFI_a INTEGER,DT_TOT_RX_BYTES_WIFI_b INTEGER,DT_TOT_TX_BYTES_
CELL_a INTEGER,DT_TOT_TX_BYTES_CELL_b INTEGER,DT_TOT_RX_BYTES_CELL_a INTEGER,DT_TOT_RX_BYTES_CELL_b INTEGER,DT_DELTA_INTERVAL_a INTEGER,DT_DELTA_INTERVAL_b I
NTEGER,DT_DELTA_TX_DROPS_WIFI_a INTEGER,DT_DELTA_TX_DROPS_WIFI_b INTEGER,DT_DELTA_TX_PACKETS_WIFI_a INTEGER,DT_DELTA_TX_PACKETS_WIFI_b INTEGER,DT_DELTA_TX_DR
OPS_CELL_a INTEGER,DT_DELTA_TX_DROPS_CELL_b INTEGER,DT_DELTA_TX_PACKETS_CELL_a INTEGER,DT_DELTA_TX_PACKETS_CELL_b INTEGER,DT_DELTA_RX_DROPS_WIFI_a INTEGER,DT
_DELTA_RX_DROPS_WIFI_b INTEGER,DT_DELTA_RX_PACKETS_WIFI_a INTEGER,DT_DELTA_RX_PACKETS_WIFI_b INTEGER,DT_DELTA_RX_DROPS_CELL_a INTEGER,DT_DELTA_RX_DROPS_CELL_
b INTEGER,DT_DELTA_RX_PACKETS_CELL_a INTEGER,DT_DELTA_RX_PACKETS_CELL_b INTEGER,DT_TOT_TX_DROPS_WIFI_a INTEGER,DT_TOT_TX_DROPS_WIFI_b INTEGER,DT_TOT_TX_PACKE
TS_WIFI_a INTEGER,DT_TOT_TX_PACKETS_WIFI_b INTEGER,DT_TOT_TX_DROPS_CELL_a INTEGER,DT_TOT_TX_DROPS_CELL_b INTEGER,DT_TOT_TX_PACKETS_CELL_a INTEGER,DT_TOT_TX_P
ACKETS_CELL_b INTEGER,DT_TOT_RX_DROPS_WIFI_a INTEGER,DT_TOT_RX_DROPS_WIFI_b INTEGER,DT_TOT_RX_PACKETS_WIFI_a INTEGER,DT_TOT_RX_PACKETS_WIFI_b INTEGER,DT_TOT_
RX_DROPS_CELL_a INTEGER,DT_TOT_RX_DROPS_CELL_b INTEGER,DT_TOT_RX_PACKETS_CELL_a INTEGER,DT_TOT_RX_PACKETS_CELL_b INTEGER,PM_ACCESS_COARSE_LOCATION_a INTEGER,
PM_ACCESS_COARSE_LOCATION_b INTEGER,PM_ACCESS_FINE_LOCATION_a INTEGER,PM_ACCESS_FINE_LOCATION_b INTEGER,PM_READ_PHONE_STATE_a INTEGER,PM_READ_PHONE_STATE_b I
NTEGER,DT_APP_0_PACKAGE_a TEXT,DT_APP_0_PACKAGE_b TEXT,DT_APP_0_TOT_RX_BYTES_a INTEGER,DT_APP_0_TOT_RX_BYTES_b INTEGER,DT_APP_0_TOT_RX_PACKETS_a INTEGER,DT_A
PP_0_TOT_RX_PACKETS_b INTEGER,DT_APP_0_TOT_TX_BYTES_a INTEGER,DT_APP_0_TOT_TX_BYTES_b INTEGER,DT_APP_0_TOT_TX_PACKETS_a INTEGER,DT_APP_0_TOT_TX_PACKETS_b INT
EGER,DT_APP_0_DELTA_INTERVAL_a INTEGER,DT_APP_0_DELTA_INTERVAL_b INTEGER,DT_APP_0_DELTA_RX_BYTES_a INTEGER,DT_APP_0_DELTA_RX_BYTES_b INTEGER,DT_APP_0_DELTA_R
X_PACKETS_a INTEGER,DT_APP_0_DELTA_RX_PACKETS_b INTEGER,DT_APP_0_DELTA_TX_BYTES_a INTEGER,DT_APP_0_DELTA_TX_BYTES_b INTEGER,DT_APP_0_DELTA_TX_PACKETS_a INTEG
ER,DT_APP_0_DELTA_TX_PACKETS_b INTEGER,PROXIMITY_a REAL,PROXIMITY_b REAL,PROXIMITY_ACC_a REAL,PROXIMITY_ACC_b REAL,CE_CODE INTEGER,CE_MSG INTEGER,CALL_DIRECT
ION TEXT )SRP_b INTEGER,LTE_RSRQ_a INTEGER,LTE_RSRQ_b INTEGER,LTE_RSSNR_a INTEGER,LTE_RSSNR_b INTEGER,LTE_CQI_a INTEGER,LTE_CQI_b INTEGER,SS_OPERATOR_ALPHA_a
 TEXT,SS_OPERATOR_ALPHA_b TEXT,SS_OPERATOR_ALPHA_LNG_a TEXT,SS_OPERATOR_ALPHA_LNG_b TEXT,SS_IS_MANUAL_a NUMERIC,SS_IS_MANUAL_b NUMERIC,SS_OPERATOR_NUM_a TEXT
,SS_OPERATOR_NUM_b TEXT,SS_ROAMING_a INTEGER,SS_ROAMING_b INTEGER,SS_STATE_a INTEGER,SS_STATE_b INTEGER,CI_POPULATED_a NUMERIC,CI_POPULATED_b NUMERIC,CDMA_LA
T_a INTEGER,CDMA_LAT_b INTEGER,CDMA_LNG_a INTEGER,CDMA_LNG_b INTEGER,CDMA_NET_ID_a INTEGER,CDMA_NET_ID_b INTEGER,CDMA_SYS_ID_a INTEGER,CDMA_SYS_ID_b INTEGER,
CDMA_BSID_a INTEGER,CDMA_BSID_b INTEGER,CS_CDMA_ASU_a INTEGER,CS_CDMA_ASU_b INTEGER,CS_CDMA_DBM_a INTEGER,CS_CDMA_DBM_b INTEGER,CS_CDMA_ECIO_a INTEGER,CS_CDM
A_ECIO_b INTEGER,CS_CDMA_LEVEL_a INTEGER,CS_CDMA_LEVEL_b INTEGER,CS_EVDO_DBM_a INTEGER,CS_EVDO_DBM_b INTEGER,CS_EVDO_ECIO_a INTEGER,CS_EVDO_ECIO_b INTEGER,CS
_EVDO_LEVEL_a INTEGER,CS_EVDO_LEVEL_b INTEGER,CS_EVDO_SNR_a INTEGER,CS_EVDO_SNR_b INTEGER,GSM_CID_a INTEGER,GSM_CID_b INTEGER,GSM_LAC_a INTEGER,GSM_LAC_b INT
```

```
                                                ,??!m?3)7emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/databases # chmod 775 *
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/databases # exit
emulator_arm64:/ $ exit
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % ./adb pull /data/data/com.Gold_Finger.V.X.your_Facebook/databases/reports
adb: error: failed to stat remote object '/data/data/com.Gold_Finger.V.X.your_Facebook/databases/reports': Permission denied
(base) taniajaswal@Tanias-MacBook-Pro platform-tools %
```

```
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % ./adb pull /data/data/com.Gold_Finger.V.X.your_Facebook/databases/reports
adb: error: failed to stat remote object '/data/data/com.Gold_Finger.V.X.your_Facebook/databases/reports': Permission denied
```

Findings for Files Directory-

A realm database named "default" was identified within the application. However, due to the app's non-debuggable nature, extraction of the files for inspection in the realm browser was not possible.

```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook # cd files
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/files # ls
default_config.json
```

```
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % ./adb pull /data/data/com.Gold_Finger.V.X.your_Facebook/files/
adb: error: failed to stat remote object '/data/data/com.Gold_Finger.V.X.your_Facebook/files/': Permission denied
```

Finding for Shared_prefs-

Shared Preferences are inherently insecure and lack encryption by default. Our examination revealed several instances of sensitive information within files like CookieSave.xml, Preference.xml, APPFIREWORKS.xml, and oscontribution.xml. These files contain data such as session cookies, SID, device location details, and SD contents, which could potentially be exploited if accessed by unauthorized parties.

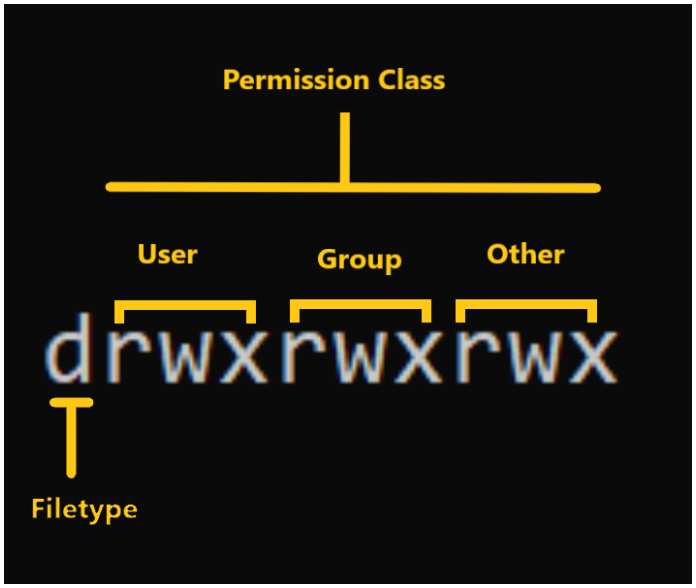
```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # ls
APPFIREWORKS.xml  WebViewChromiumPrefs.xml  koha_a_nrregull.xml        numruesi_pref.xml     prefrenc_per_start.xml  tahej_link_kontroll.xml
CookieSave.xml    dont_ask.xml              myapp.xml                  oscontribution.xml    share_par_pref.xml      timeri_host_cechk_pref.xml
Preference.xml    here_par_pref.xml         numri_per_standar_url.xml  permisssion_pref.xml  share_the_new_app.xml   update_app_pref.xml
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs #
```

```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cat tahej_link_kontroll.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="tahej_link_kontroll_numri" value="1" />
</map>
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cat timeri_host_cechk_pref.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="timeri_host_cechk_pref_numri" value="21600000" />
</map>
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cat update_app_pref.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <long name="update_app_numri" value="1712279155823" />
</map>
```

Permissions of the files in /data/data/com.Gold_Finger.V.X.your_Facebook-

```
emulator_arm64:/ $ su
emulator_arm64:/ # cd /data/data/com.Gold_Finger.V.X.your_Facebook
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook # ls -l
total 48
drwxrwx--x 2 u0_a176 u0_a176       4096 2024-04-04 18:05 app_textures
drwx------ 3 u0_a176 u0_a176       4096 2024-04-04 20:25 app_webview
drwxrws--x 5 u0_a176 u0_a176_cache 4096 2024-04-04 18:06 cache
drwxrwx--x 2 u0_a176 u0_a176       4096 2024-04-04 18:05 databases
drwxrwx--x 2 u0_a176 u0_a176       4096 2024-04-04 18:05 files
drwxrwx--x 2 u0_a176 u0_a176       4096 2024-04-04 20:25 shared_prefs
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook #
```

To know the permissions better-



– User: This is the owner of a file and the owner of the file belongs to this class.
– Group: The members of the file's group belong to this class
– Other: Any users that are not part of the user or group classes belong to this class.

Most directories, such as app_textures, cache, databases, files, and shared_prefs, have read, write, and execute permissions for both the owner (u0_a176) and the group (u0_a176). However, app_webview has these permissions exclusively for the owner. Additionally, the cache directory has a special setuid/setgid permission.

Conclusion for MASVS-STORAGE-1-

In conclusion, the app fails to securely store sensitive information, as evidenced by the presence of unprotected data in various storage locations. This non-compliance with MASVS-STORAGE-1 indicates a potential vulnerability in the app's data storage practices.

MASVS-STORAGE-2

MASVS-STORAGE-2 entails ensuring that the app effectively prevents any sensitive data from leaking or being exposed to unauthorized access.

Conducted Testing:

1. **Testing Backups for Sensitive Data-**

AllowBackup-

```
<application
    android:theme="@style/AppTheme"
    android:label="@string/app_name"
    android:icon="@drawable/splash_icon"
    android:name="com.Gold_Finger.V.X.your_Facebook.App"
    android:allowBackup="true"
    android:hardwareAccelerated="true"
    android:largeHeap="true"
    android:supportsRtl="true">
    <activity
```

The 'AllowBackup' setting is configured to 'true,' enabling the application to generate backups, potentially leading to the inadvertent storage and exposure of sensitive data. Consequently, the application does not meet the required standards and fails this evaluation.

Shared preferences-

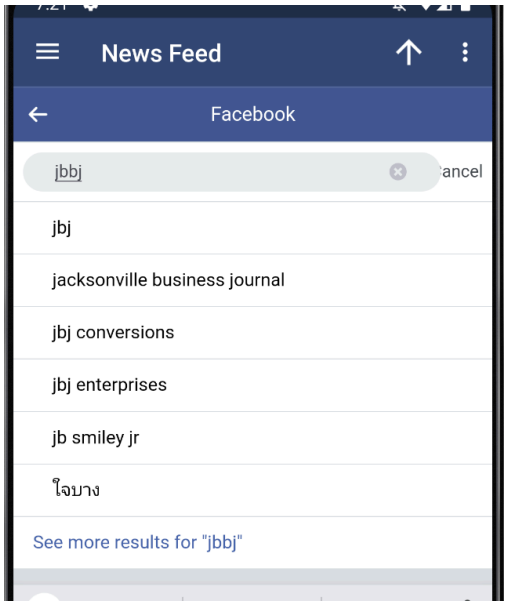
```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # ls
APPFIREWORKS.xml  WebViewChromiumPrefs.xml  koha_a_nrregull.xml       numruesi_pref.xml     prefrenc_per_start.xml  tahej_link_kontroll.xml
CookieSave.xml    dont_ask.xml              myapp.xml                oscontribution.xml    share_par_pref.xml      timeri_host_cechk_pref.xml
Preference.xml    here_par_pref.xml         numri_per_standar_url.xml  permisssion_pref.xml  share_the_new_app.xml   update_app_pref.xml
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs #
```

Shared preferences encompass files susceptible to cloud backup. Upon scrutiny, it's evident that CookieSave.xml and Preference.xml harbor sensitive user information, such as session cookies and SD contents. These data elements are vulnerable to exploitation, paving the way for session hijacking and data leakage. Though not all entries may be equally sensitive, items like session cookies in CookieSave.xml, SID in APPFIREWORKS.xml, and device location details in oscontribution.xml, present tangible security risks if compromised or exploited. The application falls short in this evaluation.

```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cat CookieSave.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="cookie_key">sb=moolZgmE5qYuUignEe-b3mEt; datr=moolZo8bXKcgEZ-Kq3lPEJID; m_pixel_ratio=2.75; fr=0LG2VDi3043XcmGke.AWVEoi7nP7BiGAG7k9aVyGlAEc
Q.BmJYqa..AAA.0.0.BmJYq_.AWUZMVSaw64; c_user=61557365424661; xs=10%3AbdYShC-YLWJtSw%3A2%3A1713736384%3A-1%3A-1; m_page_voice=61557365424661; x-referer=eyJyIj
oiL3Byb2ZpbGUucGhwP3Y9aW5mbyZsc3Q9NjE1NTczNjU0MjQ2NjE1M0E2MTU1NzM2NTQyNDY2MSUzQTE3MTM3MzY0MjEmZWF2PUFmYTFENkJTdVhtNDQ1Q0F6V29BRnRudEhLNGF3VmdWTDNZN2Q2dnJsTG1
5dVNTeS1FdGxGRkd2Wi03QVNVXzFqUmsmcGFpcHY9MCIsImgiOiIvcHJvZmlsZS5waHA%2Fdj1pbmZvJmxzdD02MTU1NzM2NTQyNDY2MSUzQTYxNTU3MzY1NDI0NjYxJTNBMTcxMzczNjQyMSZlYXY9QWZhMU
Q2QlN1WG00NDVDQXpXb0FGdG50SEs0YXdWZ1ZMM1k3ZDZ2cmxMbXl1U1N5LUV0bEZGR3ZaLTdBU1VfMWpSayZwYWlwdj0wIiwicyI6Im0ifQ%3D%3D; ps_n=1; ps_l=1; locale=en_US; wd=393x704;
 fbl_st=101422146%3BT%3A28537987; wl_cbv=v2%3Bclient_version%3A2472%3Btimestamp%3A1713736438</string>
</map>
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cat Preference.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="SD_CONTEXTS">VDA5YkdMemc4WEFHZEhKYlpKMC7x7fpxorMC64Z4hvXZv3p7ygKuexMcUFdvLPqeL3dYBPhtAEKVrCchiXapPJkaNpxl8Kp0q9623ev7ipeGIDgEjcxU9nL16n5O-G
yGDL1m5j4NKUXWugf5uQrtlsnt1Aw1XgT7gRdt9ynRHlB-IKAD9NhmqJJ_56tMXSMrWNSAoUixHXgVQGt-RbLtLoIUxn4NjGAsusaTf5tn4GmpvfNqcCkcilgMdLEtJkVH2rnVDSIP-M0waPXHuph0wVhJunK
_MPyamNsDaW7rJYVsQyuVe3LNJ82BIRM2qqxq9vg77aTAu76oivWHVZnwW1ii1gWkBhTUd6k9ZTTUr4lfKBxJ5HQJQAbp8pmljpb_1ExNUXj7JSKzDsiogKENgcdp6eF3KGr66NjELXA4pLcwBBbFGiZTTRiJq
JBWOpM__1DcOj6zpUcG174DYjQKu6A1HCmsBYXlldrVudiOpSaoKAubt-ZQW62XwLZMUOZAhv9mDsTqS2lhPMclygBFFWz_nf3XN0nxnE0N9Rr7kOpYX1Ss4dr56GVIoP8LFTlqdymtaF_J_p2jjcO3QXP3-r
EX7e2CyN-zSbuzPxWyOdXGAZ1qd1SuXWEJTJf21MvRIfk6sej4Bpps15J33IRppHnE-K9zNSA_wt7PdaJ49TJ-_IcemXYsiQFBvZMmV4wUahkbpX4ByXBbgXcgLCOVGtU7W08JGMjgR-ty6cHsAZEHxrb6NYT
duOKtsk-DWLNLmsqJubB7mQwH5hcGOOSTqWlkmVyjz8CGR423h75mRBNyP4iMm4MPryHz4tS_HViuc1rcjzbZLekNE0CUO_wiBycORgaUBCEvof8VcPnBxMtAwr9kJRN1h5Y0chw2c09d8xLMKvDQ2EsZWrHX
Ihh5f7op39yRVXK14mNw-W30v2PBlp9r4EhTrp2pxAdfiHxFxTkgXK0RM648nVPOtVs3KzA==</string>
    <long name="SD_CONTEXTS_UPDATE_TIME" value="1712279153687" />
    <boolean name="SD_CONTEXTS_INPROGRESS" value="false" />
```

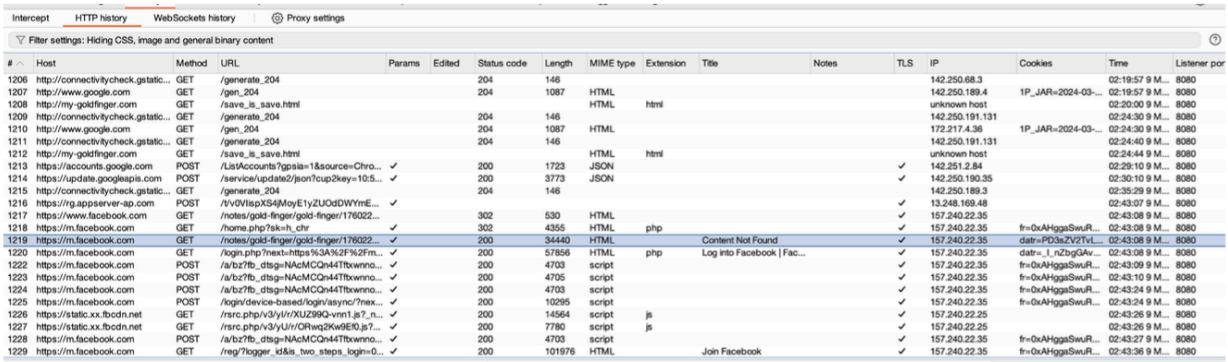
2. Determining Whether the Keyboard Cache Is Disabled for Text Input Fields-

While the application provides search suggestions akin to Facebook's functionality, it notably lacks suggestions in other areas. Additionally, it's observed that the keyboard cache remains enabled for certain input fields. Despite this, considering that only people's names are suggested, which typically aren't deemed sensitive unless coupled with additional data, it could be argued that the application successfully meets the test criteria. Moreover, there was no keyboard cache identified within the cache directory. Thus, the application is deemed compliant with this evaluation.



3. **Determining Whether Sensitive Data is Sent to Third Parties by Embedded Services-**

During communication testing, it was observed that the application interacted with Facebook, which is expected given its origin as a derivative of Facebook. However, in our recent investigation, no data pertinent to Facebook, such as user IDs, was identified as being transmitted to or from the app. Therefore, based on these findings, the application successfully passes this test.


Intercept HTTP history WebSockets history Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP	Cookies	Time	Listener por
1206	http://connectivitycheck.gstatic...	GET	/generate_204			204	146						142.250.68.3		02:19:57 9 M...	8080
1207	http://www.google.com	GET	/gen_204			204	1087	HTML					142.250.189.4	1P_JAR=2024-03-...	02:19:57 9 M...	8080
1208	http://my-goldfinger.com	GET	/save_is_save.html					HTML	html				unknown host		02:20:00 9 M...	8080
1209	http://connectivitycheck.gstatic...	GET	/generate_204			204	146						142.250.191.131		02:24:30 9 M...	8080
1210	http://www.google.com	GET	/gen_204			204	1087	HTML					172.217.4.36	1P_JAR=2024-03-...	02:24:30 9 M...	8080
1211	http://connectivitycheck.gstatic...	GET	/generate_204			204	146						142.250.191.131		02:24:40 9 M...	8080
1212	http://my-goldfinger.com	GET	/save_is_save.html					HTML	html				unknown host		02:24:44 9 M...	8080
1213	https://accounts.google.com	POST	/ListAccounts?gpsia=1&source=Chro...	✓		200	1723	JSON				✓	142.251.2.84		02:29:10 9 M...	8080
1214	https://update.googleapis.com	POST	/service/update2/json?cup2key=10:5...	✓		200	3773	JSON				✓	142.250.190.35		02:30:10 9 M...	8080
1215	http://connectivitycheck.gstatic...	GET	/generate_204			204	146						142.250.189.3		02:35:29 9 M...	8080
1216	https://rg.appserver-ap.com	POST	/tV0VIispXS4jMoyE1yZUOdDWYmE...	✓								✓	13.248.169.48		02:43:07 9 M...	8080
1217	https://www.facebook.com	GET	/notes/gold-finger/gold-finger/176022...			302	530	HTML				✓	157.240.22.35		02:43:08 9 M...	8080
1218	https://m.facebook.com	GET	/home.php?sk=h_chr	✓		302	4355	HTML	php			✓	157.240.22.35	fr=0xAHggaSwuR...	02:43:08 9 M...	8080
1219	https://m.facebook.com	GET	/notes/gold-finger/gold-finger/176022...	✓		200	34440	HTML		Content Not Found		✓	157.240.22.35	datr=PD3aZV2TvL...	02:43:08 9 M...	8080
1220	https://m.facebook.com	GET	/login.php?next=https%3A%2F%2Fm...	✓		200	57856	HTML	php	Log into Facebook | Fac...		✓	157.240.22.35	datr=_I_nZbgGAv...	02:43:08 9 M...	8080
1222	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcMCQn44Tftxwnno...	✓		200	4703	script				✓	157.240.22.35	fr=0xAHggaSwuR...	02:43:09 9 M...	8080
1223	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcMCQn44Tftxwnno...	✓		200	4705	script				✓	157.240.22.35	fr=0xAHggaSwuR...	02:43:10 9 M...	8080
1224	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcMCQn44Tftxwnno...	✓		200	4703	script				✓	157.240.22.35	fr=0xAHggaSwuR...	02:43:24 9 M...	8080
1225	https://m.facebook.com	POST	/login/device-based/login/async/?nex...	✓		200	10295	script				✓	157.240.22.35	fr=0xAHggaSwuR...	02:43:24 9 M...	8080
1226	https://static.xx.fbcdn.net	GET	/rsrc.php/v3/yU/r/XUZ99Q-vnn1.js?_n...	✓		200	14564	script	js			✓	157.240.22.25		02:43:26 9 M...	8080
1227	https://static.xx.fbcdn.net	GET	/rsrc.php/v3/yU/r/ORwq2Kw9Ef0.js?...	✓		200	7780	script	js			✓	157.240.22.25		02:43:26 9 M...	8080
1228	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcMCQn44Tftxwnno...	✓		200	4703	script				✓	157.240.22.35	fr=0xAHggaSwuR...	02:43:27 9 M...	8080
1229	https://m.facebook.com	GET	/reg/?logger_id&is_two_steps_login=0...	✓		200	101976	HTML		Join Facebook		✓	157.240.22.35	fr=0xAHggaSwuR...	02:43:36 9 M...	8080

Conclusion for MASVS-STORAGE-2-

The application demonstrates vulnerabilities in preventing the leakage of sensitive data. Notably, the allowance for backups introduces the potential for sensitive information to be stored insecurely. Additionally, an examination of shared preferences reveals XML files housing sensitive data, posing exploitable risks. These findings highlight areas where the application's data protection measures fall short, necessitating immediate attention and remediation to mitigate potential security breaches and safeguard user information effectively.

Extra MASVS-STORAGE Testing

1. **Log Testing-**

```
emulator_arm64:/ $ pidof -s com.Gold_Finger.V.X.your_Facebook
16327
emulator_arm64:/ $ exit
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % ./adb logcat --pid=16327 > miniforfacelog.txt
^C
(base) taniajaswal@Tanias-MacBook-Pro platform-tools %
```

In the log testing of the app, it was observed that despite logging in and utilizing various app functionalities, no sensitive information was found in the logs.

2. **Memory Testing-**

During memory testing, attempts to dump the memory and extract a Txt file were unsuccessful. Despite the app being operational during testing, fridump failed to connect to it. However, the process IP of the app was successfully identified.

```
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % frida --version
16.2.1
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % ./adb push
adb: push requires <source> and <destination> arguments
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % ./adb push ~/Downloads/frida-core-devkit-16.2.1-android-arm64 /data/local/tmp/
/Users/taniajaswal/Downloads/frida-core-devkit-16.2.1-android-arm64/: 4 files pushed, 0 skipped. 167.1 MB/s (243473485 bytes in 1.390s)
```

```
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % ./adb shell
emulator_arm64:/ $ su
emulator_arm64:/ # chmod 755 /data/local/tmp/*
```

```
emulator_arm64:/ # ./data/local/tmp/frida-server-16.2.1-android-arm64
```

```
emulator_arm64:/ # "/data/local/tmp/frida-server-16.2.1-android-arm64"
```

```
e) taniajaswal@Tanias-MacBook-Pro fridump % frida-ps -U
```

```
14962  Mini For Facebook
14169  Photos
```

```
15559  com.Gold_Finger.V.X.your_Facebook:background
14985  com.Gold_Finger.V.X.your_Facebook:ndc_background_sdk
```

```
                                    |_|

Can't connect to App. Have you connected the device?
(base) taniajaswal@Tanias-MacBook-Pro fridump-master % python fridump.py -U -s 17508

        ______    _     _
        |  ___|  (_)   | |
        | |_ _ __ _  __| |_   _ _ __ ___  _ __
        |  _| '__| |/ _` | | | | '_ ` _ \| '_ \
        | | | |  | | (_| | |_| | | | | | | |_) |
        \_| |_|  |_|\__,_|\__,_|_| |_| |_| .__/
                                          | |
                                          |_|

Can't connect to App. Have you connected the device?
(base) taniajaswal@Tanias-MacBook-Pro fridump-master % python fridump.py -U -s 17192

        ______    _     _
        |  ___|  (_)   | |
        | |_ _ __ _  __| |_   _ _ __ ___  _ __
        |  _| '__| |/ _` | | | | '_ ` _ \| '_ \
        | | | |  | | (_| | |_| | | | | | | |_) |
        \_| |_|  |_|\__,_|\__,_|_| |_| |_| .__/
                                          | |
                                          |_|

Can't connect to App. Have you connected the device?
```

Conclusion for Log and Memory Testing-

In conducting both log and memory testing on the application, it was observed that while log testing revealed no instances of sensitive information exposure within the application's logs, memory testing encountered difficulties. Despite efforts to dump the memory and extract data using Fridump, the tool failed to establish a connection with the running application. Although the process ID of the application was identified, Fridump was unable to interact with it successfully.

MASVS Cryptography

MASVS-CRYPTO-1

MASVS-CRYPTO-1 assesses if the app employs up-to-date and robust encryption methods in line with industry standards. It ensures sensitive data, like user credentials, remains well-protected against modern cyber threats, enhancing overall security and reducing the risk of unauthorized access or tampering.

Testing Conducted for Cryptography Testing:

1. The MobSF report indicates that the app utilizes inadequate random number generators, a critical security flaw. This finding highlights a significant vulnerability in the app's cryptographic implementation, potentially exposing sensitive data to exploitation by attackers. Therefore, the app does not meet the requirements for robust cryptographic practices.

NO	ISSUE	SEVERITY	STANDARDS	FILES
				com/pro100svitlo/fingerprintAuthHelper/b.java com/pro100svitlo/fingerprintAuthHelper/e.java d/a/a/a/b/c.java d/a/a/a/d.java
2	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/Gold_Finger/V/X/your_Facebook/MainActivity.java com/opensignal/datacollection/measurements/invariable/Installation.java com/opensignal/datacollection/measurements/speedtest/CdnDownloadTest.java com/opensignal/datacollection/measurements/speedtest/CdnUploadTest.java com/opensignal/datacollection/sending/DailySendingConfig.java org/a/a/a.java

2. The app's utilization of MD5 and SHA-1 cryptographic algorithms signifies a concerning lapse in security measures. Both MD5 and SHA-1 are widely recognized as outdated and vulnerable to exploitation by attackers, rendering them unsuitable for robust data protection. By employing these weak algorithms, the app exposes user data to significant risks, contravening industry best practices for cryptographic security. Consequently, the app fails to meet the requisite standards for secure cryptographic implementation.

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	com/opensignal/datacollection/measurements/invariable/Installation.java

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/opensignal/datacollection/androidwebsockets/WebSocketClient.java

The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	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	com/pro100svitlo/fingerprintAuthHelper/d.java

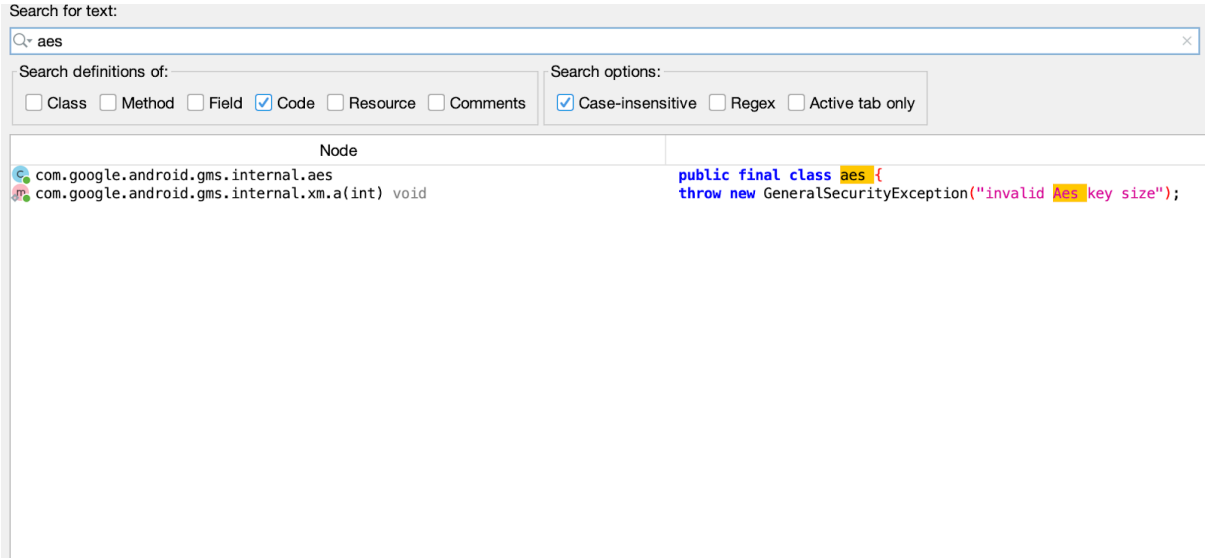
3. The application effectively meets the criteria for hard-coded secrets, as the ones highlighted in the MobSF report were unrelated to the app's functionalities. Additionally, no passwords were discovered within the assets, ensuring compliance with security standards in this regard.

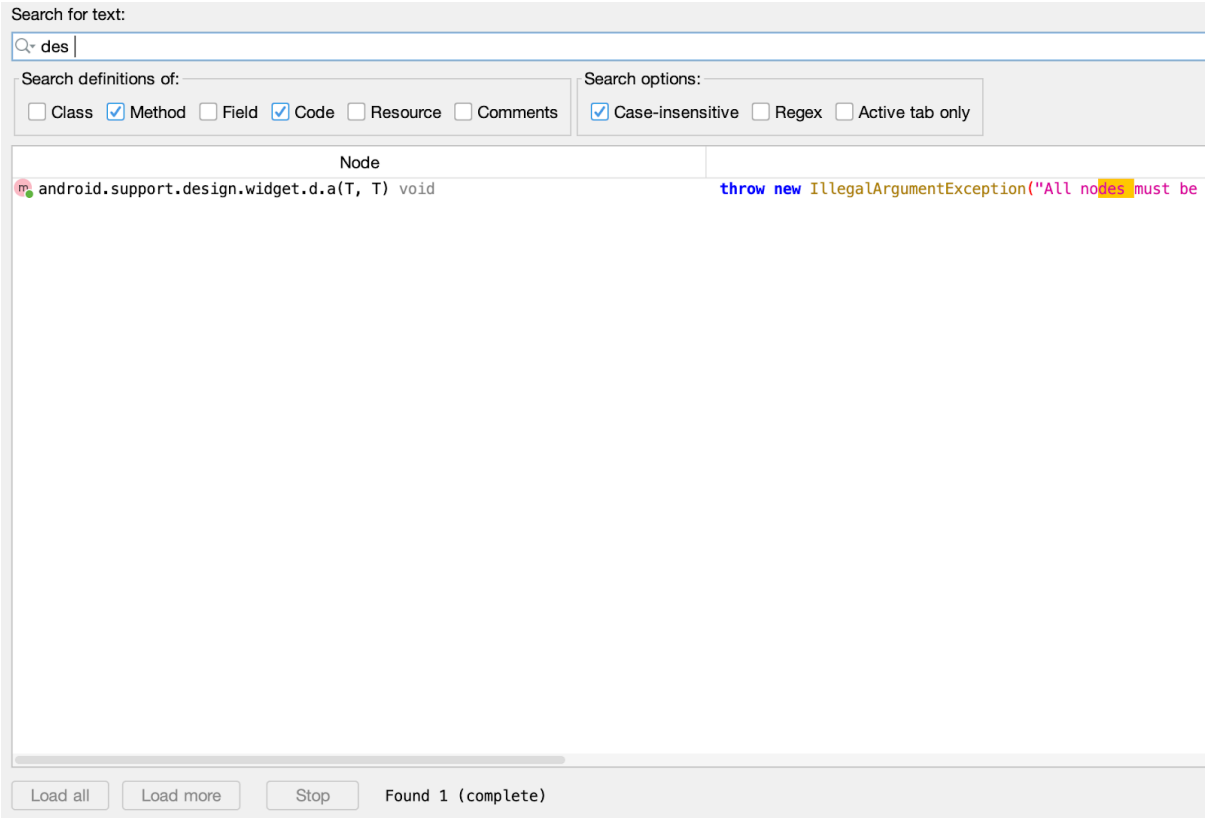
HARDCODED SECRETS

POSSIBLE SECRETS
"library_FloatingActionButton_authorWebsite" : "https://github.com/makovkastar/FloatingActionButton"
"library_introduction_authorWebsite" : "https://github.com/RubenGees"
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

POSSIBLE SECRETS
NjjdWKeusqbr2mhpoA2g1k80SENu31+kVl6okgBC0lR1TAOBy1c5K6TDka9FL0qb
FUnu12BLeA90PMRjjzlkVEPyqHD6uiYJ0wfE9HQOe8=
115792089210356248762697446949407573530086143415290314195533631308867097853951
q6PH7Tul6eeQUbRopl+wAdHRUZoqOJe+k6S+oAH1OLINqD9Nw3bstul41/tEKqJf
OOD7Mmy72hHlaT8E6Bavpqcej+Bv/26VLB5BKy2vdFU=
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
nq+dK1ZBazPeiOwzPjxFVi/DAdimINGjjC3dmnjHFWeFHhcvKyvaGTwBjbCXbYjP
l33Ewtb1FLQfjku9hMTlspljUsfXZHPtUVdiwVobzqc=
rFH4ecfOE6wTQWQMNZCbGEOnX/EvnKk7o423XnmLCwo=
sZx5dM9LN5T6tOU5PFWOx9ynOF1nN101RoY1lhhzYQc=
N4oD0+QrGPgqj6dk3gy+T0oV4HkE0l59PeQMyXije14=
X3Mc2F1m5PVCvtRNCNygVlhNRZ5PADTpqvT3rpTRDQW0QXZdeilMadj4uFo/P1Vl
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
r1hUymvZt16JgOEs1sQFtIZ7A08SjznmvklWeDcQtPU=

4. The absence of AES and DES encryption relevant to the application ensures compliance, indicating that the app successfully passes this test.





Conclusion for MASVS Cryptography:

In conclusion, the cryptography testing of the app identified several critical vulnerabilities in its encryption practices, highlighting areas of concern for data security. The app's reliance on inadequate random number generators and the use of weak cryptographic algorithms such as MD5 and SHA-1 pose significant risks to user data, potentially exposing it to exploitation by malicious actors. While the app demonstrates satisfactory handling of hard-coded secrets and does not employ vulnerable encryption methods like AES and DES, the identified vulnerabilities overshadow these strengths. Moving forward, addressing these cryptographic weaknesses is imperative to enhance the overall security posture of the app and mitigate the risk of unauthorized access or data tampering. By adopting up-to-date encryption methods and implementing robust cryptographic practices, the app can better protect sensitive user data and ensure compliance with industry standards for secure data handling.

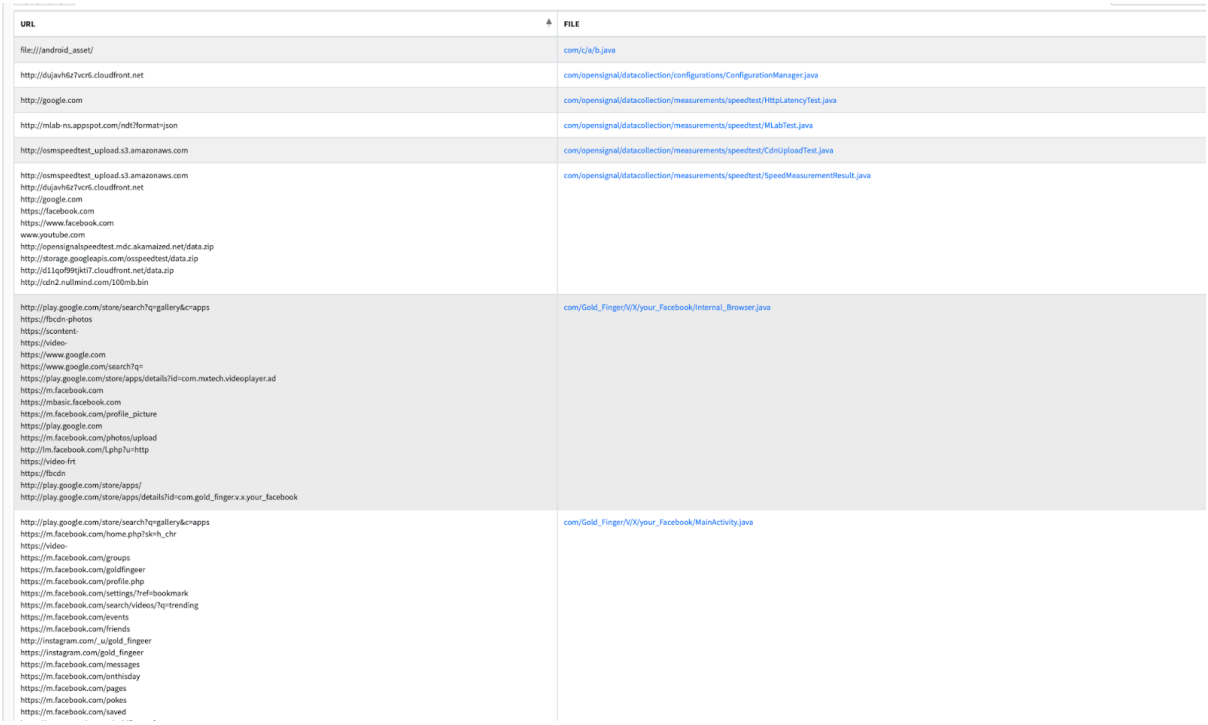
MASVS Authentication

MASVS-AUTH-1

Testing Methods Conducted for Authentication Testing:

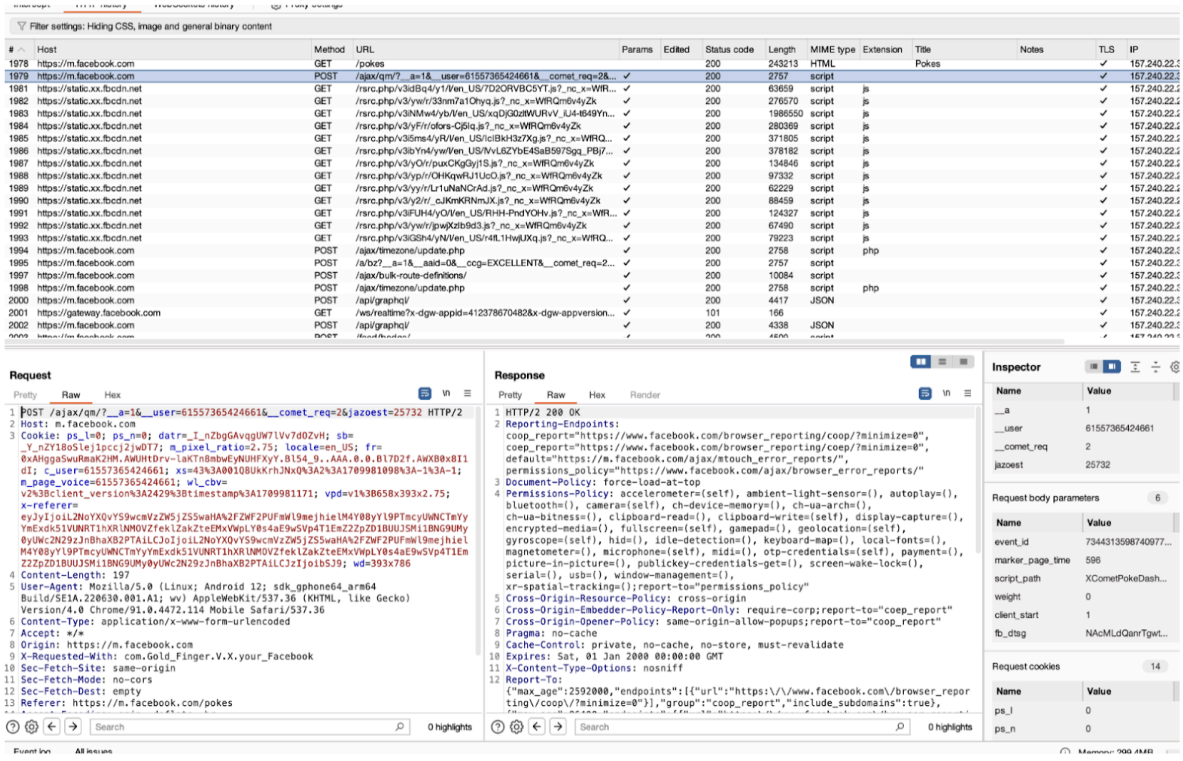
1. **Endpoint URLs-**

The MobSF report did not include URLs in the PDF report, but they were accessible in the original report. According to the findings, the app predominantly utilizes URLs that necessitate authentication, such as those for Google, Facebook, Instagram, and YouTube. Based on this assessment, the app successfully passes the test.



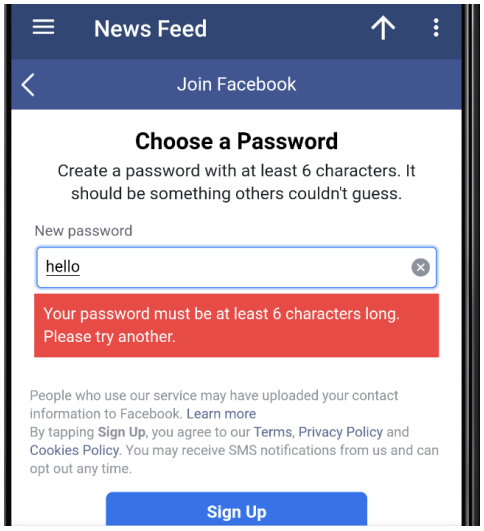
URL	FILE
file:///android_asset/	com/c/a/b.java
http://dujavh6z7vcr6.cloudfront.net	com/opensignal/datacollection/configurations/ConfigurationManager.java
http://google.com	com/opensignal/datacollection/measurements/speedtest/HttpLatencyTest.java
http://mlab-ns.appspot.com/ndt?format=json	com/opensignal/datacollection/measurements/speedtest/MLabTest.java
http://osmspeedtest_upload.s3.amazonaws.com	com/opensignal/datacollection/measurements/speedtest/CdnUploadTest.java
http://osmspeedtest_upload.s3.amazonaws.com http://dujavh6z7vcr6.cloudfront.net http://google.com https://facebook.com https://www.facebook.com www.youtube.com http://opensignalspeedtest.mdc.akamaized.net/data.zip http://storage.googleapis.com/osspeedtest/data.zip http://d11qof9tfjkh57.cloudfront.net/data.zip http://cdn2.nullmind.com/100mb.bin	com/opensignal/datacollection/measurements/speedtest/SpeedMeasurementResult.java
http://play.google.com/store/search?q=gallery&c=apps https://fbcdn-photos https://scontent- https://video- https://www.google.com https://www.google.com/search?q= https://play.google.com/store/apps/details?id=com.mxtech.videoplayer.ad https://m.facebook.com https://mbasic.facebook.com https://m.facebook.com/profile_picture https://play.google.com https://m.facebook.com/photos/upload http://lm.facebook.com/l.php?u=http https://video-frt https://fbcdn http://play.google.com/store/apps/ http://play.google.com/store/apps/details?id=com.gold_finger.v.x.your_facebook	com/Gold_Finger/V/X/your_Facebook/Internal_Browser.java
http://play.google.com/store/search?q=gallery&c=apps https://m.facebook.com/home.php?sk=h_chr https://video- https://m.facebook.com/groups https://m.facebook.com/goldfingeer https://m.facebook.com/profile.php https://m.facebook.com/settings/?ref=bookmark https://m.facebook.com/search/videos/?q=trending https://m.facebook.com/events https://m.facebook.com/friends http://instagram.com/_u/gold_fingeer https://instagram.com/gold_fingeer https://m.facebook.com/messages https://m.facebook.com/onthisday https://m.facebook.com/pages https://m.facebook.com/pokes https://m.facebook.com/saved	com/Gold_Finger/V/X/your_Facebook/MainActivity.java

2. Since this app serves as a mini version of Facebook, it's apparent that authentication is directed to Facebook servers, as observed in prior testing phases. However, it's unclear whether local authentication mechanisms are entirely absent. Therefore, the testing outcome remains inconclusive.

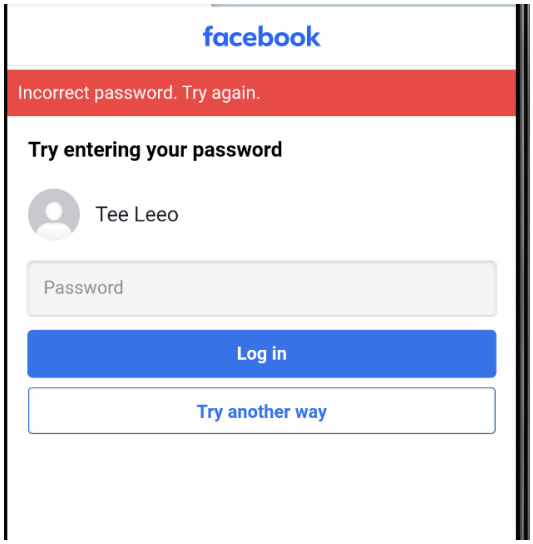


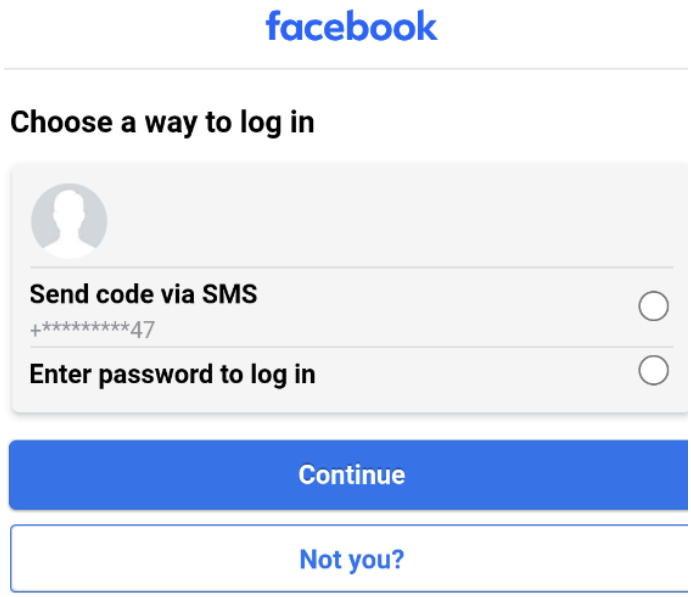
3. **Strong Password Policy-**

The app imposes no additional constraints on passwords beyond a minimum length of six characters. Therefore, it meets the criteria for a strong password policy, and the test is considered passed.

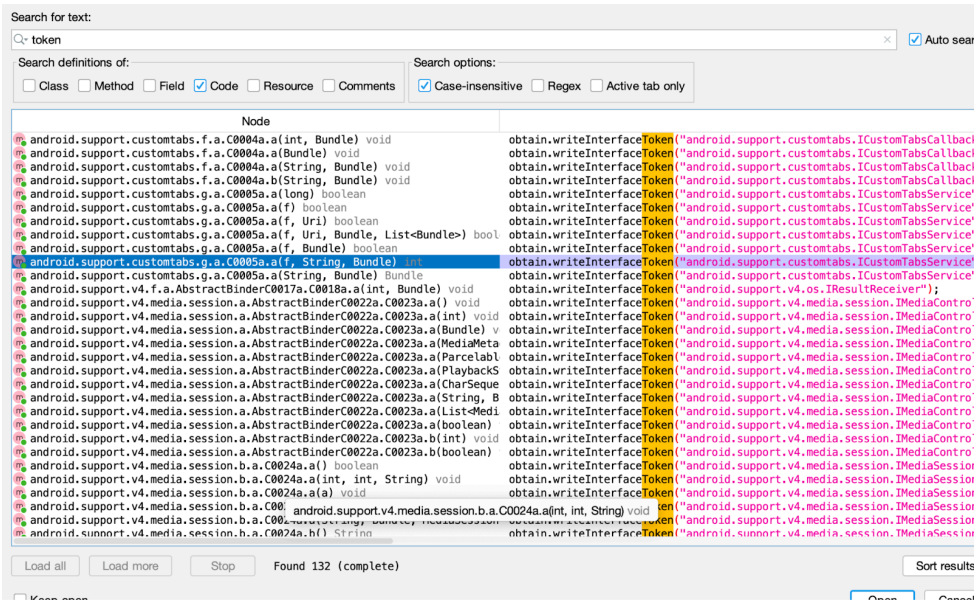


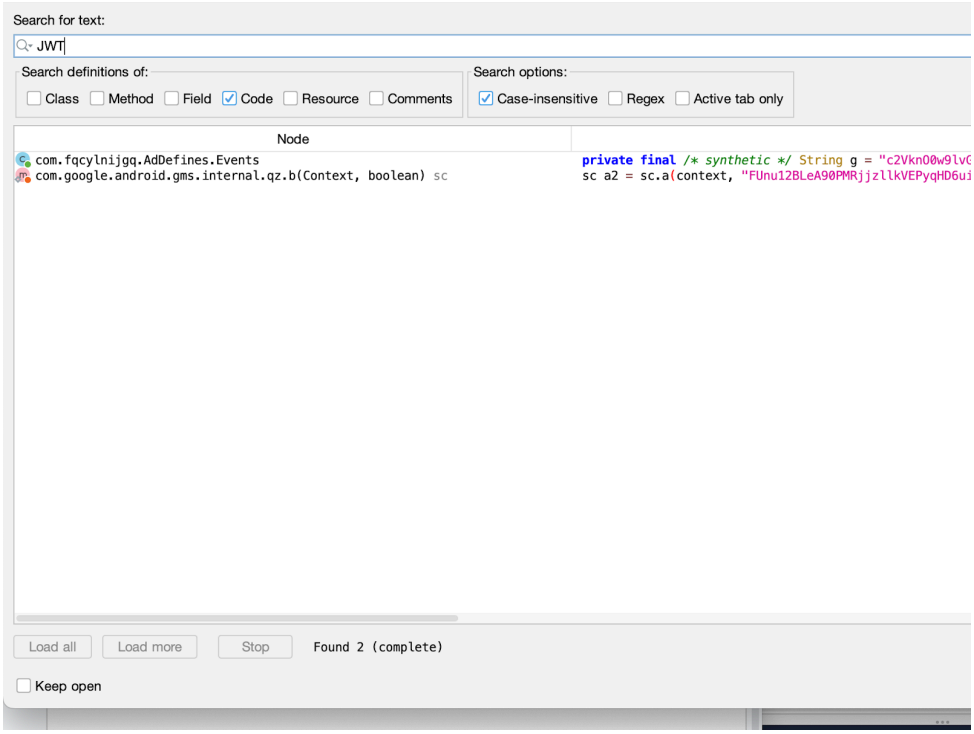
4. The app fails the test as it allows unlimited attempts on passwords without any prevention, limits, or blocking mechanisms. However, an alternative login method via SMS to the phone number is provided by the app.



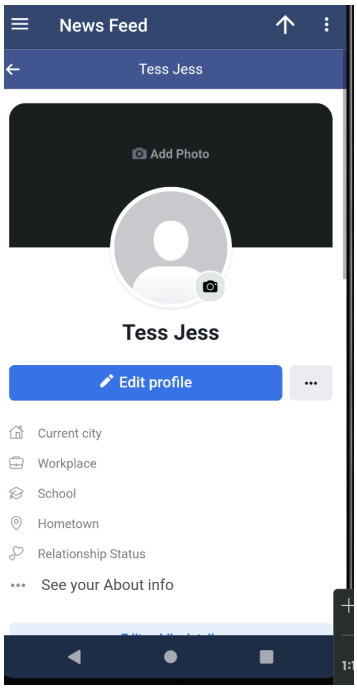


5. The app passed the test as there were no relevant instances of "token" or JWT found in the code, and none of the hardcoded secrets were related to the app. Therefore, no hidden tokens were discovered in the code.

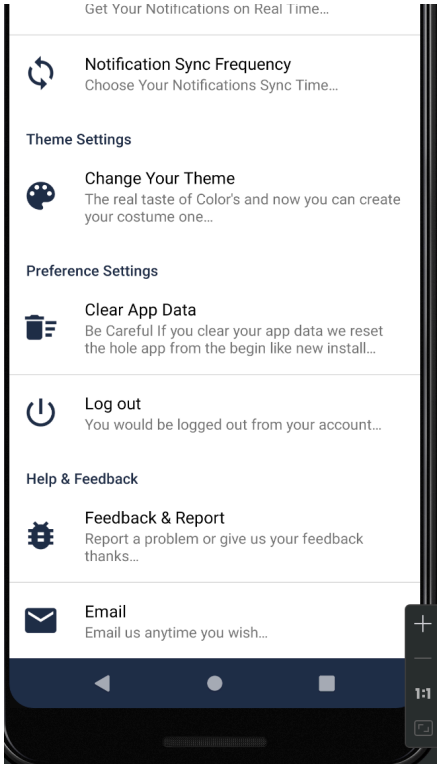


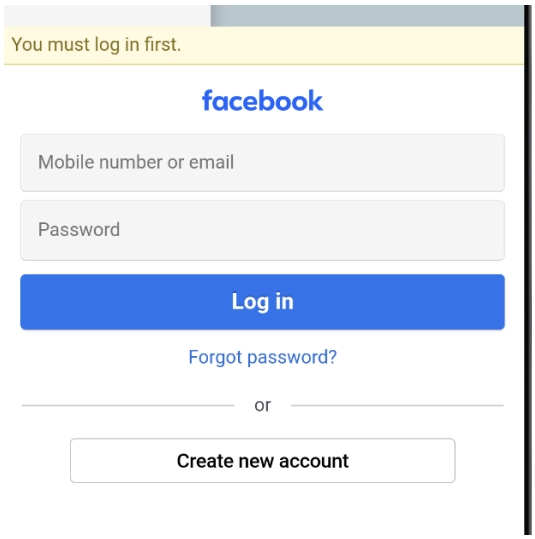


6. The app fails the test due to its lack of session timeout functionality, which leaves user sessions vulnerable to exploitation. This could potentially lead to unauthorized access to user accounts if a device is left unattended with an active session. Implementing session timeout measures is crucial for enhancing overall security and protecting user data from unauthorized access.

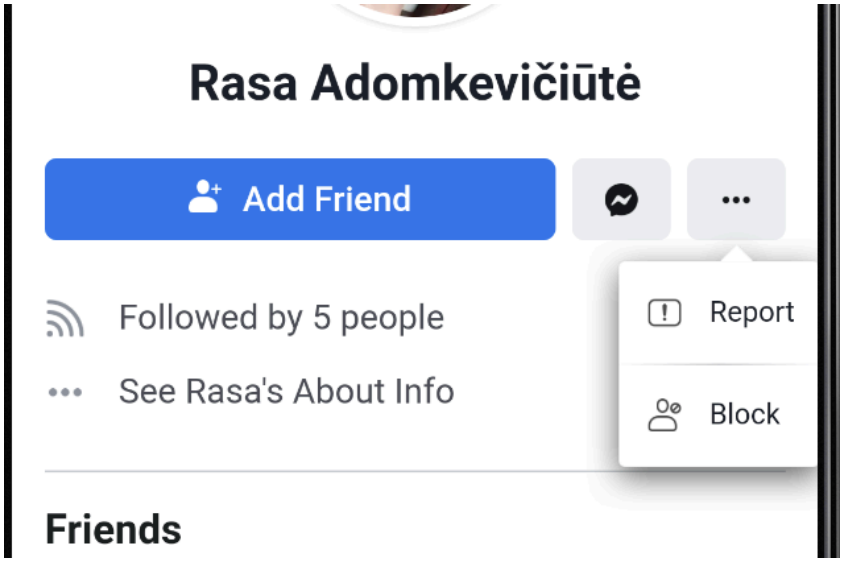


7. The app successfully passes the test as it requires users to log in again after logging out, even when attempting to return using the back button. This indicates that the auto-login feature is disabled upon logout, enhancing security by preventing unauthorized access to user accounts.





8. The app successfully passes this test as it provides users with the functionality to block or report other individuals, similar to the features available on the Facebook platform. This capability enhances user control over their interactions within the app, contributing to a safer and more secure user experience.

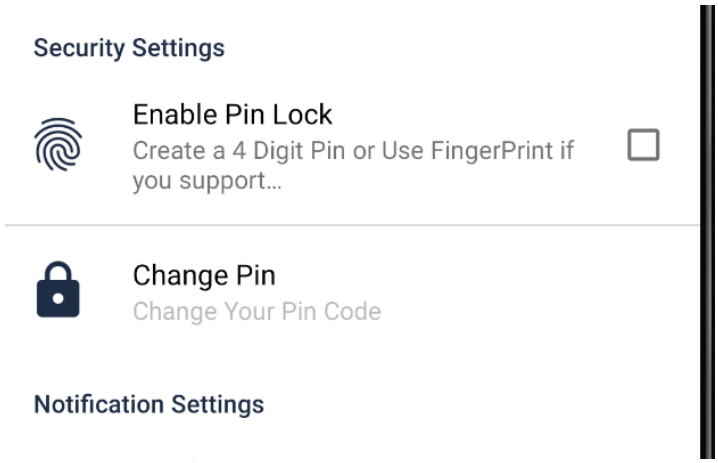


MASVS-AUTH-2

MASVS-AUTH-2 assesses whether the app securely implements local authentication in accordance with platform best practices. This involves ensuring that the app follows established guidelines and standards for handling authentication processes locally on the device. Key considerations include securely storing and managing authentication credentials, implementing secure login mechanisms, and protecting user data from unauthorized access. In essence, MASVS-AUTH-2 evaluates whether the app adheres to platform-specific security recommendations to safeguard user authentication within the application.

Testing Methods Used:

1. While the app primarily relies on external authentication services, such as Facebook, it does offer users the option to enhance security through local authentication by setting up a PIN within the app. This feature allows users to add an extra layer of protection to their accounts, providing greater control over access to their personal information and interactions within the app.



MASVS-AUTH-3

MASVS-AUTH-3 requires apps to implement additional authentication measures for sensitive operations, such as making financial transactions or changing critical settings. This ensures that even if a user's session is compromised, unauthorized access to sensitive functionalities is prevented. In essence, it adds an extra layer of security to safeguard against potential misuse or unauthorized access to critical app functionalities.

1. The app only utilizes SMS verification when users forget their passwords; however, it lacks multi-factor authentication (MFA) beyond this scenario. As MFA is a crucial security measure for protecting user accounts, its absence renders the app non-compliant with this test.

Conclusion for MASVS Authentication:

In conclusion, the authentication testing of the app revealed both strengths and weaknesses in its implementation of authentication mechanisms. While the app effectively utilizes external authentication services for user login, such as those provided by Facebook, it lacks robust local authentication mechanisms. The absence of password complexity requirements and limitations on login attempts poses security risks, albeit mitigated to some extent by the availability of alternative login methods like SMS verification. Additionally, the app fails to implement session timeout functionality, leaving user sessions vulnerable to exploitation. However, it demonstrates adequate measures for user account management, including options to block or report other users. Moving forward, addressing these authentication vulnerabilities and implementing additional security measures, such as robust password policies and session management controls, is crucial for enhancing the overall security posture of the app and safeguarding user data.

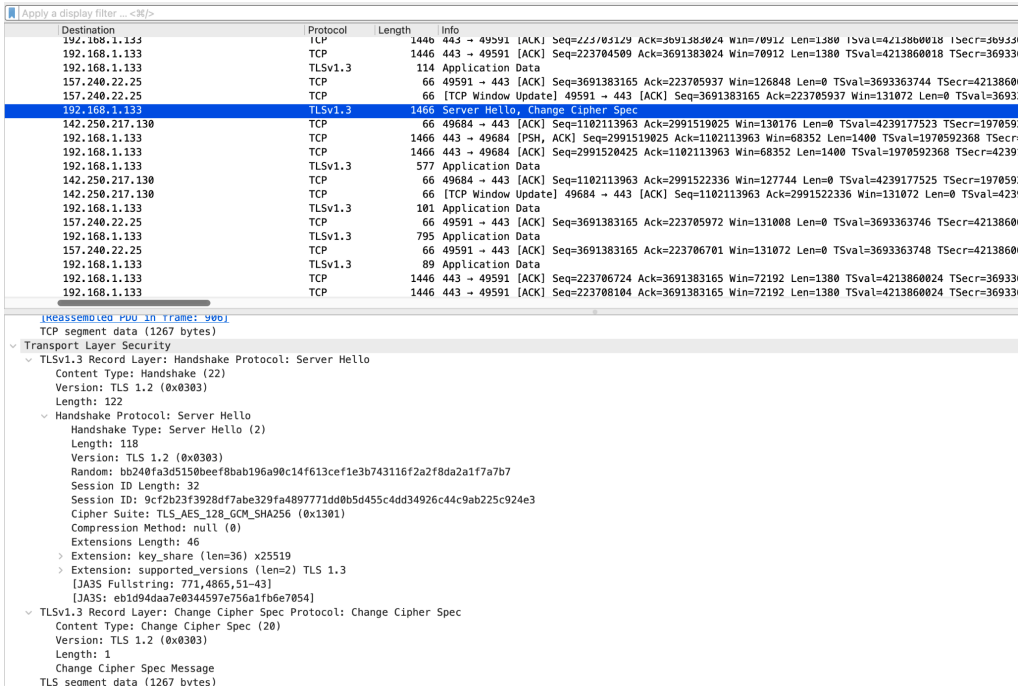
MASVS Network Communication

MASVS-NETWORK-1

MASVS-NETWORK-1 evaluates how securely an app communicates over networks. It assesses whether the app uses secure communication protocols to transmit data, ensuring confidentiality, integrity, and authenticity. Essentially, this test examines whether the app employs encryption and secure transmission mechanisms to protect user data from eavesdropping, tampering, and unauthorized access while in transit over networks.

Testing Conducted for **MASVS-NETWORK-1:**

1. The Wi-Fi traffic analysis, conducted using Wireshark to scrutinize all app functions such as login and account viewing, successfully passed the testing. Through meticulous filtering, no unencrypted HTTP usage was detected, affirming robust encryption practices. TLS, including versions 1.2 and 1.3, was identified, ensuring secure data transmission. No clear-text credentials were observed during the Wireshark analysis. The data was encrypted by TLS protocol. Overall, the findings confirm the efficacy of the encryption measures, thus indicating a passing result for the analysis.

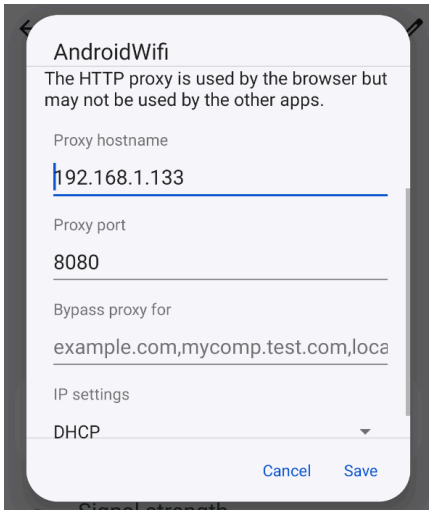


```
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
  my-goldfinger.com: type AAAA, class IN
      Name: my-goldfinger.com
      [Name Length: 17]
      [Label Count: 2]
      Type: AAAA (28) (IP6 Address)
      Class: IN (0x0001)
[Response In: 83]
```

```
[Bytes in flight: 3343]
[Bytes sent since last PSH flag: 268]
TCP payload (268 bytes)
Transport Layer Security
  TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 263
    Encrypted Application Data [truncated]: 6cc52a4d75cfd104301b44aa7dcf8fdc6a3ecbd16dc783e4d445f93cf85d4eb803b4a2be2b416021d01a2ba9a6f3cad3403ec0a3aed59f4fefa15e1b36dd02373d539d8f6d4
    [Application Data Protocol: Hypertext Transfer Protocol]
```

2. Capture HTTPS Traffic with Burp Suite-

The app did not work properly with the proxy because the app uses SSL Pinning which blocks the proxy, we will use Frida to solve this issue.



Investigated SSL pinning using Frida:

SSL pinning was implemented on the app, so bypassing was necessary. Bypassed using Frida tool. After bypassing, the traffic of the Facebook app was captured. The traffic shows that the app uses HTTP/2 which supports encryption through the use of Transport Layer Security (TLS), which is also used by the app. There were no findings of clear text seen in the traffic. The app also uses cookies to store the user information.

Commands used ->

```
(base) taniajaswal@Tanias-MacBook-Pro Downloads % cd ..
(base) taniajaswal@Tanias-MacBook-Pro ~ % pip install frida-tools
Requirement already satisfied: frida-tools in ./opt/anaconda3/lib/python3.9/site-packages (12.3.0)
Requirement already satisfied: pygments<3.0.0,>=2.0.2 in ./opt/anaconda3/lib/python3.9/site-packages (from frida-tools) (2.11.2)
Requirement already satisfied: frida<17.0.0,>=16.0.9 in ./opt/anaconda3/lib/python3.9/site-packages (from frida-tools) (16.2.1)
Requirement already satisfied: colorama<1.0.0,>=0.2.7 in ./opt/anaconda3/lib/python3.9/site-packages (from frida-tools) (0.4.5)
Requirement already satisfied: prompt-toolkit<4.0.0,>=2.0.0 in ./opt/anaconda3/lib/python3.9/site-packages (from frida-tools) (3.0.20)
Requirement already satisfied: typing-extensions in ./opt/anaconda3/lib/python3.9/site-packages (from frida<17.0.0,>=16.0.9->frida-tools) (4.3.0)
Requirement already satisfied: wcwidth in ./opt/anaconda3/lib/python3.9/site-packages (from prompt-toolkit<4.0.0,>=2.0.0->frida-tools) (0.2.5)
(base) taniajaswal@Tanias-MacBook-Pro ~ % frida --version
16.2.1
(base) taniajaswal@Tanias-MacBook-Pro ~ % cd Downloads
(base) taniajaswal@Tanias-MacBook-Pro Downloads % /Users/taniajaswal/Library/Android/sdk/platform-tools/adb push frida-server-16.2.1-android-arm64 /data/local/tmp/
frida-server-16.2.1-android-arm64: 1 file pushed, 0 skipped. 81.3 MB/s (51256968 bytes in 0.601s)
(base) taniajaswal@Tanias-MacBook-Pro Downloads % /Users/taniajaswal/Library/Android/sdk/platform-tools/adb root
adbd is already running as root
(base) taniajaswal@Tanias-MacBook-Pro Downloads % /Users/taniajaswal/Library/Android/sdk/platform-tools/adb shell
emulator64_arm64:/ # cd data/local/tmp
emulator64_arm64:/data/local/tmp # ls
frida-server-16.2.1-android-arm64
hmod +x frida-server-16.2.1-android-arm64 &                                                    <
[1] 24588
/frida-server-16.2.1-android-arm64 &                                                           <
[2] 24850
[1] - Done                    \chmod +x frida-server-16.2.1-android-arm64
(base) taniajaswal@Tanias-MacBook-Pro Downloads %
```

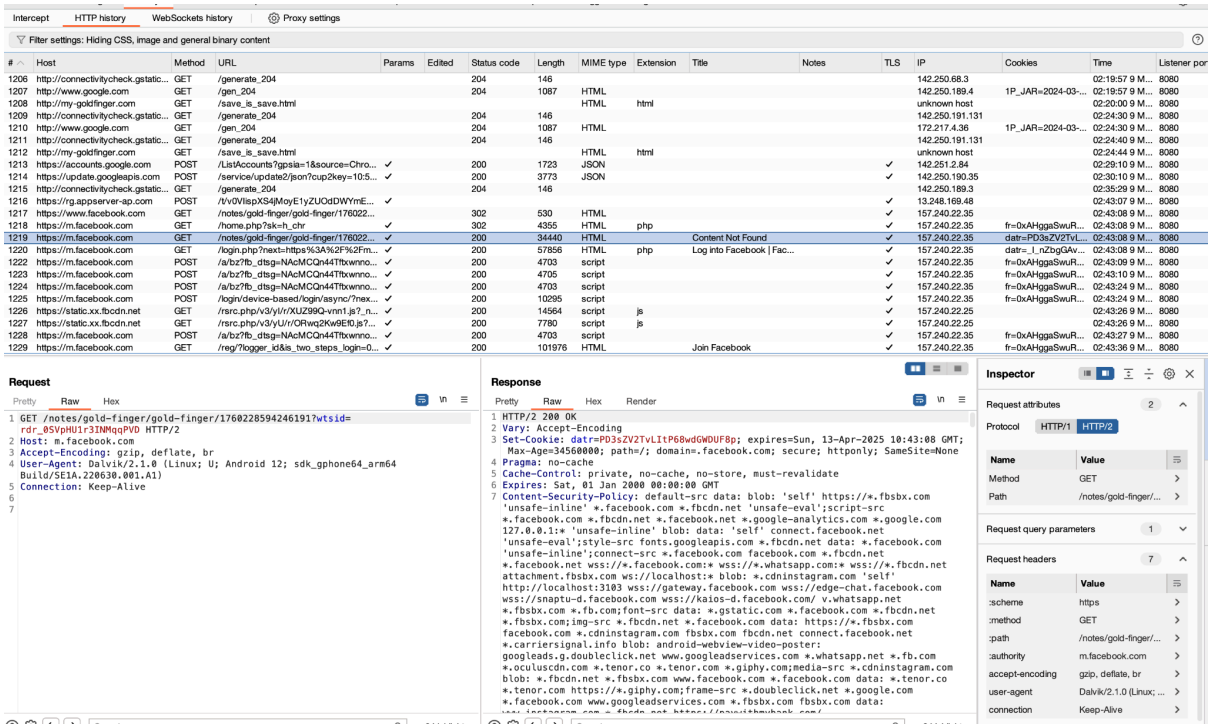
```
(base) taniajaswal@Tanias-MacBook-Pro / % frida -UF

     ____
    / _  |   Frida 16.2.1 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)
[Android Emulator 5554::Mini For Facebook ]-> console.log("test");
test
[Android Emulator 5554::Mini For Facebook ]-> exit

Thank you for using Frida!
(base) taniajaswal@Tanias-MacBook-Pro / % frida -U --codeshare akabe1/frida-multiple-unpinning -f com.Gold_Finger.V.X.your_Facebook

     ____
    / _  |   Frida 16.2.1 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Android Emulator 5554 (id=emulator-5554)
Spawned `com.Gold_Finger.V.X.your_Facebook`. Resuming main thread!
[Android Emulator 5554::com.Gold_Finger.V.X.your_Facebook ]->
======
[#] Android Bypass for various Certificate Pinning methods [#]
======
[-] OkHTTPv3 {1} pinner not found
[-] OkHTTPv3 {2} pinner not found
[-] OkHTTPv3 {3} pinner not found
[-] OkHTTPv3 {4} pinner not found
[-] Trustkit {1} pinner not found
[-] Trustkit {2} pinner not found
[-] Trustkit {3} pinner not found
[-] Appcelerator PinningTrustManager pinner not found
[-] Fabric PinningTrustManager pinner not found
[-] OpenSSLSocketImpl Conscrypt {1} pinner not found
[-] OpenSSLSocketImpl Conscrypt {2} pinner not found
[-] OpenSSLEngineSocketImpl Conscrypt pinner not found
[-] OpenSSLSocketImpl Apache Harmony pinner not found
[-] PhoneGap sslCertificateChecker pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {1} pinner not found
[-] IBM MobileFirst pinTrustedCertificatePublicKey {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {1} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {2} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {3} pinner not found
[-] IBM WorkLight HostNameVerifierWithCertificatePinning {4} pinner not found
[-] Conscrypt CertPinManager (Legacy) pinner not found
[-] CWAC-Netsecurity CertPinManager pinner not found
[-] Worklight Androidgap WLCertificatePinningPlugin pinner not found
[-] Netty FingerprintTrustManagerFactory pinner not found
[-] Squareup CertificatePinner {1} pinner not found
[-] Squareup CertificatePinner {2} pinner not found
[-] Squareup OkHostnameVerifier check not found
[-] Squareup OkHostnameVerifier check not found
[-] Android WebViewClient {3} check not found
[-] Apache Cordova WebViewClient check not found
[-] Boye AbstractVerifier check not found
[-] Chromium Cronet pinner not found
[-] Flutter HttpCertificatePinning pinner not found
```

Mini for Facebook App Traffic Captured ->



#	Host	Method	URL	Status code	Length	MIME type	Extension	Title	TLS	IP	Time
1206	http://connectivitycheck.gstatic...	GET	/generate_204	204	146					142.250.68.3	02:19:57 9 M...
1207	http://www.google.com	GET	/gen_204	204	1087	HTML				142.250.189.4	02:19:57 9 M...
1208	http://my-goldfinger.com	GET	/save_is_save.html			HTML	html			unknown host	02:20:00 9 M...
1209	http://connectivitycheck.gstatic...	GET	/generate_204	204	146					142.250.191.131	02:24:30 9 M...
1210	http://www.google.com	GET	/gen_204	204	1087	HTML				172.217.4.36	02:24:30 9 M...
1211	http://connectivitycheck.gstatic...	GET	/generate_204	204	146					142.250.191.131	02:24:40 9 M...
1212	http://my-goldfinger.com	GET	/save_is_save.html			HTML	html			unknown host	02:24:44 9 M...
1213	https://accounts.google.com	POST	/ListAccounts?gpsia=1&source=Chro...	200	1723	JSON				142.251.2.84	02:29:10 9 M...
1214	https://update.googleapis.com	POST	/service/update2/json?cup2key=10:5...	200	3773	JSON				142.250.190.35	02:30:10 9 M...
1215	http://connectivitycheck.gstatic...	GET	/generate_204	204	146					142.250.189.3	02:35:29 9 M...
1216	https://rg.appserver-ap.com	POST	/t/v0VlispXS4jMoyE1yZUOdDWYmE...							13.248.169.48	02:43:07 9 M...
1217	https://www.facebook.com	GET	/notes/gold-finger/gold-finger/176022...	302	530	HTML				157.240.22.35	02:43:08 9 M...
1218	https://m.facebook.com	GET	/home.php?sk=h_chr	302	4355	HTML	php			157.240.22.35	fr=0xAHggaSwuR... 02:43:08 9 M...
1219	https://m.facebook.com	GET	/notes/gold-finger/gold-finger/176022...	200	34440	HTML		Content Not Found		157.240.22.35	datr=PD3sZV2TvL... 02:43:08 9 M...
1220	https://m.facebook.com	GET	/login.php?next=https%3A%2F%2Fm...	200	57856	HTML	php	Log into Facebook | Fac...		157.240.22.35	datr=_I_nZbgGAv... 02:43:08 9 M...
1222	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcMCQn44TfbwnnO...	200	4703	script				157.240.22.35	fr=0xAHggaSwuR... 02:43:09 9 M...
1223	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcMCQn44TfbwnnO...	200	4705	script				157.240.22.35	fr=0xAHggaSwuR... 02:43:10 9 M...
1224	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcMCQn44TfbwnnO...	200	4703	script				157.240.22.35	fr=0xAHggaSwuR... 02:43:24 9 M...
1225	https://m.facebook.com	POST	/login/device-based/login/async/?nex...	200	10295	script				157.240.22.35	fr=0xAHggaSwuR... 02:43:24 9 M...
1226	https://static.xx.fbcdn.net	GET	/rsrc.php/v3/yl/r/XUZ99Q-vnn1.js?_n...	200	14564	script	js			157.240.22.25	02:43:26 9 M...
1227	https://static.xx.fbcdn.net	GET	/rsrc.php/v3/yU/r/ORwq2Kw9Et0.js?...	200	7780	script	js			157.240.22.25	02:43:26 9 M...
1228	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcMCQn44TfbwnnO...	200	4703	script				157.240.22.35	fr=0xAHggaSwuR... 02:43:27 9 M...
1229	https://m.facebook.com	GET	/reg/?logger_id&is_two_steps_login=0...	200	101976	HTML		Join Facebook		157.240.22.35	fr=0xAHggaSwuR... 02:43:36 9 M...

```
GET /notes/gold-finger/gold-finger/1760228594246191?wtsid=
 rdr_0SVpHU1r3INMqqPVD HTTP/2
Host: m.facebook.com
Accept-Encoding: gzip, deflate, br
User-Agent: Dalvik/2.1.0 (Linux; U; Android 12; sdk_gphone64_arm64
 Build/SE1A.220630.001.A1)
Connection: Keep-Alive
```

```
HTTP/2 200 OK
Vary: Accept-Encoding
Set-Cookie: datr=PD3sZV2TvLItP68wdGWDUF8p; expires=Sun, 13-Apr-2025 10:43:08 GMT;
 Max-Age=34560000; path=/; domain=.facebook.com; secure; httponly; SameSite=None
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Expires: Sat, 01 Jan 2000 00:00:00 GMT
Content-Security-Policy: default-src data: blob: 'self' https://*.fbsbx.com
 'unsafe-inline' *.facebook.com *.fbcdn.net 'unsafe-eval';script-src
 *.facebook.com *.fbcdn.net *.facebook.net *.google-analytics.com *.google.com
 127.0.0.1:* 'unsafe-inline' blob: data: 'self' connect.facebook.net
 'unsafe-eval';style-src fonts.googleapis.com *.fbcdn.net data: *.facebook.com
 'unsafe-inline';connect-src *.facebook.com facebook.com *.fbcdn.net
 *.facebook.net wss://*.facebook.com:* wss://*.whatsapp.com:* wss://*.fbcdn.net
 attachment.fbsbx.com ws://localhost:* blob: *.cdninstagram.com 'self'
 http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com
 wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ v.whatsapp.net
 *.fbsbx.com *.fb.com;font-src data: *.gstatic.com *.facebook.com *.fbcdn.net
 *.fbsbx.com;img-src *.fbcdn.net *.facebook.com data: https://*.fbsbx.com
 facebook.com *.cdninstagram.com fbsbx.com fbcdn.net connect.facebook.net
 *.carriersignal.info blob: android-webview-video-poster:
 googleads.g.doubleclick.net www.googleadservices.com *.whatsapp.net *.fb.com
 *.oculuscdn.com *.tenor.co *.tenor.com *.giphy.com;media-src *.cdninstagram.com
 blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data: *.tenor.co
 *.tenor.com https://*.giphy.com;frame-src *.doubleclick.net *.google.com
 *.facebook.com www.googleadservices.com *.fbsbx.com fbsbx.com data:
```

1743	https://m.facebook.com	POST	/a/bz?fb_dtsg=NAcNHKxz590cTos9zpwvp7U8TC9hd4m7fES...	✓
1744	https://m.facebook.com	GET	/sem_campaigns/sem_pixel_test/?category=5&src=https%3A...	✓

Request

```
POST /a/bz?fb_dtsg=
NAcPveOBepqqnQz4KkfRrodk_iaiS14cEkIGOtESF-iqmGChpfamFEQ%3A43%3A1709981098&
jazoest=25715&lsd=sgAH7RVqkvxIT5ponG0Pj1&__dyn=
1KQEGiE5q5U5yfDg9ppoW5UqxKcwRwAxu3-UcodUbEdEc8uK0AUlxK4o2fwcW4o3Bw4Ewk9EdEnw65
xO0FE6S0x81vohwlE16U52229wcq0DUdE2IzU2Xwp834wmE2ewnE2Lx-220n6azo11E2ZwrU6C2-0l
e0ue&__csr=&__req=5&__a=
AYnCO7Xj3DFnoK5uoFgs3zLaa9VIA5aAiH8Gqzx1P1Jfsq4s54gfG9JzNHzHfBtAFvysw95a0Ni-GU
VfZQSFzPJBrn6VoX3MVXvUQxa5yitI5w&__user=61557365424661 HTTP/2
Host: m.facebook.com
Cookie: ps_l=0; ps_n=0; datr=_I_nZbgGAvqgUW7lVv7dOZvH; sb=
_Y_nZY18oSlej1pccj2jwDT7; m_pixel_ratio=2.75; locale=en_US; fr=
0xAHggaSwuRmaK2HM.AWUHtDrv-laKTn8mbwEyNUHFXyY.Bl54_9..AAA.0.0.Bl7D2f.AWXB0x8I1
dI; c_user=61557365424661; xs=43%3A001Q8UkKrhJNxQ%3A2%3A1709981098%3A-1%3A-1;
m_page_voice=61557365424661; x-referer=
eyJyIjoiL2NvbmZpcm1lbWFpbC5waHA%2FbmV4dD1odHRwcyUzQSUyRiUyRm0uZmFjZWJvb2suY29t
JTJGaG9tZS5waHAlM0ZzayUzRGhfY2hyJnBhaXB2PTAmZWF2PUFmYXM2MmJzUENHMTlLaGptWE95ZF
BjSkM4YWs2SDh2TEVVQ2RyMy1kYW9xWUhERWs1Q2lzWDQ2RjZ5TmFFa05OWGcmc29mdD1oamsiLCJo
IjoiL2NvbmZpcm1lbWFpbC5waHA%2FbmV4dD1odHRwcyUzQSUyRiUyRm0uZmFjZWJvb2suY29tJTJG
aG9tZS5waHAlM0ZzayUzRGhfY2hyJnBhaXB2PTAmZWF2PUFmYXM2MmJzUENHMTlLaGptWE95ZFBjSk
M4YWs2SDh2TEVVQ2RyMy1kYW9xWUhERWs1Q2lzWDQ2RjZ5TmFFa05OWGcmc29mdD1oamsiLCJzIjoi
bSJ9; wl_cbv=v2%3Bclient_version%3A2429%3Btimestamp%3A1709981171; vpd=
v1%3B658x393x2.75; wd=393x708
Content-Length: 1071
X-Fb-Lsd: sgAH7RVqkvxIT5ponG0Pj1
X-Requested-With: XMLHttpRequest
X-Asbd-Id: 129477
```

Response

```
HTTP/2 200 OK
Reporting-Endpoints:
coop_report="https://www.facebook.
coep_report="https://www.facebook.
default="https://m.facebook.com/aj
 permissions_policy="https://www.f
Report-To:
{"max_age":2592000,"endpoints":[{"
ting\/coop\/?minimize=0"}],"group"
{"max_age":86400,"endpoints":[{"ur
ng\/coep\/?minimize=0"}],"group":"
{"max_age":259200,"endpoints":[{"u
or_reports\/?device_level=unknown"
{"max_age":21600,"endpoints":[{"ur
rror_reports\/"}],"group":"permiss
Content-Security-Policy: default-s
'unsafe-inline' *.facebook.com *.f
*.facebook.com *.fbcdn.net *.faceb
127.0.0.1:* 'unsafe-inline' blob:
'unsafe-eval';style-src fonts.goog
'unsafe-inline';connect-src *.face
*.facebook.net wss://*.facebook.co
attachment.fbsbx.com ws://localhos
http://localhost:3103 wss://gatewa
wss://snaptu-d.facebook.com wss://
*.fbsbx.com *.fb.com;font-src data
```

Search 0 highlights

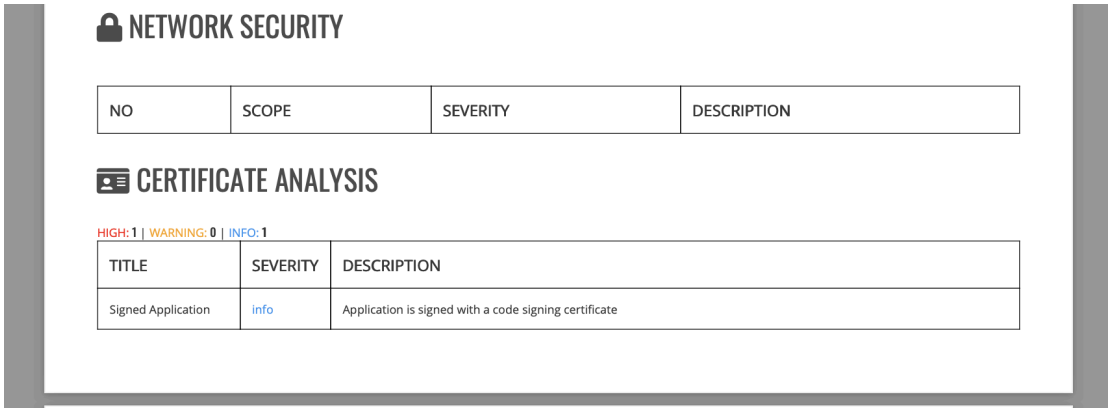
Search

MASVS-NETWORK-2

MASVS-NETWORK-2 mandates encrypting data in transit to secure sensitive information exchanged between mobile apps and servers, mitigating interception risks and ensuring compliance with industry standards.

1. MobSF did detect the SSL certificate pinning mechanisms in the app. The app passes this test.

13	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	b/v.java org/a/a/b.java



NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 1 | WARNING: 0 | INFO: 1

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

Conclusion for MASVS NETWORK :

The final project app demonstrates a robust communication protocol, adhering to MASVS standards for network security. No plaintext traffic or clear text credentials were observed during testing. The app uses TLS supported by HTTP/2, ensuring secure communication with the server. Additionally, certificate pinning mechanisms were detected as the app uses SSL pinning to detect attacks. Overall, the app's communication architecture meets security best practices and ensures the confidentiality and integrity of user data during transmission.

MASVS Platform Interaction

MASVS-PLATFORM-1

MASVS-PLATFORM-1 necessitates the secure implementation of Inter-Process Communication (IPC) mechanisms within the mobile application, ensuring that communication between different processes or components is protected against unauthorized access, data leakage, or manipulation. Compliance involves practices such as implementing proper access controls, encrypting sensitive data, using secure communication channels, and validating input to prevent exploitation vulnerabilities, thus maintaining the integrity and confidentiality of inter-process communication and aligning with best practices for secure application development.

Testing Conducted for MASVS-PLATFORM-1:

1. **Testing for App Permissions-**

These are the app permissions that the app uses-

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="156"
    android:versionName="3.3.3"
    android:installLocation="auto"
    package="com.Gold_Finger.V.X.your_Facebook">
    <uses-sdk
        android:minSdkVersion="16"
        android:targetSdkVersion="26"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_GPS"/>
    <uses-permission android:name="android.permission.ACCESS_ASSISTED_GPS"/>
    <uses-permission android:name="android.permission.ACCESS_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.VIBRATE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-feature android:name="android.hardware.camera"/>
    <uses-permission android:name="android.permission.USE_FINGERPRINT"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <application
        android:theme="@style/AppTheme"
        android:label="@string/app_name"
```

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/24	android.permission.READ_PHONE_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_ACCOUNTS, android.permission.VIBRATE, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.READ_EXTERNAL_STORAGE
Other Common Permissions	1/45	android.permission.CHANGE_WIFI_STATE

In evaluating app permissions, several potentially risky permissions were identified, including ACCESS_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_FINE_LOCATION, CAMERA, WRITE_EXTERNAL_STORAGE, and READ_EXTERNAL_STORAGE. According to the Mobsf report, there are indications that the app might be misusing these permissions, raising concerns about potential abuse. Consequently, based on these findings, the test results are deemed unsuccessful.

2. **Testing Deep Links-**

The test for deep links yielded no discoveries within the app, as no deep links were detected in the XML file, indicating a lack of data elements associated with intents. Based on this outcome, it can be concluded that the test was successful.

3. **Testing for Sensitive Functionality Exposure Through IPC-**

The test aimed at uncovering sensitive functionality exposure through Inter-Process Communication (IPC) highlighted that none of the activities were exported except for the service elements. However, the only activity with an intent filter was identified as com.Gold_Finger.p037V.p038X.your_Facebook.MainActivity serves as the main activity for the app. The test passes.

```
            android:name="com.apptracker.android.module.AppModuleActivity"
            android:configChanges="screenSize|orientation|keyboardHidden|keyboard"
            android:hardwareAccelerated="false"/>
        <service android:name="com.apptracker.android.track.AppTrackerService"/>
        <meta-data
            android:name="android.support.VERSION"
            android:value="26.1.0"/>
        <activity
            android:theme="@style/IntroductionActivityStyle"
            android:name="com.rubengees.introduction.IntroductionActivity"/>
        <service
            android:name="com.pro100svitlo.fingerprintAuthHelper.FahTimeOutService"
            android:enabled="true"
            android:exported="true"/>
        <activity
            android:theme="@android:style/Theme.Translucent"
            android:name="com.google.android.gms.ads.AdActivity"
            android:exported="false"
            android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"/>
        <activity
            android:theme="@android:style/Theme.Translucent.NoTitleBar"
            android:name="com.google.android.gms.common.api.GoogleApiActivity"
            android:exported="false"/>
        <service
            android:name="com.txusballesteros.bubbles.BubblesService"
            android:enabled="true"
            android:exported="false"/>
        <receiver
            android:name="com.opensignal.datacollection.schedules.monitors.InstallReferrerReceiver"
            android:exported="true"
            android:process=":ndc_background_sdk"/>
        <receiver
            android:name="com.opensignal.datacollection.schedules.monitors.BootReceiver"
            android:process=":ndc_background_sdk">
```

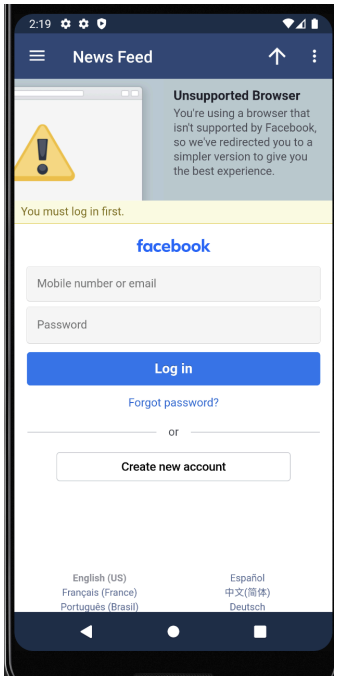
```
    <activity
        android:label="@string/app_name"
        android:name="com.Gold_Finger.p037V.p038X.your_Facebook.MainActivity"
        android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"
        android:noHistory="false">
        <intent-filter>
            <action android:name="android.intent.action.MAIN"/>
            <category android:name="android.intent.category.LAUNCHER"/>
            <category android:name="android.intent.category.DEFAULT"/>
        </intent-filter>
    </activity>
```

3	Service (com.pro100svitlo.fingerprintAuthHelper.FahTimeOutService) is not Protected. [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Broadcast Receiver (com.opensignal.datacollection.schedules.monitors.InstallReferrerReceiver) is not Protected. [android:exported=true]	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.

NO	ISSUE	SEVERITY	DESCRIPTION
5	Broadcast Receiver (com.opensignal.datacollection.schedules.monitors.BootReceiver) 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.
6	Broadcast Receiver (com.opensignal.datacollection.schedules.monitors.BatteryLowReceiver) 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.
7	Broadcast Receiver (com.opensignal.datacollection.schedules.monitors.BatteryOkayReceiver) 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.
8	Broadcast Receiver (com.opensignal.datacollection.schedules.monitors.PowerConnectedReceiver) 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.
9	Broadcast Receiver (com.opensignal.datacollection.schedules.monitors.PowerDisconnectedReceiver) 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.

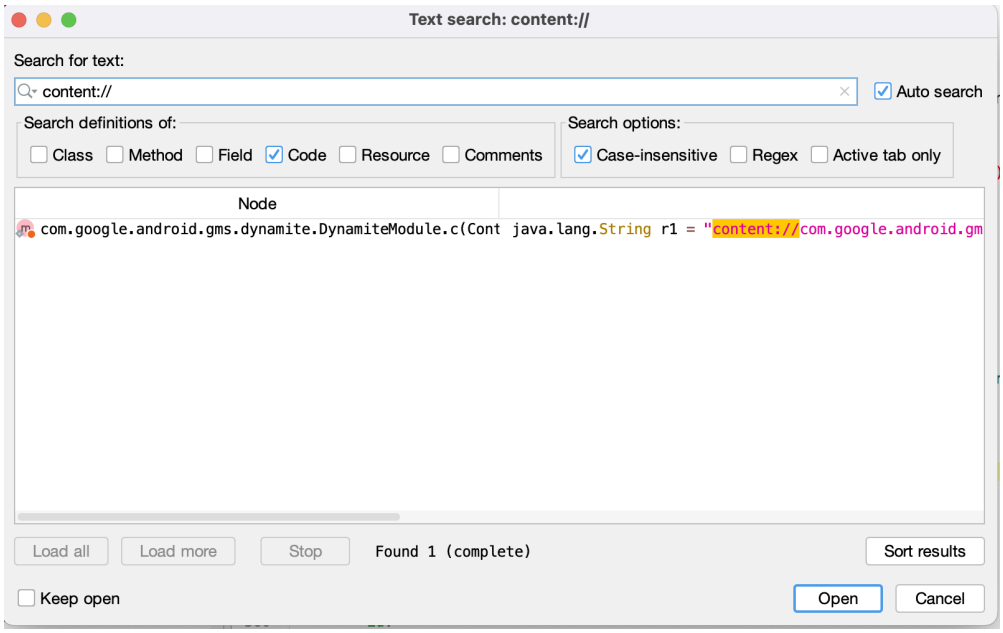
```
(base) taniajaswal@Tanias-MacBook-Pro platform-tools % ./adb shell am start -n com.Gold_Finger.V.X.your_Facebook/.MainActivity

Starting: Intent { cmp=com.Gold_Finger.V.X.your_Facebook/.MainActivity }
(base) taniajaswal@Tanias-MacBook-Pro platform-tools %
```



4. **Determining Whether Sensitive Stored Data Has Been Exposed via IPC Mechanisms-**

The assessment aimed at determining whether sensitive stored data had been exposed via Inter-Process Communication (IPC) mechanisms revealed that the app lacked any associated content providers. As a result, the test is considered successful, indicating that sensitive stored data has not been exposed via IPC mechanisms.

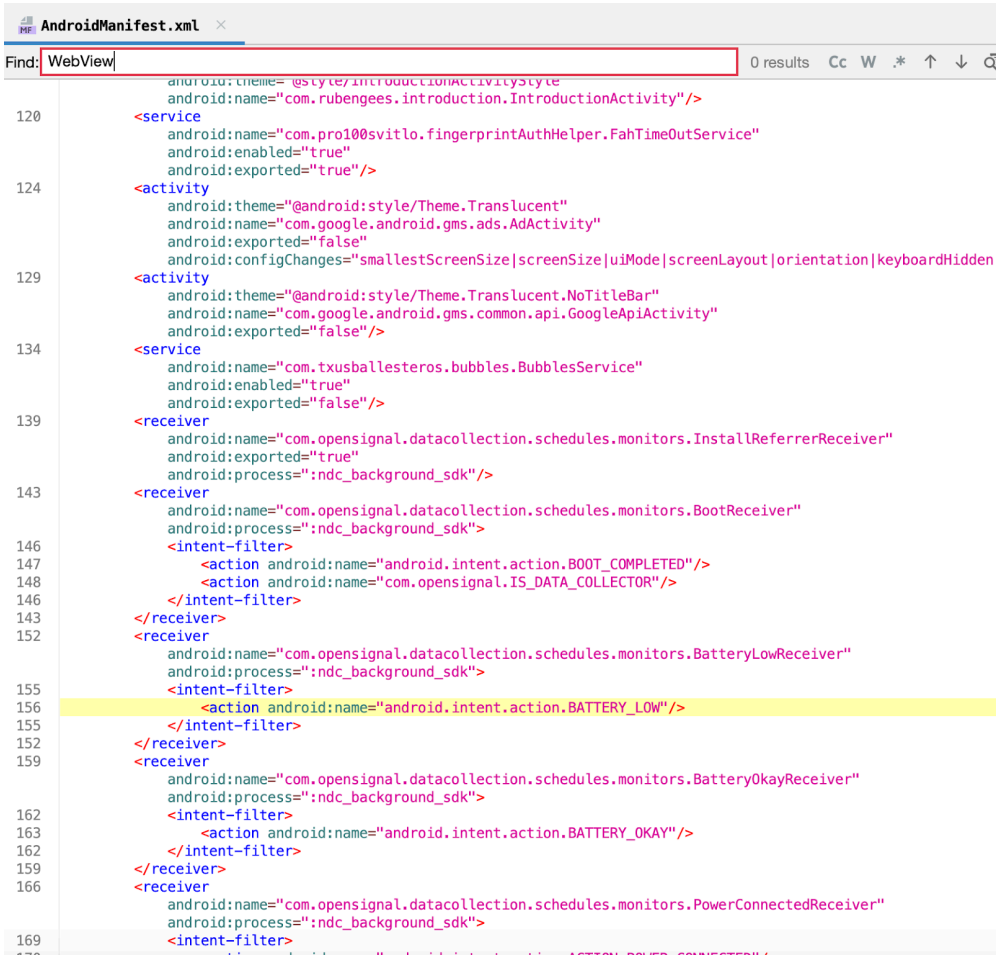


MASVS-PLATFORM-2

MASVS-PLATFORM-2 requires securely integrating and using WebViews in the mobile app to mitigate web-related security risks. Compliance involves implementing measures like input validation, output encoding, and Content Security Policy enforcement. This ensures consistent security across different app components using web content, enhancing overall security against malicious attacks.

1. **Testing WebView Protocol Handlers-**

After Checking for “android.webkit.WebView.EnableSafeBrowsing” in AndroidManifest.xlm, it is not present hence safe browsing is enabled. Tested how the Webview was handled in the app. This test passed since safe browsing is enabled.

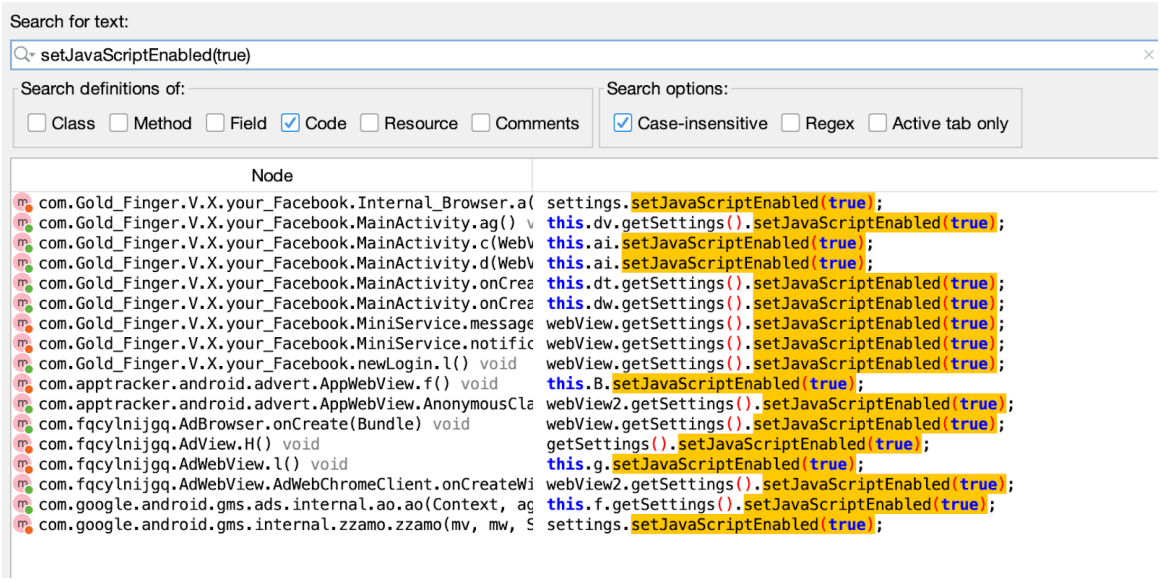


2. Testing JavaScript Execution in WebViews-

The setJavaScriptEnabled is set to true in the application's com file. The test failed as the javascript execution is set to true in the app.

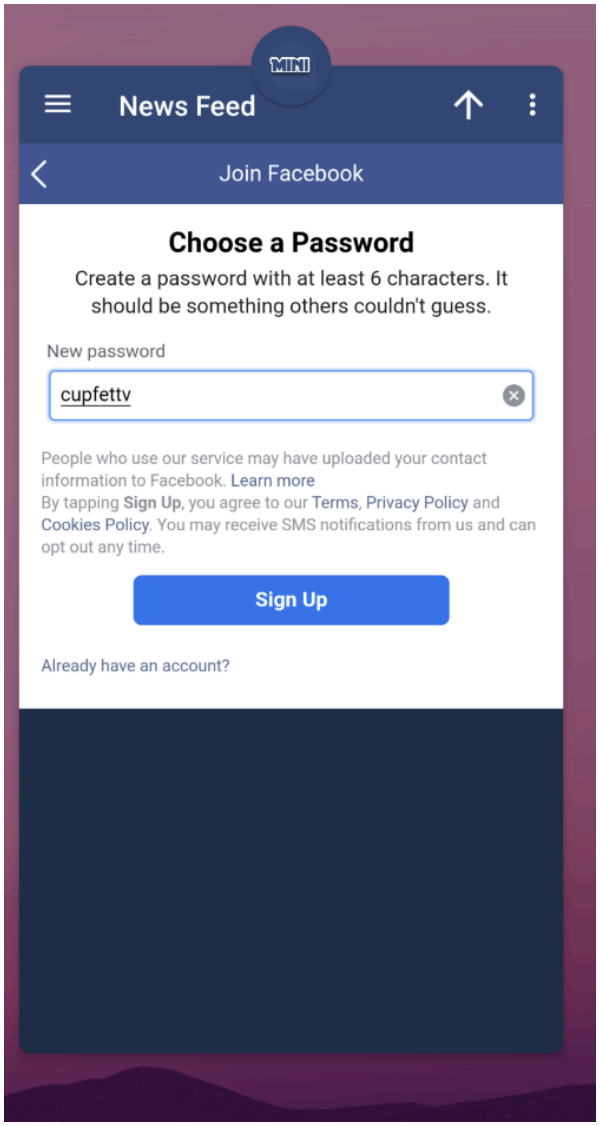
```
@SuppressLint({"SetJavaScriptEnabled"})
private void a(WebView webView) {
    WebSettings settings = webView.getSettings();
    settings.setJavaScriptEnabled(true);
    settings.setAppCacheEnabled(true);
    settings.setSupportZoom(true);
    settings.setAppCacheMaxSize(1L);
    settings.setSaveFormData(false);
    settings.setBuiltInZoomControls(true);
    if (Build.VERSION.SDK_INT >= 11) {
        settings.setDisplayZoomControls(false);
    }
    settings.setGeolocationEnabled(true);
    settings.setCacheMode(1);
    webView.setBackgroundColor(Color.parseColor("#ffffff"));
    if (Build.VERSION.SDK_INT >= 19) {
        webView.setLayerType(2, null);
    } else if (Build.VERSION.SDK_INT >= 11) {
        webView.setLayerType(1, null);
    }
    webView.setHapticFeedbackEnabled(true);
    webView.setLongClickable(true);
    if ((this.ak == 2 || this.ak == 3) && Build.VERSION.SDK_INT > 13) {
        settings.setUserAgentString("Mozilla/5.0 (Macintosh; Intel Mac OS
    }
}

/* JADX INFO: Access modifiers changed from: private */
@SuppressLint({"SimpleDateFormat"})
```



MASVS-PLATFORM-3

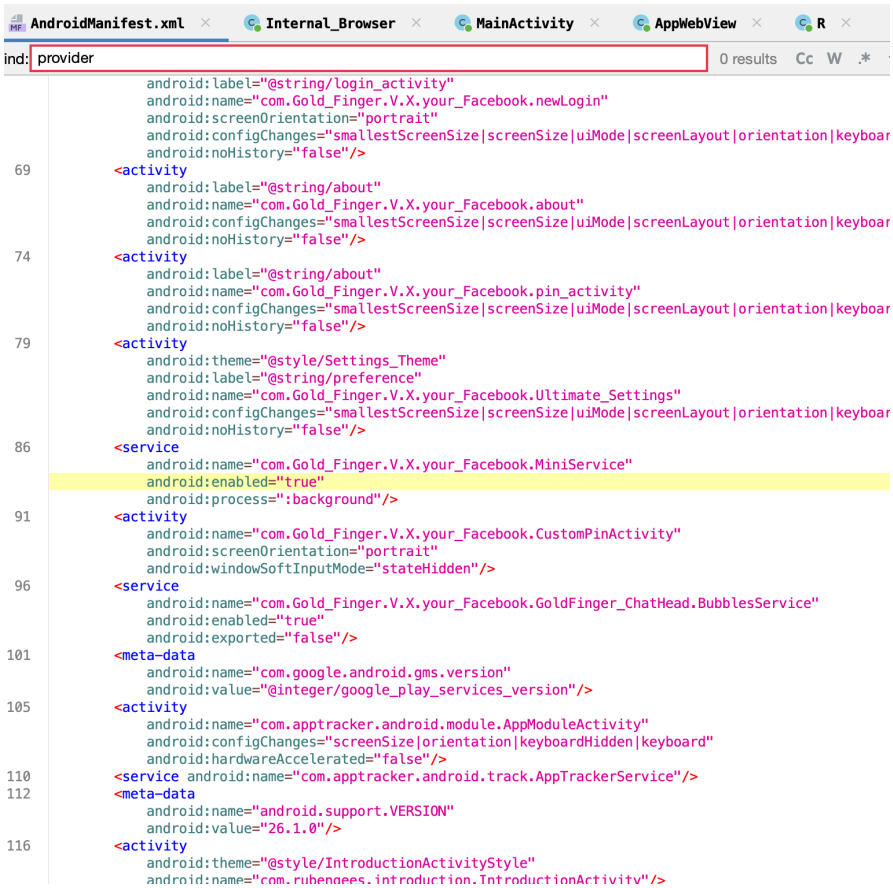
1. **Finding Sensitive Information in Auto-Generated Screenshots-**

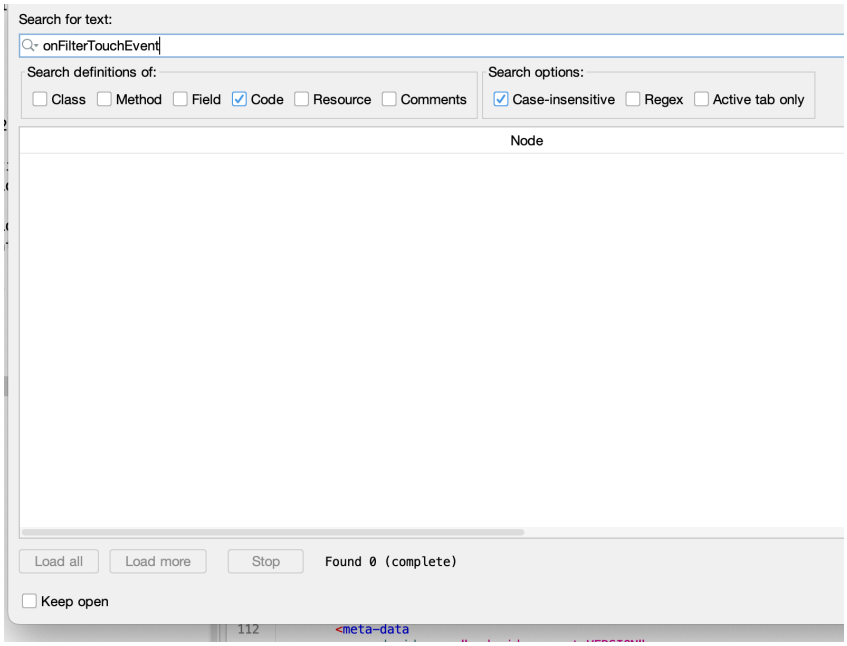


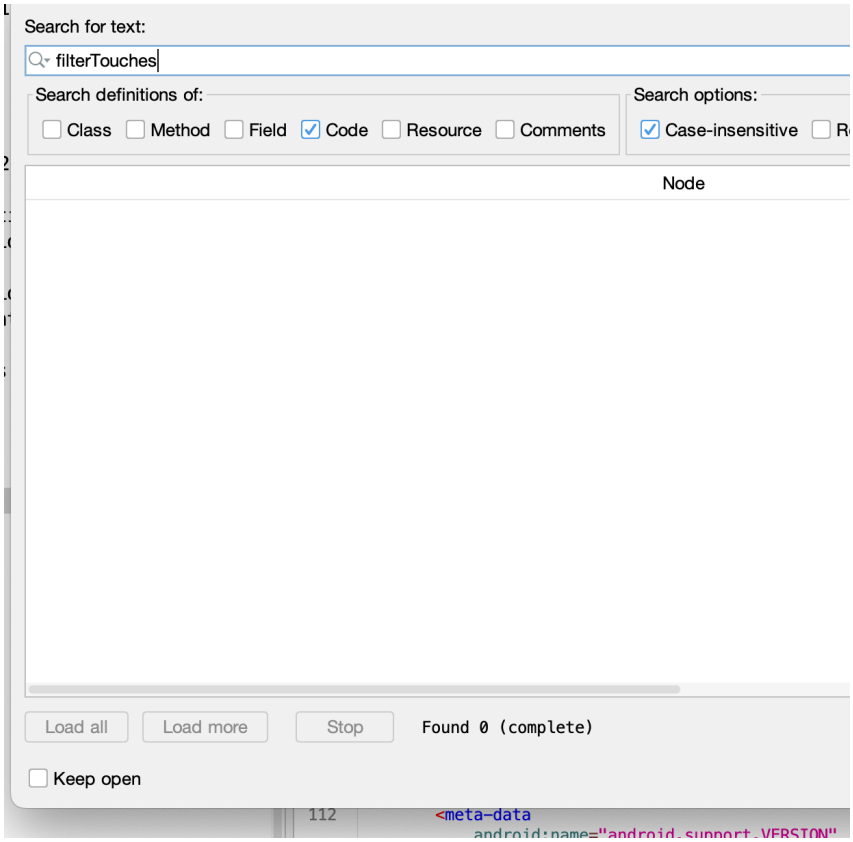
The FLAG_SECURE flag has not been set so the activity information is being shown. This test failed as we were able to find relevant information on the app and how it protects sensitive information.

2. Testing for Overlay Attacks-

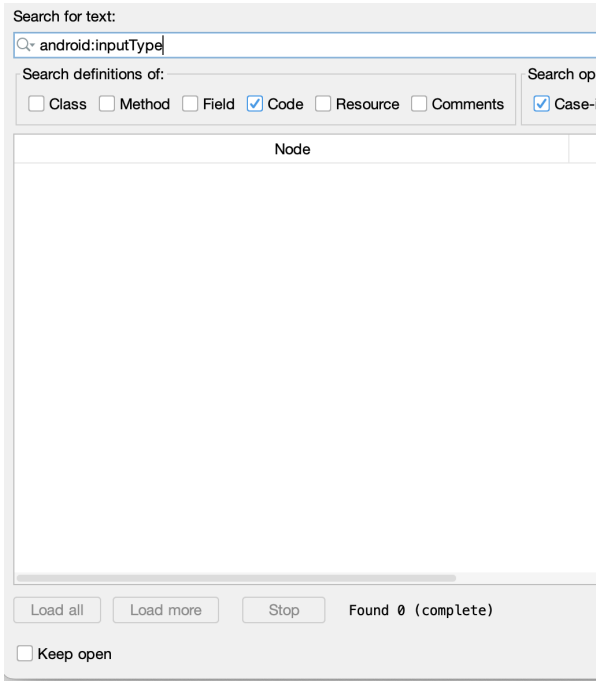
This can not be tested on the app since it doesn't have any content providers in the manifest. So, the test passes due to no content element. The app doesn't use any of the onFilterTouchEventForSecurity, android:filterTouchesWhenObscured, and FLAG_WINDOW that could be used to overlay or override. This test passed since no information could be found.

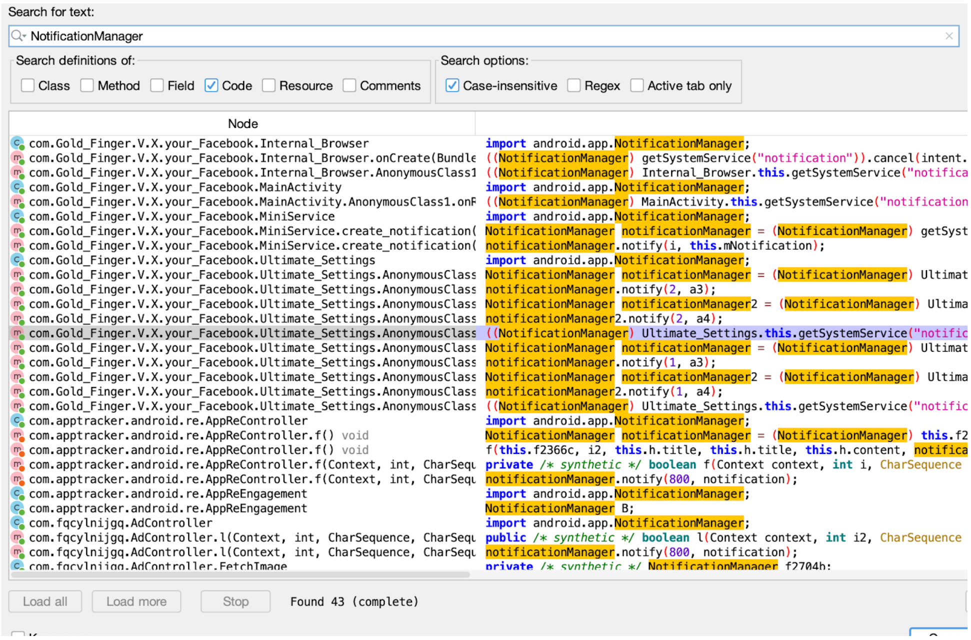



Search for text:
onFilterTouchEvent
Search definitions of:
Class
Method
Field
Code
Resource
Comments
Search options:
Case-insensitive
Regex
Active tab only
Node
Load all
Load more
Stop
Found 0 (complete)
Keep open
112
<meta-data


Search for text:
filterTouches
Search definitions of:
Class
Method
Field
Code
Resource
Comments
Search options:
Case-insensitive
Node
Load all
Load more
Stop
Found 0 (complete)
Keep open
112
<meta-data
android:name="android.support.VERSION"

3. Checking for Sensitive Data Disclosure Through the User Interface-





The app doesn't use any hard-coded input type password which suggests that the passwords are handled correctly. The app uses the Notification Manager function to manage the notifications that are sent from the app. The app doesn't disclose any sensitive data through any password leak. The use of sensitive data is completely removed. Hence, the test passes.

Conclusion for MASVS PLATFORM:

In summary, the testing conducted for MASVS-PLATFORM standards showcased a comprehensive assessment of various security aspects within the mobile application. While certain areas demonstrated successful compliance, such as the secure usage of WebViews, implementation of safe browsing, and absence of sensitive data disclosure through the user interface, other areas highlighted potential vulnerabilities. These include concerns regarding the misuse of app permissions, issues with JavaScript execution in WebViews, and exposure of sensitive information in auto-generated screenshots. However, positive outcomes were also observed, such as the absence of deep links and vulnerability to overlay attacks. Overall, the evaluation underscores a proactive approach to enhancing the application's security posture while identifying areas for further improvement to meet MASVS standards comprehensively.

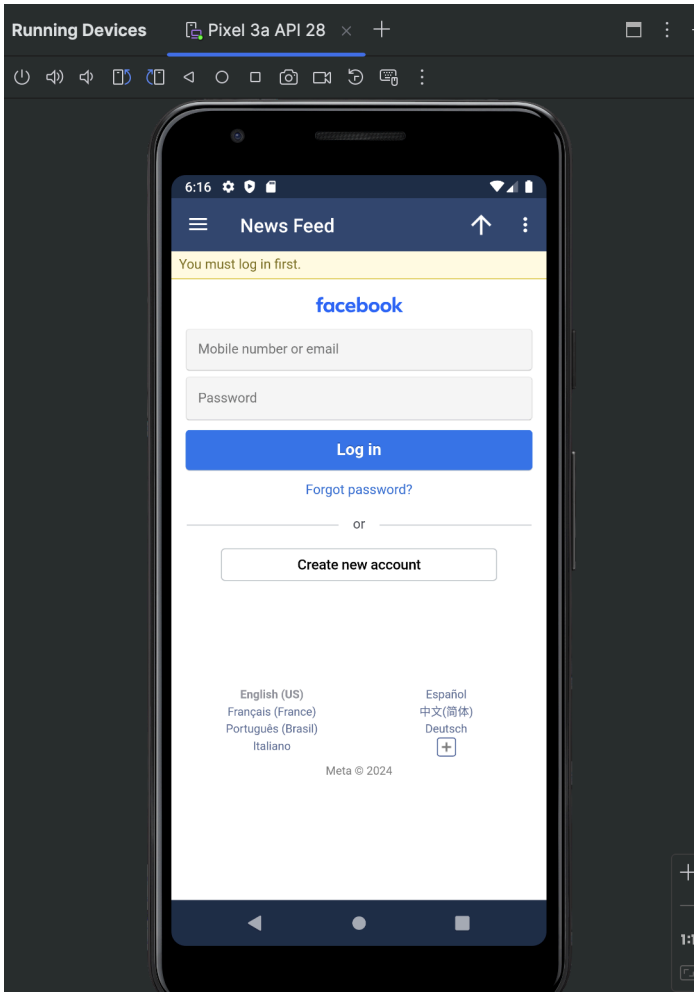
MASVS Code Quality and Build Settings

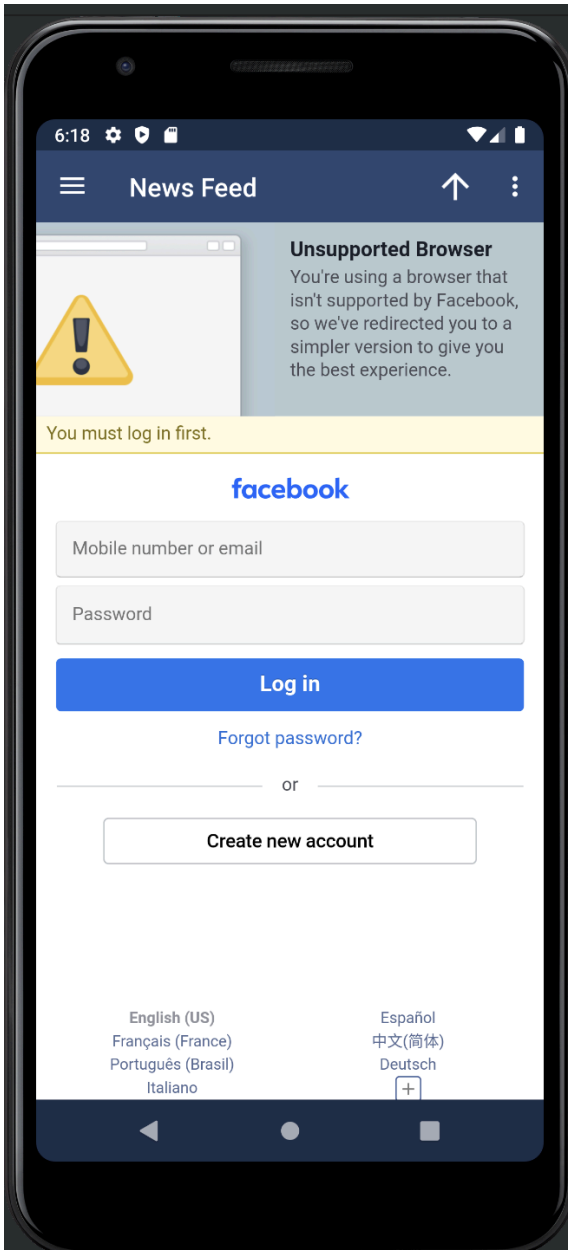
MASVS-CODE-1

MASVS-CODE-1 mandates that the mobile application necessitates an up-to-date platform version, emphasizing the importance of using the latest operating system and software updates. This requirement aims to mitigate security vulnerabilities by ensuring compatibility with the most recent security patches and enhancements, thereby enhancing the overall security posture of the application.

1. **Check if the app runs on the unsupported Android version-**

The app does run on the unsupported Android version 28. Hence, this test failed.




6:18
News Feed
Unsupported Browser
You're using a browser that isn't supported by Facebook, so we've redirected you to a simpler version to give you the best experience.
You must log in first.
facebook
Mobile number or email
Password
Log in
Forgot password?
or
Create new account
English (US)
Français (France)
Português (Brasil)
Italiano
Español
中文(简体)
Deutsch

MASVS-CODE-2

In the testing process, an older version of the Mini for Facebook APK was downloaded, with two different options explored. Both downloads resulted in the same error message, indicating the utilization of an unsupported version, thereby hindering Facebook login. This test passes, demonstrating successful observation of the app's handling of older versions and its implementation of appropriate version compatibility checks.


6:43
Log in Disabled
For your account security, logging into Facebook from an embedded browser is disabled. You may be able to continue by updating the app you're logging in from and trying again.

MASVS-CODE-3

In the binary analysis section, no vulnerable libraries were identified in the Mobsf report. As a result, no conclusions could be drawn regarding potential vulnerabilities. This test passes, indicating that no concerning findings were detected during the analysis of the binary.

NO	ISSUE	SEVERITY	STANDARDS	FILES
14	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	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	com/pro100svitlo/fingerprintAuthHelper/d.java
15	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/github/javiersantos/appupdater/k.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

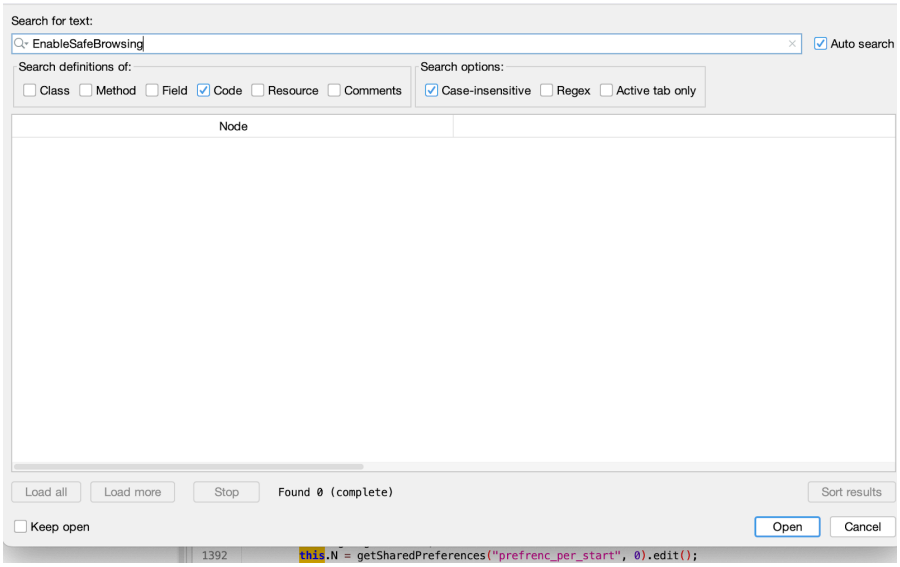
ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	13/24	android.permission.READ_PHONE_STATE, android.permission.SYSTEM_ALERT_WINDOW, android.permission.INTERNET, android.permission.ACCESS_WIFI_STATE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.CAMERA, android.permission.RECEIVE_BOOT_COMPLETED, android.permission.GET_ACCOUNTS, android.permission.VIBRATE.

MASVS-CODE-4

1. **Testing for URL Loading in WebViews-**

The examination for URL loading in WebViews revealed the absence of "EnableSafeBrowsing" in the manifest file. As this feature was not detected, it can be inferred that safe browsing is enabled by default. Therefore, this test is considered successful, confirming the presence of safe browsing functionality within the application's WebViews.



2. **Testing for Injection Flaws-**

The assessment revealed no presence of deep links within the app, as confirmed by the absence of data elements in the XML file and no exported activities except for service elements. Furthermore, the main activity, com.Gold_Finger.p037V.p038X.your_Facebook.MainActivity, was identified without any intent filter. Additionally, due to the absence of content providers in the manifest and no utilization of overlay-related attributes, overlay attacks couldn't be tested but were implicitly passed. Moreover, the absence of signs of injection flaws led to the successful completion of the injection flaw test.

Conclusion for MASVS Code Quality and Build Settings:

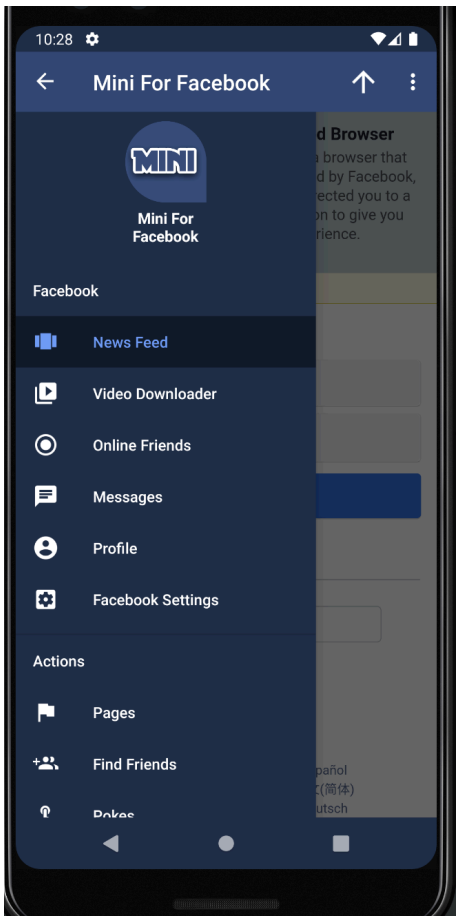
In conclusion, the evaluation of MASVS Code Quality and Build Settings encompassed several tests assessing the application's adherence to secure coding practices and platform standards. While the app failed the compatibility test for running on unsupported Android version 28 (MASVS-CODE-1), it demonstrated successful handling of older versions during login (MASVS-CODE-2). The absence of vulnerable libraries in the binary analysis (MASVS-CODE-3) and secure URL loading in WebViews (MASVS-CODE-4) further reinforced its robust security posture. Overall, these findings highlight the app's commitment to maintaining code quality and adherence to industry standards.

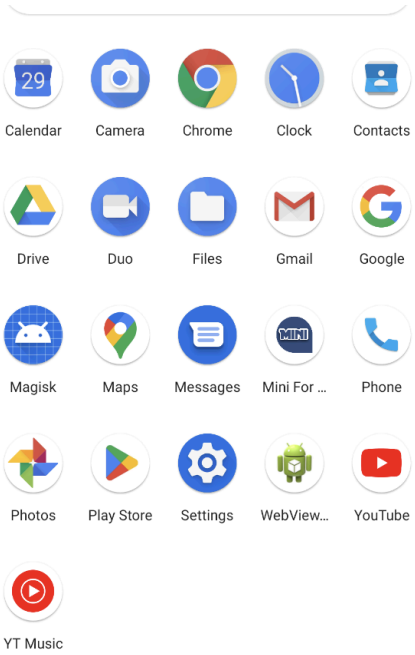
MASVS Resilience Requirements

MASVS-RESILIENCE-1

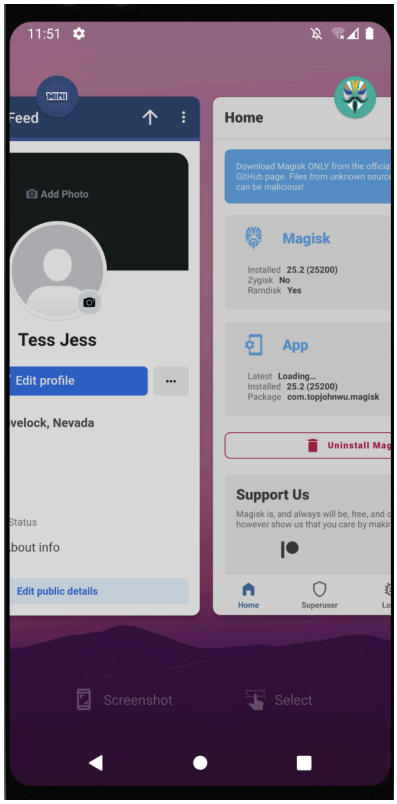
MASVS-RESILIENCE-1 mandates that the app validates the integrity of the platform. This involves verifying the authenticity and integrity of the underlying operating system and platform components to ensure they have not been tampered with or compromised. This requirement aims to mitigate risks associated with unauthorized modifications or attacks targeting the app's underlying platform, thereby enhancing its resilience against potential security threats.

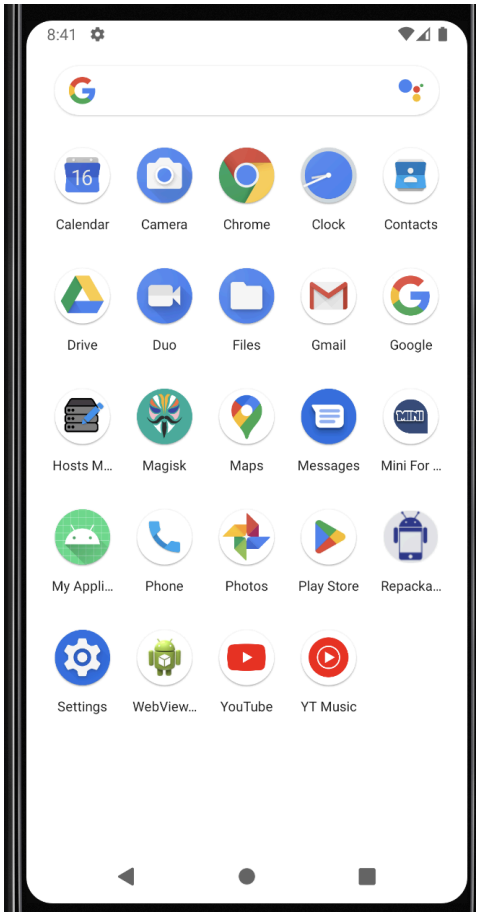
1. **The app runs on the emulator using the APK, hence the app passes this test-**





2. **The app runs on a rooted device hence the app passes this test-**




8:41
Calendar
Camera
Chrome
Clock
Contacts
Drive
Duo
Files
Gmail
Google
Hosts M...
Magisk
Maps
Messages
Mini For ...
My Appli...
Phone
Photos
Play Store
Repacka...
Settings
WebView...
YouTube
YT Music

MASVS-RESILIENCE-2

1. The app employs a valid APK signature utilizing SHA-256 with RSA. However, it relies on a v1 signature, which is insecure. The app fails the test since it uses an insecure APK signature.

```
APK signature verification result:

Signature verification succeeded
Valid APK signature v1 found

    Signer CERT.RSA (META-INF/CERT.SF)

        Type: X.509
        Version: 3
        Serial number: 0x18433ffa
        Subject: CN=Vuki Xami, OU=Budall
        Valid from: Thu Nov 13 09:39:49 PST 2014
        Valid until: Sat Nov 05 10:39:49 PDT 2044

        Public key type: RSA
        Exponent: 65537
        Modulus size (bits): 2048
        Modulus: 24915121235070212199490221998290747345740712916707843461293892807075622479337125516388706773448334192812

        Signature type: SHA256withRSA
        Signature OID: 1.2.840.113549.1.1.11

        MD5 Fingerprint: DA 6E 34 D9 27 16 18 FC CF 2B 73 C2 D8 20 7C E0
        SHA-1 Fingerprint: F2 FF 05 FA 1C EC BF CC 86 6B 65 94 E7 70 BE 7B 33 E3 CC DA
        SHA-256 Fingerprint: B4 1B C0 53 80 CC 5C 21 D9 3D 5A 7A 1D 81 4B 80 9A B1 28 14 78 0D 68 67 6C 66 E6 E0 6A 3A 4E

Warnings

    Files that are not protected by APK signature v1. Unauthorized modifications to these entries can only be detected by APK signature v2 an

        META-INF/kotlin-runtime.kotlin_module
        META-INF/kotlin-stdlib.kotlin_module
        META-INF/rxjava.properties
        META-INF/services/com.fasterxml.jackson.core.JsonFactory
```

MASVS-RESILIENCE-3

1. **MASTG-TEST-0041**

The app's use of strict mode suggests that it is implementing measures to enhance its resilience against certain types of errors or vulnerabilities. Strict mode is a programming feature that enforces stricter parsing and error handling, helping to identify potential issues and prevent them from causing system failures or security vulnerabilities. Therefore, the app's adoption of strict mode aligns with best practices for resilience and security. Overall, this aspect of the app can be considered a pass.

```
package com.google.android.gms.internal;

import android.content.Context;
import android.os.StrictMode;
import java.util.concurrent.Callable;

@awk
/* loaded from: classes.dex */
public final class hw {
    public static <T> T a(Context context, Callable<T> callable) {
        StrictMode.ThreadPolicy threadPolicy = StrictMode.getThreadPolicy();
        try {
            try {
                StrictMode.setThreadPolicy(new StrictMode.ThreadPolicy.Builder(threadPolicy).permitDiskReads().permitDiskW
                return callable.call();
            } catch (Throwable th) {
                Cif.b("Unexpected exception.", th);
                awd.a(context).a(th, "StrictModeUtil.runWithLaxStrictMode");
                StrictMode.setThreadPolicy(threadPolicy);
                return null;
            }
        } finally {
            StrictMode.setThreadPolicy(threadPolicy);
        }
    }

    public static <T> T b(Context context, Callable<T> callable) {
        StrictMode.ThreadPolicy threadPolicy = StrictMode.getThreadPolicy();
        try {
            StrictMode.setThreadPolicy(new StrictMode.ThreadPolicy.Builder(threadPolicy).permitDiskReads().permitDiskWrite
            return callable.call();
        } finally {
            StrictMode.setThreadPolicy(threadPolicy);
        }
    }
}
```

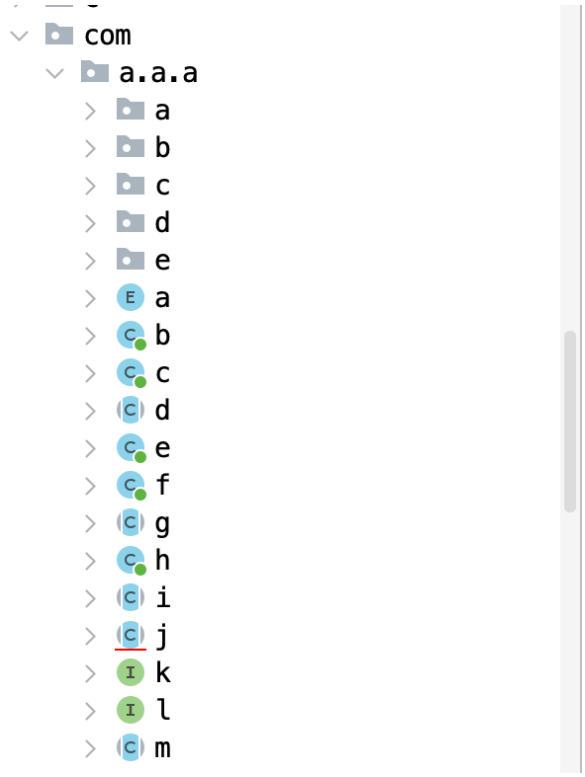
2. **MASTG-TEST-0051-**

The app contains unintelligible names for classes, methods, and variables, which makes it harder to understand the code hence obfuscating the meaning behind it.
It dynamically fetches the encryption algorithm and key generation methods from encoded strings.

```
/* renamed from: a, reason: collision with root package name */
public static final h f1721d = a("SSL_RSA_EXPORT_WITH_RC4_40_MD5", 3);
public static final h e = a("SSL_RSA_WITH_RC4_128_MD5", 4);
public static final h f = a("SSL_RSA_WITH_RC4_128_SHA", 5);
public static final h g = a("SSL_RSA_EXPORT_WITH_DES40_CBC_SHA", 8);
public static final h h = a("SSL_RSA_WITH_DES_CBC_SHA", 9);
public static final h i = a("SSL_RSA_WITH_3DES_EDE_CBC_SHA", 10);
public static final h j = a("SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA", 17);
public static final h k = a("SSL_DHE_DSS_WITH_DES_CBC_SHA", 18);
public static final h l = a("SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA", 19);
public static final h m = a("SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA", 20);
public static final h n = a("SSL_DHE_RSA_WITH_DES_CBC_SHA", 21);
public static final h o = a("SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA", 22);
public static final h p = a("SSL_DH_anon_EXPORT_WITH_RC4_40_MD5", 23);
public static final h q = a("SSL_DH_anon_WITH_RC4_128_MD5", 24);
public static final h r = a("SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA", 25);
public static final h s = a("SSL_DH_anon_WITH_DES_CBC_SHA", 26);
public static final h t = a("SSL_DH_anon_WITH_3DES_EDE_CBC_SHA", 27);
public static final h u = a("TLS_KRB5_WITH_DES_CBC_SHA", 30);
public static final h v = a("TLS_KRB5_WITH_3DES_EDE_CBC_SHA", 31);
public static final h w = a("TLS_KRB5_WITH_RC4_128_SHA", 32);
public static final h x = a("TLS_KRB5_WITH_DES_CBC_MD5", 34);
public static final h y = a("TLS_KRB5_WITH_3DES_EDE_CBC_MD5", 35);
public static final h z = a("TLS_KRB5_WITH_RC4_128_MD5", 36);
public static final h A = a("TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA", 38);
public static final h B = a("TLS_KRB5_EXPORT_WITH_RC4_40_SHA", 40);
public static final h C = a("TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5", 41);
public static final h D = a("TLS_KRB5_EXPORT_WITH_RC4_40_MD5", 43);
public static final h E = a("TLS_RSA_WITH_AES_128_CBC_SHA", 47);
public static final h F = a("TLS_DHE_DSS_WITH_AES_128_CBC_SHA", 50);
public static final h G = a("TLS_DHE_RSA_WITH_AES_128_CBC_SHA", 51);
public static final h H = a("TLS_DH_anon_WITH_AES_128_CBC_SHA", 52);
public static final h I = a("TLS_RSA_WITH_AES_256_CBC_SHA", 53);
public static final h J = a("TLS_DHE_DSS_WITH_AES_256_CBC_SHA", 56);
```

```
    }
    this.cr = getSharedPreferences("lisho_pref", 0);
    this.cy = this.cr.edit();
    this.cn = this.cr.getInt("lisho_numri", this.cn);
    this.cx = getSharedPreferences("numruesi_pref", 0);
    this.cE = this.cx.edit();
    this.cW = this.cx.getInt("numruesi_pref_numri", this.cW);
    this.cs = getSharedPreferences("koha_rate_pref", 0);
    this.cz = this.cs.edit();
    this.co = this.cs.getInt("koha_rate_numri", this.co);
    if (this.co == 0) {
        this.co = 120;
    }
    this.J = getSharedPreferences("rate_the_app_pref", 0).edit();
    this.K = getSharedPreferences("rate_the_app_pref", 0).getLong("rate_the_app_pref_numr
    this.ct = getSharedPreferences("qelsi_her_par_pref", 0);
    this.cA = this.ct.edit();
    this.cp = this.ct.getInt("qelsi_para_numri", this.cp);
    this.cu = getSharedPreferences("share_par_pref", 0);
    this.cB = this.cu.edit();
    this.cq = this.cu.getInt("share_par_pref_numri", this.cq);
    this.cv = getSharedPreferences("kto_nale_app_ri_pref", 0);
    this.cC = this.cv.edit();
    this.G = this.cv.getInt("kto_nale_appi_ri", this.G);
    if (Build.VERSION.SDK_INT > 13) {
        this.bQ = getSharedPreferences("ads_kontrolla13", 0);
        this.bS = this.bQ.edit();
        this.cX = this.bQ.getInt("ads_kontrolla_numri13", this.cX);
        this.bU = b((Context) this, "ka_hy_useri_pref_numri");
        this.bP = getSharedPreferences("ads_check_prefs", 0);
        this.bR = this.bP.edit();
        this.bT = this.bP.getInt("ads_check_prefs_numri", this.bT);
        if (this.bU != 3) {
            if (this.cn == 1) {
                this.bU = 3;
                a(this, "ka_hy_useri_pref_numri", 3);
```

```
@SuppressLint({"TrulyRandom"})
public static byte[] encryptData(byte[] bArr, byte[] bArr2, byte[] bArr3) {
    try {
        Cipher cipher = Cipher.getInstance(AppDeviceParamaters.f("s\u0002ahq\u0005qhb\fq\u0014\u0007\u0017S#V.\\ "));
        SecretKeySpec secretKeySpec = new SecretKeySpec(bArr2, Triple.f("D}V"));
        int i = 16;
        byte[] bArr4 = new byte[16];
        if (bArr3.length <= 16) {
            i = bArr3.length;
        }
        System.arraycopy(bArr3, 0, bArr4, 0, i);
        cipher.init(1, secretKeySpec, new IvParameterSpec(bArr4));
        return cipher.doFinal(bArr);
    } catch (Exception e) {
        StringBuilder insert = new StringBuilder().insert(0, AppDeviceParamaters.f("^(S#s#t5]*q&Q/WgW)Q5K7F\u0003S3SgW?Q\'
        insert.append(e);
        AppLog.e(AppConstants.APPLOGTAG, insert.toString());
        return null;
    }
}
```



```
/* loaded from: classes.dex */
public class MainActivity extends e implements c {
    static boolean m;
    String A;
    WebView C;
    int F;
    int H;
    int I;
    SharedPreferences.Editor J;
    long K;
    int M;
    SharedPreferences.Editor N;
    SharedPreferences.Editor O;
    int P;
    FloatingActionButton Q;
    FloatingActionButton R;
    com.gitonway.lee.niftymodaldialogeffects.lib.c S;
    com.gitonway.lee.niftymodaldialogeffects.lib.c T;
    com.gitonway.lee.niftymodaldialogeffects.lib.c U;
    com.gitonway.lee.niftymodaldialogeffects.lib.c V;
    com.gitonway.lee.niftymodaldialogeffects.lib.c W;
    com.gitonway.lee.niftymodaldialogeffects.lib.c X;
    TextView Y;
    TextView Z;
    int aJ;
    Menu aK;
    MenuItem aL;
    WebView.HitTestResult aM;
    String aN;
    String aO;
    String aP;
    String aQ;
    SwipeRefreshLayout aR;
    SwipeRefreshLayout aS;
    SwipeRefreshLayout aT;
    TextView aW;
    String aY;
    ImageView aZ;
    TextView aa;
    View ab;
    View ac;
    View ad;
    View ae;
    int af;
```

MASVS-RESILIENCE-4

1. **MASTG-TEST-0039-**

The app is not debuggable since the debuggable is not set in AndroidManifest.xml.

Other remarks:
The app requests a broad range of permissions, including access to sensitive device information (e.g., READ_PHONE_STATE), network access (INTERNET), camera access (CAMERA), and storage access (WRITE_EXTERNAL_STORAGE, READ_EXTERNAL_STORAGE). The extensive permission requests may raise privacy concerns.
The app incorporates third-party libraries for functionalities like ads, fingerprint authentication, and app tracking.

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="156"
    android:versionName="3.3.3"
    android:installLocation="auto"
    package="com.Gold_Finger.V.X.your_Facebook">
    <uses-sdk
        android:minSdkVersion="16"
        android:targetSdkVersion="26"/>
    <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_GPS"/>
    <uses-permission android:name="android.permission.ACCESS_ASSISTED_GPS"/>
    <uses-permission android:name="android.permission.ACCESS_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
    <uses-permission android:name="android.permission.CAMERA"/>
    <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.VIBRATE"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-feature android:name="android.hardware.camera"/>
    <uses-permission android:name="android.permission.USE_FINGERPRINT"/>
    <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
    <application
        android:theme="@style/AppTheme"
        android:label="@string/app_name"
        android:icon="@drawable/splash_icon"
        android:name="com.Gold_Finger.p037V.p038X.your_Facebook.App"
        android:allowBackup="true"
        android:hardwareAccelerated="true"
        android:largeHeap="true"
        android:supportsRtl="true">
        <activity
            android:label="@string/app_name"
            android:name="com.Gold_Finger.p037V.p038X.your_Facebook.MainActivity"
            android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"
            android:noHistory="false">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
```

```
android:supportsRtl="true" >
<activity
    android:label="@string/app_name"
    android:name="com.Gold_Finger.p037V.p038X.your_Facebook.MainActivity"
    android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"
    android:noHistory="false">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
        <category android:name="android.intent.category.DEFAULT"/>
    </intent-filter>
</activity>
<activity
    android:theme="@style/Mini_bro_theme"
    android:label="Mini&apos;s Browser"
    android:name="com.Gold_Finger.p037V.p038X.your_Facebook.Internal_Browser"
    android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"
    android:noHistory="false"
    android:hardwareAccelerated="true"/>
<activity
    android:label="@string/login_activity"
    android:name="com.Gold_Finger.p037V.p038X.your_Facebook.newLogin"
    android:screenOrientation="portrait"
    android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"
    android:noHistory="false"/>
<activity
    android:label="@string/about"
    android:name="com.Gold_Finger.p037V.p038X.your_Facebook.about"
    android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"
    android:noHistory="false"/>
<activity
    android:label="@string/about"
    android:name="com.Gold_Finger.p037V.p038X.your_Facebook.pin_activity"
    android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"
    android:noHistory="false"/>
<activity
    android:theme="@style/Settings_Theme"
    android:label="@string/preference"
    android:name="com.Gold_Finger.p037V.p038X.your_Facebook.Ultimate_Settings"
    android:configChanges="smallestScreenSize|screenSize|uiMode|screenLayout|orientation|keyboardHidden|keyboard"
    android:noHistory="false"/>
<service
    android:name="com.Gold_Finger.p037V.p038X.your_Facebook.MiniService"
    android:enabled="true"
    android:process=":background"/>
<activity
```

Conclusion for MASVS RESILIENCE:

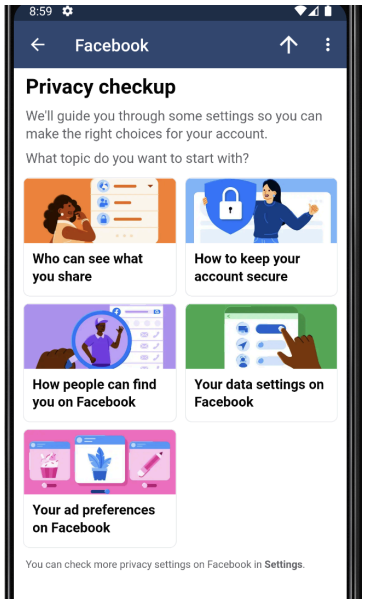
In conclusion, the app exhibits varying degrees of resilience across the MASVS-RESILIENCE standards. While MASVS-RESILIENCE-1 demonstrates successful platform validation, as evidenced by its functionality on the emulator, concerns arise regarding its compatibility with rooted devices. On the other hand, MASVS-RESILIENCE-2 highlights the implementation of a standard APK signature mechanism, ensuring the integrity of the APK. Moreover, the app showcases resilience against static analysis through obfuscation techniques, as outlined in MASVS-RESILIENCE-3. However, it lacks robust anti-dynamic analysis measures, as evidenced by the absence of debuggable flags. Overall, while the app demonstrates resilience in some areas, further enhancements are warranted to bolster its overall security posture.

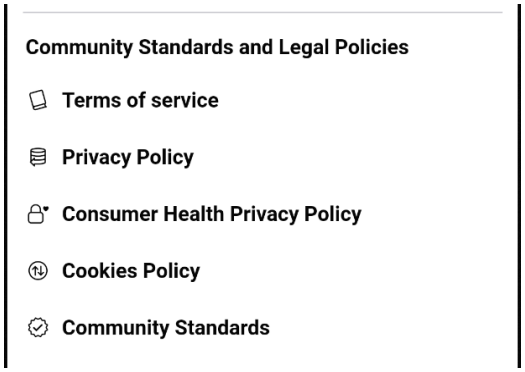
Testing App Privacy

This testing assesses the privacy compliance of Mini for Facebook, a mobile application that provides a lightweight version of the Facebook platform. The evaluation is based on the Future Privacy Foundation Best Practices for Mobile App Developers and aims to identify areas of strength and improvement regarding user privacy protection.

1. Communicate Openly and Effectively:

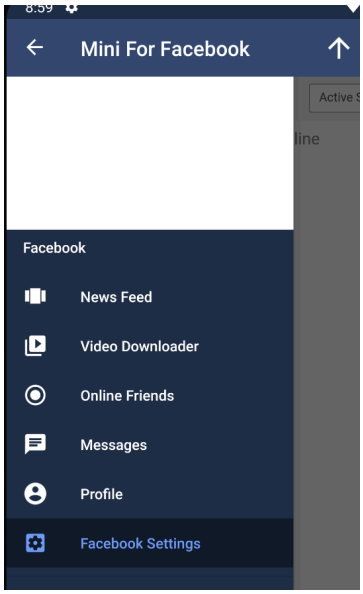
- **Privacy Policy Review:** The Mini for Facebook's privacy policy was evaluated for clarity and comprehensiveness. The policy effectively outlines data collection, sharing, and user practices using clear language understandable to the average user. It covers aspects such as what data is collected, how it's used, and users' rights. Since Mini for facebook is connected to the larger version of Facebook, it provides the same security and privacy guidelines as Facebook.





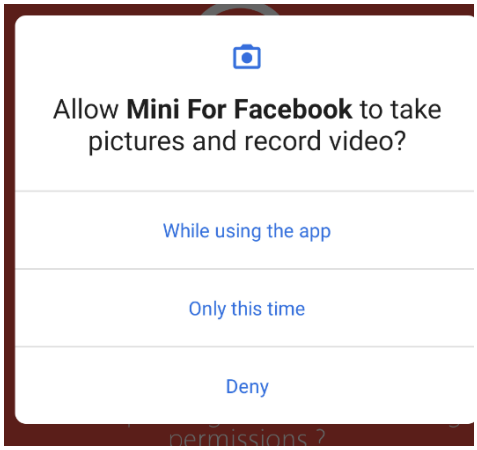
2. Make Your Privacy Policy Easily Accessible:

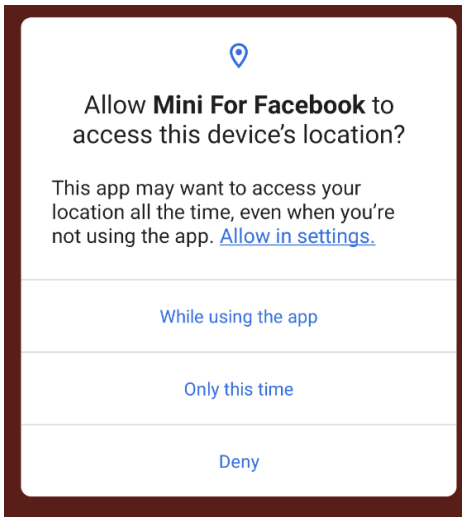
- **Prominence of Privacy Policy:** The app prominently features a link to the privacy policy within the settings menu. This ensures that users are informed about data practices before engaging with the app.
- **Accessibility:** Users can easily access the privacy policy from within the app, located in the settings menu. This accessibility ensures that users can reference the policy whenever they have privacy-related concerns.
- **Enhanced Notice:** Mini for Facebook does not currently implement enhanced notice features, such as contextual pop-ups or notifications when accessing sensitive data.



3. Use Enhanced Notice:

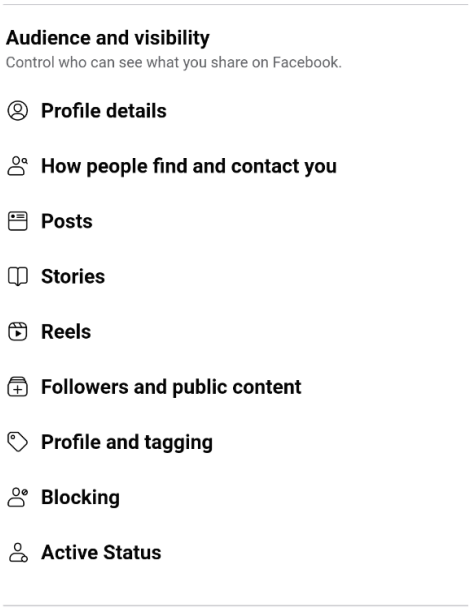
- **Contextual Awareness:** Mini for Facebook lacks enhanced notice features in situations where users might not expect certain data to be collected. For example, when accessing location data for check-ins or when enabling features that require access to the device's microphone or camera, the app does not provide contextual notifications or explanations regarding the data collection.

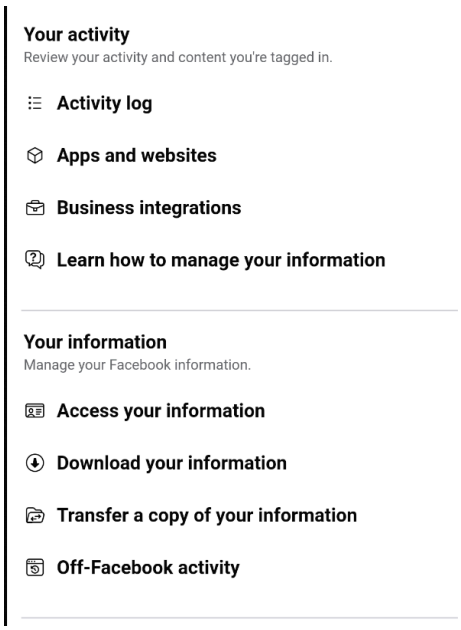




4. Provide Users with Choices and Controls:

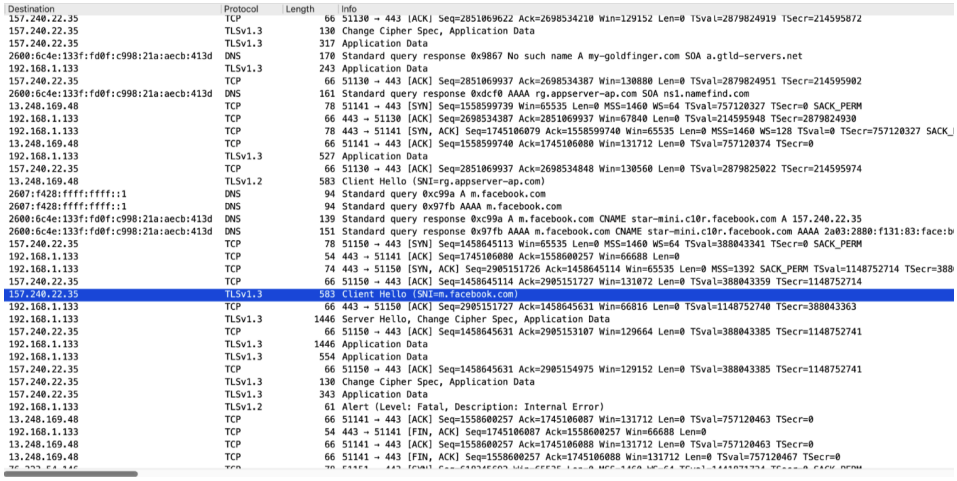
- **Choice and Control Features:** Mini for Facebook offers users various options to customize their privacy settings, including controlling who can see their posts, managing app permissions, and opting out of targeted advertising.
- **Customization:** Users can tailor their privacy settings according to their preferences, empowering them to manage their data effectively. This includes options to adjust visibility settings for posts and profile information.



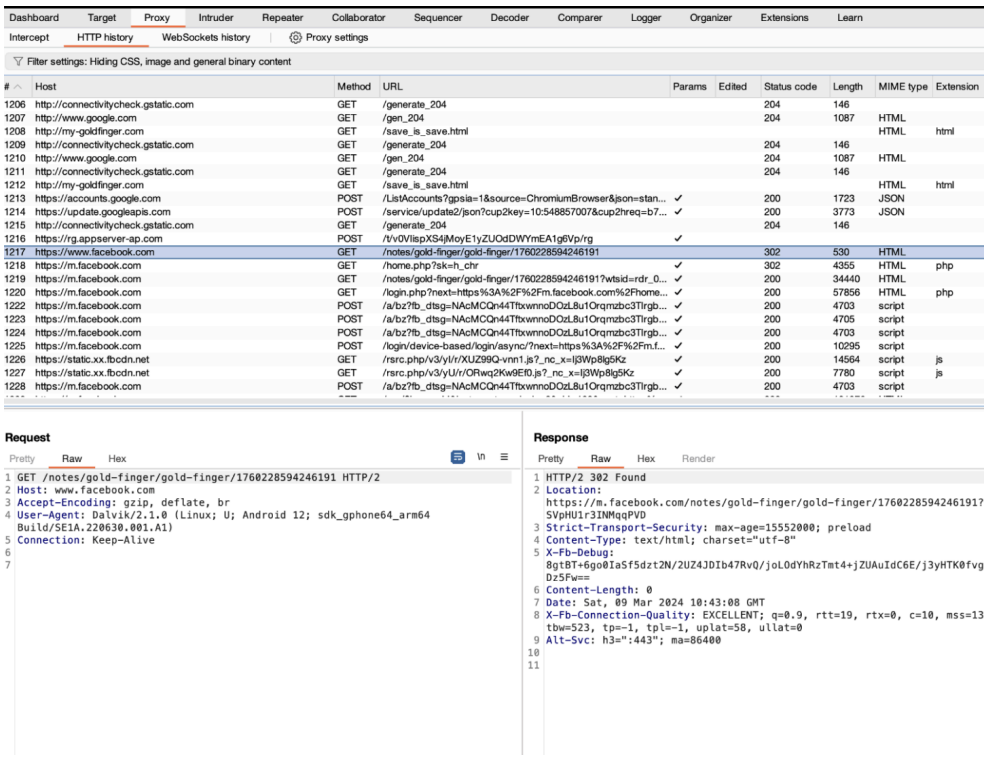


5. Secure Your Users' Data:

- **Security Measures:** Mini for Facebook employs robust encryption protocols to protect user data, including end-to-end encryption for messages and secure HTTPS connections for data transmission. Additionally, the app uses secure authentication mechanisms to prevent unauthorized access to user accounts.



```
    [Bytes in flight: 3343]
    [Bytes sent since last PSH flag: 268]
  TCP payload (268 bytes)
Transport Layer Security
  TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 263
    Encrypted Application Data [truncated]: 6cc52a4d75cfd104301b44aa7dcf8fdc6a3ecbd16dc783e4d445f93c
    [Application Data Protocol: Hypertext Transfer Protocol]
```



- **Data Handling:** While the app is secure in sending the data, there are some aspects of data storage that were not handled in a secure way. After examining the information in xml files under shared preferences, we found that CookieSave.xml and Preference.xml contains sensitive user data, including session cookies and sd contents, which can be exploited for session hijacking and data leakage. While not all data may be sensitive, some entries, like session cookies in CookieSave.xml, SID in APPFIREWORKS.xml, and device location details in oscontribution.xml, could pose security risks if exposed or misused.

```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cat APPFIREWORKS.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="A">v0VIispXS4jMoyE1yZUOdDWYmEA1g6Vp</string>
    <string name="installed">1</string>
    <long name="RT" value="1712279298855" />
    <boolean name="R" value="false" />
    <long name="PT" value="1712279281013" />
    <long name="OT" value="1712279198868" />
    <boolean name="W" value="false" />
    <long name="LT" value="1712279198868" />
    <boolean name="I" value="true" />
    <string name="SID">92221e0da1f91e21b7db15318f81acde9c934e1d</string>
```

```
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cat Preference.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="SD_CONTEXTS">VDA5YkdMemc4WEFHZEhKYlpKMC7x7fpxorMC64Z4hvXZv3p7ygKuexMcUFdvLPqeL3dYBPhtAEKVrCchiXapPJkaNpxl8Kp0q9623ev7ipeGIDgEjcxU9nL16n5O-G
yGDL1m5j4NKUXWugf5uQrtlsnt1Aw1XgT7gRdt9ynRHlB-IKAD9NhmqJJ_56tMXSMrWNSAoUixHXgVQGt-RbLtLoIUxn4NjGAsusaTf5tn4GmpvfNqcCkcilgMdLEtJkVH2rnVDSIP-M0waPXHuph0wVhJunK
_MPyamNsDaW7rJYVsQyuVe3LNJ82BIRM2qqxq9vg77aTAu76oivWHVZnwW1i1gWkBhTUd6k9ZTTUr4lfKBxJ5HQJQAbp8pmljpb_1ExNUXj7JSKzDsiogKENgcdp6eF3KGr66NjELXA4pLcwBBbFGiZTTRiJc
JBWOpM__1DcOj6zpUcG174DYjQKu6A1HCmsBYXLldrVudiOpSaoKAubt-ZQW62XwLZMUOZAhv9mDsTqS2lhPMclygBFFWz_nf3XN0nxnE0N9Rr7kOpYX1Ss4dr56GVIoP8LFTlqdymtaF_J_p2jjcO3QXP3-r
EX7e2CyN-zSbuzPxWyOdXGAZ1qd1SuXWEJTJf21MvRIfk6sej4Bpps15J33IRppHnE-K9zNSA_wt7PdaJ49TJ-_IcemXYsiQFBvZMmV4wUahkbpX4ByXBbgXcgLCOVGtU7W08JGMjgR-ty6cHsAZEHxrb6NYT
duOKtsk-DWLNLmsqJubB7mQwH5hcGOOSTqWlKmVyjz8CGR423h75mRBNyP4iMm4MPryHz4tS_HViuc1rcjzbZLekNE0CUO_wiBycORgaUBCEvof8VcPnBxMtAwr9kJRN1h5Y0chw2c09d8xLMKvDQ2EsZWrHX
Ihh5f7op39yRVXK14mNw-W30v2PBlp9r4EhTrp2pxAdfiHxFxTkgXK0RM648nVPOtVs3KzA==</string>
    <long name="SD_CONTEXTS_UPDATE_TIME" value="1712279153687" />
    <boolean name="SD_CONTEXTS_INPROGRESS" value="false" />
</map>
emulator_arm64:/data/data/com.Gold_Finger.V.X.your_Facebook/shared_prefs # cat WebViewChromiumPrefs.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <int name="lastVersionCodeUsed" value="447211484" />
</map>
```

Conclusion for Privacy Testing:

In conclusion, while Mini for Facebook exhibits commendable efforts in certain aspects of privacy compliance, such as transparent communication of privacy policies and providing users with control over their data, it falls short in other critical areas. The absence of enhanced notice features, particularly in contexts where unexpected data collection occurs, poses a significant concern. Additionally, issues regarding the security of stored data, as evidenced by sensitive information found in XML files, raise questions about the app's overall privacy performance. Therefore, while it may not be accurate to categorically label the app as failing the privacy test, there are substantial areas requiring improvement to ensure enhanced privacy protection for users.

Mini For Facebook Conclusion:

In evaluating Mini for Facebook's security and privacy posture, it's evident that while the app demonstrates strengths in certain areas, it also harbors vulnerabilities that lean it towards the less secure side. For instance, the presence of unprotected sensitive data in various storage locations, such as insecurely stored user preferences and cached data, highlights shortcomings in storage security practices. Additionally, the discovery of weak cryptographic algorithms like MD5 and SHA-1 being utilized for data encryption underscores critical flaws in cryptography practices, leaving user data susceptible to exploitation by malicious actors.

Moreover, deficiencies in authentication mechanisms, such as the absence of robust local authentication and session management controls, are particularly concerning. For example, the lack of password complexity requirements and session timeout functionality increases the risk of unauthorized access to user accounts. This was further accentuated during testing when it was observed that the app failed to implement session timeout functionality, leaving user sessions vulnerable to exploitation, potentially compromising user privacy and security.

Furthermore, issues regarding the security of stored data, such as sensitive information being found in XML files without proper encryption or access controls, raise significant red flags. For instance, during privacy testing, it was discovered that user profile information and preferences were stored in plain text XML files, leaving them susceptible to unauthorized access or extraction. These lapses in data security not only violate user privacy but also undermine user trust in the app's ability to protect their sensitive information effectively.

However, despite these vulnerabilities, Mini for Facebook has the opportunity to strengthen its security posture through proactive measures and comprehensive remediation efforts. For example, by implementing robust encryption algorithms like AES and enhancing authentication mechanisms with multifactor authentication and session management controls, the app can significantly mitigate security risks and enhance user data protection. Additionally, conducting regular security assessments and investing in employee training on security best practices can help cultivate a culture of security awareness within the organization, further bolstering its overall security posture and resilience against evolving threats.