Online Satta

VULNERABILITY ASSESSMENT AND PENETRATION TESTING
MOBILE APPLICATION TESTING REPORT

Business Confidential

Test Started on: August 11th, 2021
Reporting Date: August 11th, 2021
Project: Online Satta

Table of Contents

CONFIDENTIALITY STATEMENT

This document is the exclusive property of online sattaand Abhishek Joshi . This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both online satta and Abhishek Joshi.

Abhishek Joshi may share this document with auditors under non-disclosure agreements to demonstrate penetration testing requirement compliance.

DISCLAIMER

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Abhishek Joshi prioritized the assessment to identify the weakest security controls an attacker would exploit. Abhishek Joshi recommends conducting similar assessments on an annual basis.

CONTACT INFORMATION

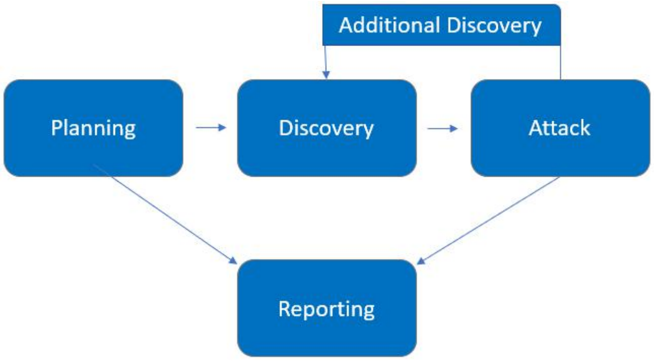
Name	Title	Contact Information
online satta		
Zehn Solutions	HR Zehn Solutions	Mobile: +91 7972444290 Email: zehnsolutions@gmail.com
Abhishek Joshi		
Abhishek Joshi	Penetration Tester	Office: +91 8788295760 Email: abhishekjoshi266@gmail.com

ASSESSMENT OVERVIEW

From August 11th, 2021 to August 12th, 2019, online sattaengaged Abhishek Joshi to evaluate the security posture of its Mobile Application to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing and customized testing frameworks*.

Phases of penetration testing activities include the following:

Planning – Customer goals are gathered and rules of engagement obtained.
Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



ASSESSMENT COMPONENTS

External Penetration Test

Abhishek Joshi, Pentester attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external Paths to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

FINDING SEVERITY RATINGS

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in Path-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

SCOPE

Assessment	Details
External Penetration Test	onlinesattabet.apk

Scope Exclusions

Per client request, Abhishek Joshi did not perform any Denial of Service attacks during testing.online sattais a vulnerable machine, I have to gather all the flags

EXECUTIVE SUMMARY

Abhishek Joshi evaluated online satta’s Mobile Application for Penetration testing from August 11th, 2021 to August 11th, 2021. By leveraging a series of attacks, Abhishek Joshi found critical level vulnerabilities. It is highly recommended that online sattanotices these vulnerabilities as soon as possible.

Manifest Analysis and Permission:

Step	Vulnerabilities
1	Clear Text Traffic is Enabled for Application
2	Service Not-Protected in Application
3	Broadcast Receiver is Found
4	Broadcast Receiver Protection-level
5	Activity is Not-Protected

Code Analysis:

Step	Vulnerabilities
1	Improper Nutralization cause SQL Injection
2	Weak Random Number Generator (RNG)
3	Files may contain hardcoded sensitive information like usernames, passwords, keys etc
4	Weak Cryptography use md5
5	Oracle attack
9	Internal IP Disclouse
10	Javascript enabled in Webview xxs injection possible
11	Webview enables DOM Storage

Quark Analysis:

Step	Vulnerabilities
1	Connect to a URL and read data from it
2	Get last known location of the device
3	Read sensitive data(SMS, CALLLOG, etc)

VULNERABILITIES WITH IMPACT

The following chart illustrates the vulnerabilities found by impact:

PENETRATION TEST FINDINGS ON MANIFEST & PERMISSIONS

Clear text Traffic is enabled for Application(High)

Description:	The application intends to use clear text network traffic, such as clear text HTTP, FTP stacks, DownloadManager and MediaPlayer. The default value for applications that target API level 27 or lower is “True”. The default value for applications that target API level 28 or Higher default to “False”. The key reason for avoiding clear text traffic is a lack of confidentiality, authenticity, and protection against tempering
Impact:	A network attacker can do sniffing and eavesdrop on transmitted data and also modify it without being detected.
Path:	android:usesCleartextTraffic=True
References:	https://support.vuplex.com/articles/how-to-enable-cleartext-traffic-on-android

Exploitation Proof of Concept

abhishek jsohi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation :

Who:	Satta Bet
Vector:	Sniffing
Action:	~Traffic should be encrypted. ~Apply SSL certifications. ~SSL-TLS should be upto-date.

Service Not-Protected in Application(High)

Description:	Service is found to be shared with other applications on the device, therefore leaving it accessible to any other application on the device. The presence of intent-filter indicates that the service is explicitly exported.
Impact:	Ways to exploit this issue may vary, depending on the intent of the attacker If the user is logged in malicious application can display pop-ups in the shopping app and use it to launch attacks. The attacker may craft the malicious application to display pop-ups that lead to malicious links or other malicious apps.
Path:	(com.idreams.project.onlinesatta.FireBaseMessagingService) is not Protected. [android:exported=true (com.idreams.project.onlinesatta.FirebaseInstantId) is not Protected. An intent-filter exists. (com.google.firebase.messaging.FirebaseMessagingService) is not Protected. [android:exported=true] (com.google.firebase.iid.FirebaseInstanceIdService) is not Protected. [android:exported=true]
References:	https://github.com/aws-amplify/amplify-js/issues/5283

Exploitation Proof of Concept

abhishek jsohi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation

Who:	Satta Bet
Vector:	Service
Action:	-Service should be protected.

	-Do not implement intent-filter.

Broadcast Receiver is Found(High)

Description:	A broadcast receiver is found to be shared with other applications on the device, therefore, leaving it accessible to any other applications on the device.
Impact:	The presence of the intent filter indicates that the broadcast receiver is explicitly exported.
Path:	(com.razorpay.RzpTokenReceiver) is not protected. An intent filter exists.
References:	https://oldbam.github.io/android/security/android-vulnerabilities-insecurebank-broadcast-receivers https://developer.android.com/guide/components/broadcasts

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation

Who:	online satta
Vector:	Broadcast Receiver
Action:	-Broadcast Receiver should be protected. -Do not implement intent-filter.

Broadcast Receiver Protection level(High)

Description:	A broadcast receiver is found to be shared with other applications on the device, therefore, leaving it accessible to any other applications on the device. It is protected by permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined.
Impact:	If it is set to normal or dangerous, a malicious application can request ansd obtain the permission and interact with the component. If it is set to signature-only applications signed with the same certificate can obtain the permission.
Path:	(com.google.firebase.iid.FirebaseInstanceIdReceiver) is protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [android:exported=true]
References:	https://github.com/phonegap/phonegap-plugin-push/issues/2208 https://stackoverflow.com/questions/9528608/restricting-android-broadcast-receiver-from-specific-app https://www.futurelearn.com/info/courses/secure-android-app-development/0/steps/21594

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation

Who:	online satta
Vector:	Broadcast Receiver
Action:	-Broadcast Receiver should be protected.

Activity is Not-Protected(High)

Description:	An activity is found to be shared with other applications on the device, therefore, leaving it accessible to any other applications on the device.
Impact:	The presence of the intent filter indicates that the activity is explicitly exported.
Path:	(com.razorpay.CheckoutActivity) is not protected and intent filter exists.
References:	https://commonsware.com/blog/2014/04/30/if-your-activity-has-intent-filter-export-it.html https://cwe.mitre.org/data/definitions/926.html

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation

Who:	online satta
Vector:	Activity
Action:	-Activity should be protected. -Do not implement intent-filter.

PENETRATION TEST FINDINGS ON CODE

Improper Neutralization Cause SQL Injection (Critical)

Description:	The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. Without sufficient removal or quoting of SQL syntax in user-controllable inputs, the generated SQL query can cause those inputs to be interpreted as SQL instead of ordinary user data. This can be used to alter query logic to bypass security checks, or to insert additional statements that modify the back-end database, possibly including execution of system commands. SQL injection has become a common issue with database-driven web sites. The flaw is easily detected, and easily exploited, and as such, any site or software package with even a minimal user base is likely to be subject to an attempted attack of this kind. This flaw depends on the fact that SQL makes no real distinction between the control and data planes.
Impact:	Attacker can perform sql injection
Files:	com/idreams/project/onlinesatta/cont/DBHelper.java
References:	https://cwe.mitre.org/data/definitions/89.html

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation:

Who:	online satta
Vector:	SQL Injection
Action:	Abhishek Joshi recommends that online satta: Database should be secure and data should be encrypted so attacker can not read easliy and use strong querries

Weak Random Number Generator (RNG) (High)

Description:	It is fundamentally impossible to produce truly random numbers on any deterministic device. Pseudo-random number generators (RNG) compensate for this by producing a stream of pseudo-random numbers - a stream of numbers that appear as if they were randomly generated. The quality of the generated numbers varies with the type of algorithm used. Cryptographically secure RNGs generate random numbers that pass statistical randomness tests, and are resilient against prediction attacks (e.g. it is statistically infeasible to predict the next number produced). Mobile SDKs offer standard implementations of RNG algorithms that produce numbers with sufficient artificial randomness. We'll introduce the available APIs in the Android and iOS specific sections.
Impact:	it may be possible for an attacker to guess the next value that will be generated, and use this guess to impersonate another user or access sensitive information.
Files:	com/idreams/project/onlinesatta/Adapter/AdapterStarLineBazar.java com/idreams/project/onlinesatta/Adapter/AdapterStarLineBazarResults.java com/idreams/project/onlinesatta/paymero/PaymeroUserDetailsActivity.java
References:	https://github.com/MobSF/owasp-mstg/blob/master/Document/0x04g-Testing-Cryptography.md#weak-random-number-generators https://cwe.mitre.org/data/definitions/330.html

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation:

Who:	online satta
Vector:	RNG
Action:	Abhishek Joshi recommends that online satta: Phase: Architecture and Design Use a well-vetted algorithm that is currently considered to be strong by experts in the field, and select well-tested implementations with adequate length seeds. In general, if a pseudo-random number generator is not advertised as being cryptographically secure, then it is probably a statistical PRNG and should not be used in security-sensitive contexts. Pseudo-random number generators can produce predictable numbers if the generator is known and the seed can be guessed. A 256-bit seed is a good starting point for producing a "random enough" number Phase: Implementation Consider a PRNG that re-seeds itself as needed from high quality pseudo-random output sources, such as hardware devices Phase: Testing Use automated static analysis tools that target this type of weakness. Many modern techniques use data flow analysis to minimize the number of false positives. This is not a perfect solution, since 100% accuracy and coverage are not feasible

Files may contain hardcoded sensitive information like usernames, passwords, keys etc.(Medium)

Description:	Files may contain hardcoded sensitive information like usernames, passwords, keys etc. The application stores sensitive information in cleartext within a resource that might be accessible to another control sphere. Because the information is stored in cleartext, attackers could potentially read it. Even if the information is encoded in a way that is not human-readable, certain techniques could determine which encoding is being used, then decode the information.
Impact:	This vulnerability impacts directly to the user's privacy.
Files:	com/razorpay/AnalyticsConstants.java com/idreams/project/onlinesatta/pojo/Data.java com/idreams/project/onlinesatta/pojo/Detail.java com/razorpay/BaseConstants.java com/idreams/project/onlinesatta/cont/Constants.java
References:	https://cwe.mitre.org/data/definitions/312.html https://github.com/MobSF/owasp-mstg/blob/master/Document/0x05d-Testing-Data-Storage.md#checking-memory-for-sensitive-data-mstg-storage-10

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation:

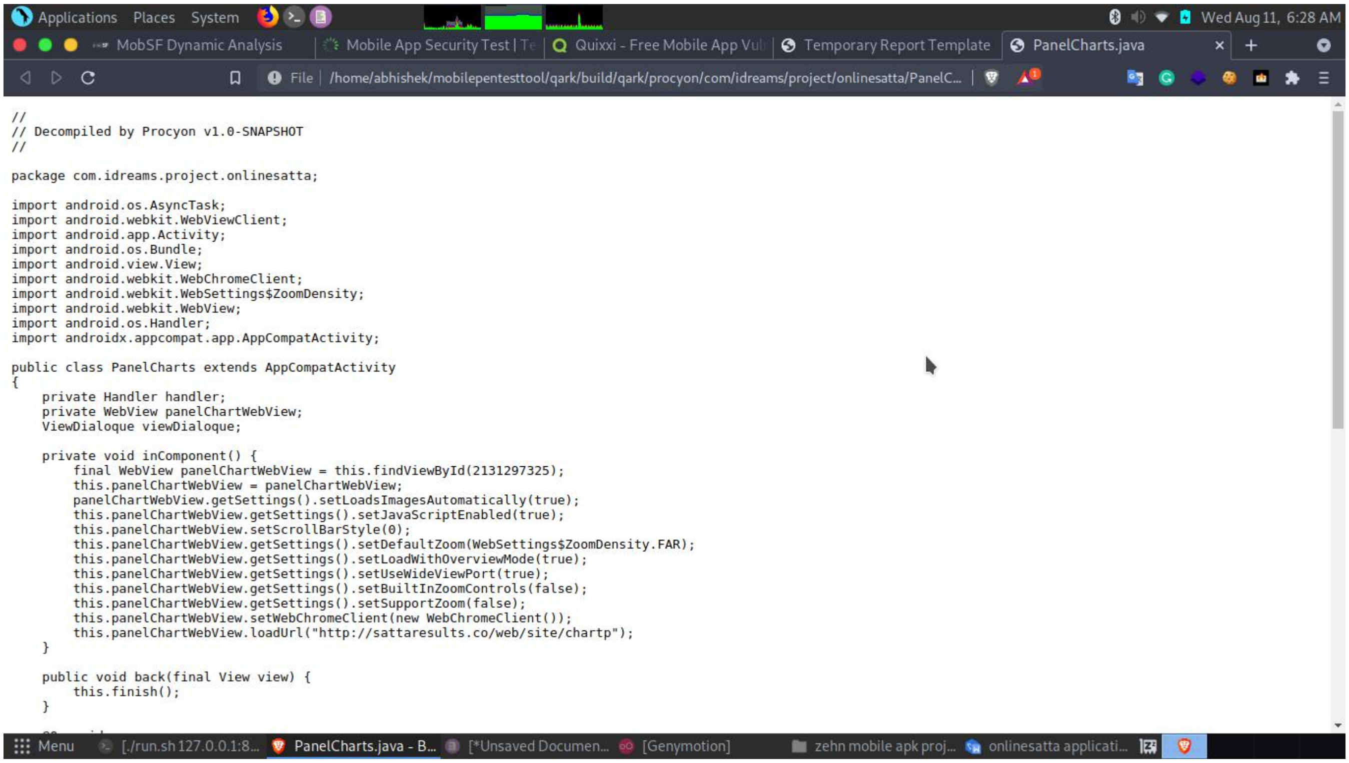
Who:	online satta
Vector:	Privacy impact
Action:	Abhishek Joshi recommends that online satta: hide sensitive data on those file attacker can steal the data and which directly impact to the user's privacy because it tends to privacy check the file and code thoroughly if there is any sensitive data contains or not

Javascript enabled in Webview xxs possible (Medium)

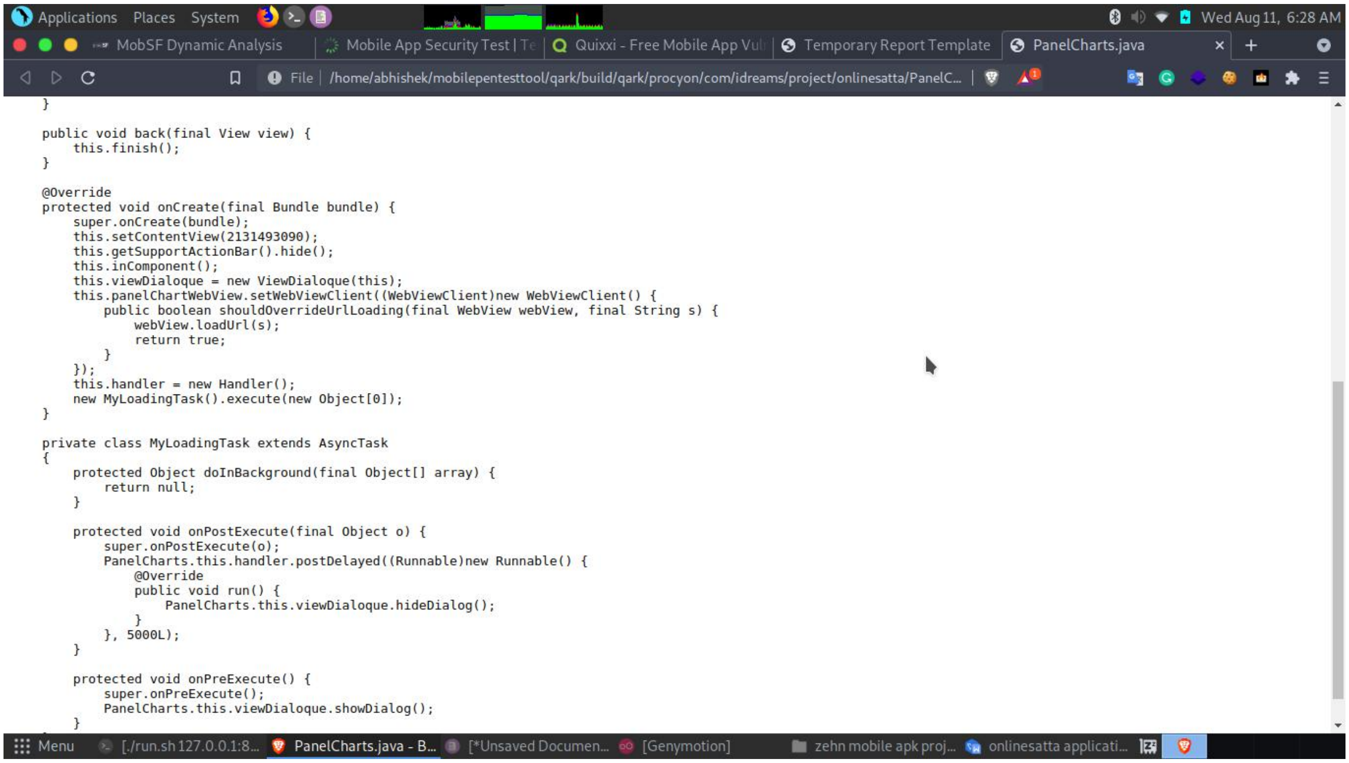
Description:	Cross-site scripting is a type of security vulnerability typically found in web applications. XSS attacks enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls such as the same-origin policy.
Impact:	Attacker can inject the malicious script and perform injection base attack .
Files:	com.idreams.project.onlinesatta
References:	http://developer.android.com/guide/practices/security.html

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from Manual testing using testing tools with proper path and parameters.


Applications Places System
Wed Aug 11, 6:28 AM
MobSF Dynamic Analysis
Mobile App Security Test | Te
Quixxi - Free Mobile App Vul
Temporary Report Template
PanelCharts.java
File | /home/abhishek/mobilepentesttool/qark/build/qark/procyon/com/idreams/project/onlinesatta/PanelC...
Menu
[./run.sh 127.0.0.1:8...
PanelCharts.java - B...
[*Unsaved Documen...
[Genymotion]
zehn mobile apk proj...
onlinesatta applicati...

```
//
// Decompiled by Procyon v1.0-SNAPSHOT
//

package com.idreams.project.onlinesatta;

import android.os.AsyncTask;
import android.webkit.WebViewClient;
import android.app.Activity;
import android.os.Bundle;
import android.view.View;
import android.webkit.WebChromeClient;
import android.webkit.WebSettings$ZoomDensity;
import android.webkit.WebView;
import android.os.Handler;
import androidx.appcompat.app.AppCompatActivity;

public class PanelCharts extends AppCompatActivity
{
    private Handler handler;
    private WebView panelChartWebView;
    ViewDialoque viewDialoque;

    private void inComponent() {
        final WebView panelChartWebView = this.findViewById(2131297325);
        this.panelChartWebView = panelChartWebView;
        panelChartWebView.getSettings().setLoadsImagesAutomatically(true);
        this.panelChartWebView.getSettings().setJavaScriptEnabled(true);
        this.panelChartWebView.setScrollBarStyle(0);
        this.panelChartWebView.getSettings().setDefaultZoom(WebSettings$ZoomDensity.FAR);
        this.panelChartWebView.getSettings().setLoadWithOverviewMode(true);
        this.panelChartWebView.getSettings().setUseWideViewPort(true);
        this.panelChartWebView.getSettings().setBuiltInZoomControls(false);
        this.panelChartWebView.getSettings().setSupportZoom(false);
        this.panelChartWebView.setWebChromeClient(new WebChromeClient());
        this.panelChartWebView.loadUrl("http://sattaresults.co/web/site/chartp");
    }

    public void back(final View view) {
        this.finish();
    }
```


Applications Places System
Wed Aug 11, 6:28 AM
MobSF Dynamic Analysis
Mobile App Security Test | Te
Quixxi - Free Mobile App Vul
Temporary Report Template
PanelCharts.java
File | /home/abhishek/mobilepentesttool/qark/build/qark/procyon/com/idreams/project/onlinesatta/PanelC...
Menu
[./run.sh 127.0.0.1:8...
PanelCharts.java - B...
[*Unsaved Documen...
[Genymotion]
zehn mobile apk proj...
onlinesatta applicati...

```
    }

    public void back(final View view) {
        this.finish();
    }

    @Override
    protected void onCreate(final Bundle bundle) {
        super.onCreate(bundle);
        this.setContentView(2131493090);
        this.getSupportActionBar().hide();
        this.inComponent();
        this.viewDialoque = new ViewDialoque(this);
        this.panelChartWebView.setWebViewClient((WebViewClient)new WebViewClient() {
            public boolean shouldOverrideUrlLoading(final WebView webView, final String s) {
                webView.loadUrl(s);
                return true;
            }
        });
        this.handler = new Handler();
        new MyLoadingTask().execute(new Object[0]);
    }

    private class MyLoadingTask extends AsyncTask
    {
        protected Object doInBackground(final Object[] array) {
            return null;
        }

        protected void onPostExecute(final Object o) {
            super.onPostExecute(o);
            PanelCharts.this.handler.postDelayed((Runnable)new Runnable() {
                @Override
                public void run() {
                    PanelCharts.this.viewDialoque.hideDialog();
                }
            }, 5000L);
        }

        protected void onPreExecute() {
            super.onPreExecute();
            PanelCharts.this.viewDialoque.showDialog();
        }
```

Remediation:

Who:	online satta
Vector:	XXS
Action:	Abhishek Joshi recommends that online satta: -dont allow to put any javascript -apply filter and sanitization

Weak Cryptography use md5(Medium)

Description:	The use of a broken or risky cryptographic algorithm is an unnecessary risk that may result in the exposure of sensitive

	information. The use of a non-standard algorithm is dangerous because a determined attacker may be able to break the algorithm and compromise whatever data has been protected. Well-known techniques may exist to break the algorithm.
Impact:	Attacker can Steal Sensitive Information risk that may result in the exposure of sensitive information.
Files:	com/razorpay/BaseUtils.java
References:	https://cwe.mitre.org/data/definitions/327.html https://github.com/MobSF/owasp-mstg/blob/master/Document/0x04g-Testing-Cryptography.md#identifying-insecure-andor-deprecated-cryptographic-algorithms-mstg-crypto-4

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation:

Who:	online satta
Vector:	Weak Cryptography Algorithm
Action:	Abhishek Joshi recommends that online satta: Sensitive Information should be encrypted. use strong cryptographic algorithm

Oracle attack (High)

Description:	The software uses obfuscation or encryption of inputs that should not be mutable by an external actor, but the software does not use integrity checks to detect if those inputs have been modified.

	When an application relies on obfuscation or incorrectly applied / weak encryption to protect client-controllable tokens or parameters, that may have an effect on the user state, system state, or some decision made on the server. Without protecting the tokens/parameters for integrity, the application is vulnerable to an attack where an adversary traverses the space of possible values of the said token/parameter in order to attempt to gain an advantage. The goal of the attacker is to find another admissible value that will somehow elevate their privileges in the system, disclose information or change the behavior of the system in some way beneficial to the attacker. If the application does not protect these critical tokens/parameters for integrity, it will not be able to determine that these values have been tampered with. Measures that are used to protect data for confidentiality should not be relied upon to provide the integrity service.
Impact:	Insufficient Cryptography. The Application uses encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attack.
Files:	com/razorpay/B_q.java
References:	https://cwe.mitre.org/data/definitions/649.html

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation:

Who:	online satta
Vector:	Cryptogarphy
Action:	Abhishek Joshi recommends that online satta: Use strong encryption method.

Private IP Disclouse (High)

Description:	RFC 1918 specifies ranges of IP addresses that are reserved for use in private networks and cannot be routed on the public Internet. Although various methods exist by which an attacker can determine the public IP addresses in use by an organization, the private addresses used internally cannot usually be determined in the same ways.
Impact:	Discovering the private addresses used within an organization can help an attacker in carrying out network-layer attacks aiming to penetrate the organization's internal infrastructure.
Files:	http://192.168.19.137/billpay/checkout/post/submit
References:	https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from automation testing using testing tools with proper path and parameters.

Remediation:

Who:	online satta
Vector:	Private IP Disclouse
Action:	There is not usually any good reason to disclose the internal IP addresses used within an organization's infrastructure. If these are being returned in

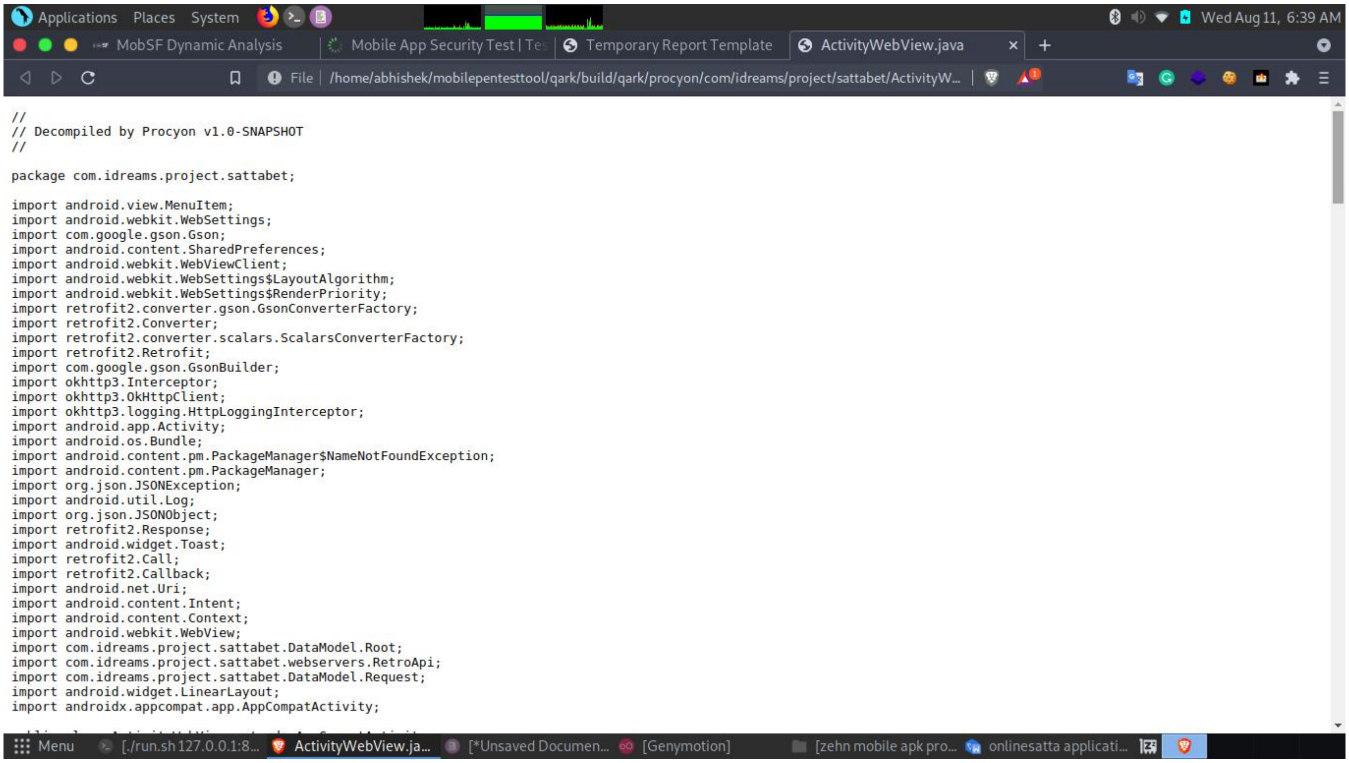
	service banners or debug messages, then the relevant services should be configured to mask the private addresses. If they are being used to track back-end servers for load balancing purposes, then the addresses should be rewritten with innocuous identifiers from which an attacker cannot infer any useful information about the infrastructure.

Webview enables DOM Storage (High)

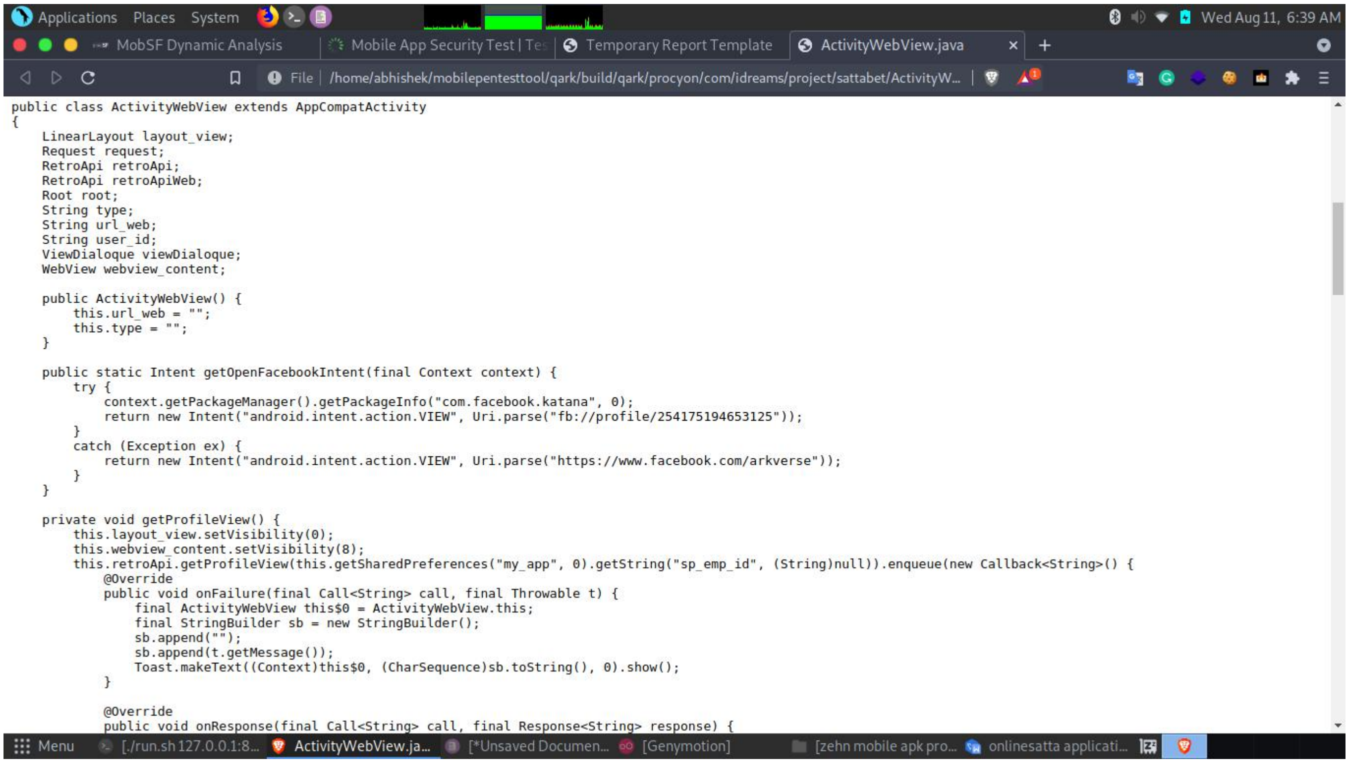
Description:	DOM Storage enabled for this WebView, there is a potential for caching sensitive information.
Impact:	Attacker can steal sensitive data .
Files:	com.idreams.project.sattabet
References:	https://stackoverflow.com/questions/5858760/what-does-enable-dom-storage-api-mean

Exploitation Proof of Concept

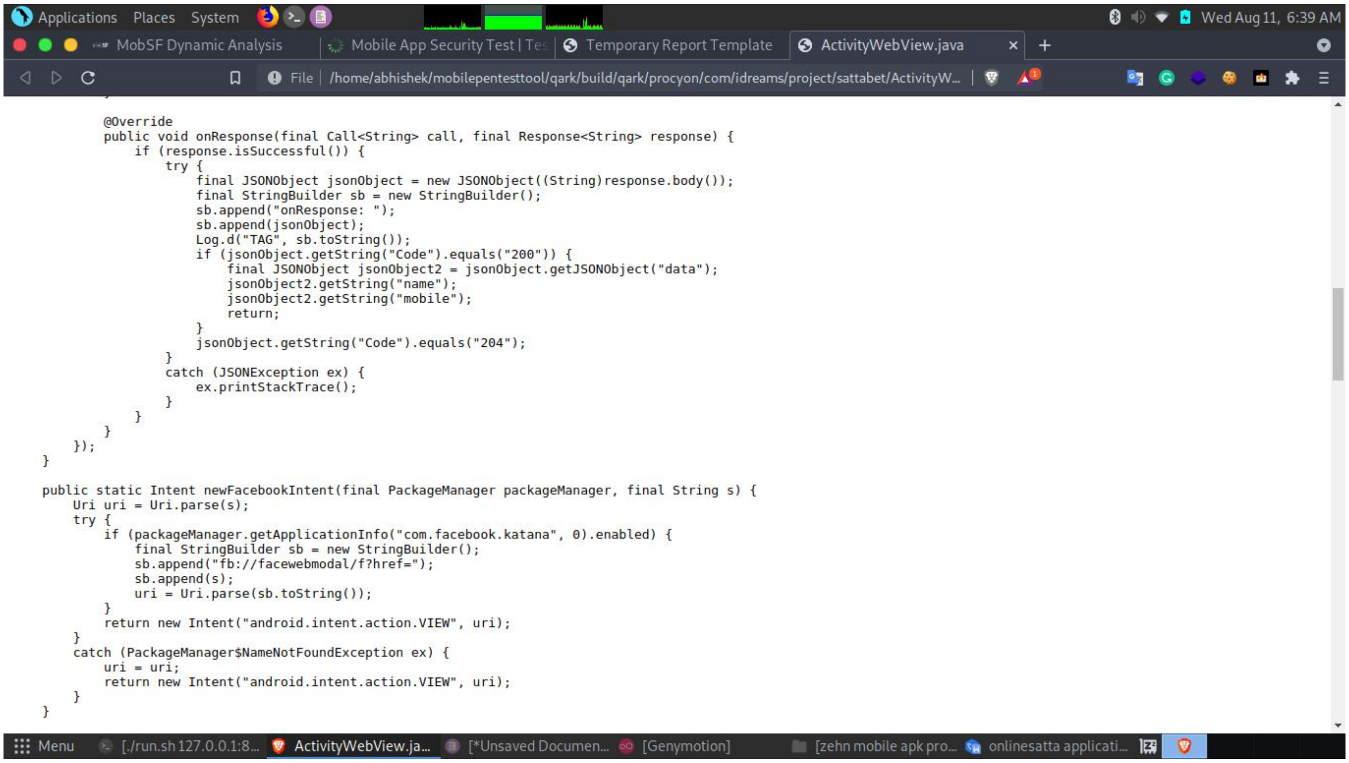
Abhishek Joshi gathered this vulnerability from Manual testing using testing tools with proper path and parameters.



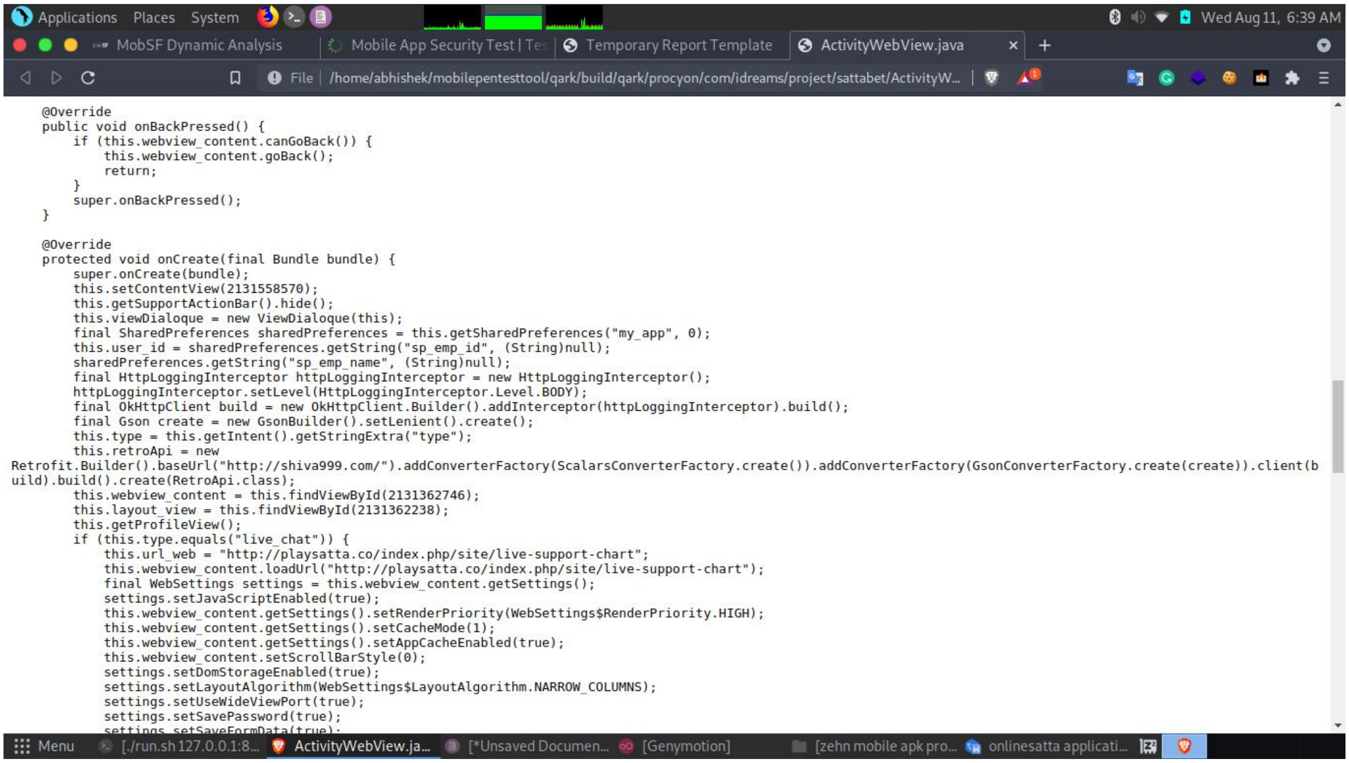
```
//
// Decompiled by Procyon v1.0-SNAPSHOT
//

package com.idreams.project.sattabet;

import android.view.MenuItem;
import android.webkit.WebSettings;
import com.google.gson.Gson;
import android.content.SharedPreferences;
import android.webkit.WebViewClient;
import android.webkit.WebSettings$LayoutAlgorithm;
import android.webkit.WebSettings$RenderPriority;
import retrofit2.converter.gson.GsonConverterFactory;
import retrofit2.Converter;
import retrofit2.converter.scalars.ScalarsConverterFactory;
import retrofit2.Retrofit;
import com.google.gson.GsonBuilder;
import okhttp3.Interceptor;
import okhttp3.OkHttpClient;
import okhttp3.logging.HttpLoggingInterceptor;
import android.app.Activity;
import android.os.Bundle;
import android.content.pm.PackageManager$NameNotFoundException;
import android.content.pm.PackageManager;
import org.json.JSONException;
import android.util.Log;
import org.json.JSONObject;
import retrofit2.Response;
import android.widget.Toast;
import retrofit2.Call;
import retrofit2.Callback;
import android.net.Uri;
import android.content.Intent;
import android.content.Context;
import android.webkit.WebView;
import com.idreams.project.sattabet.DataModel.Root;
import com.idreams.project.sattabet.webservers.RetroApi;
import com.idreams.project.sattabet.DataModel.Request;
import android.widget.LinearLayout;
import androidx.appcompat.app.AppCompatActivity;
```



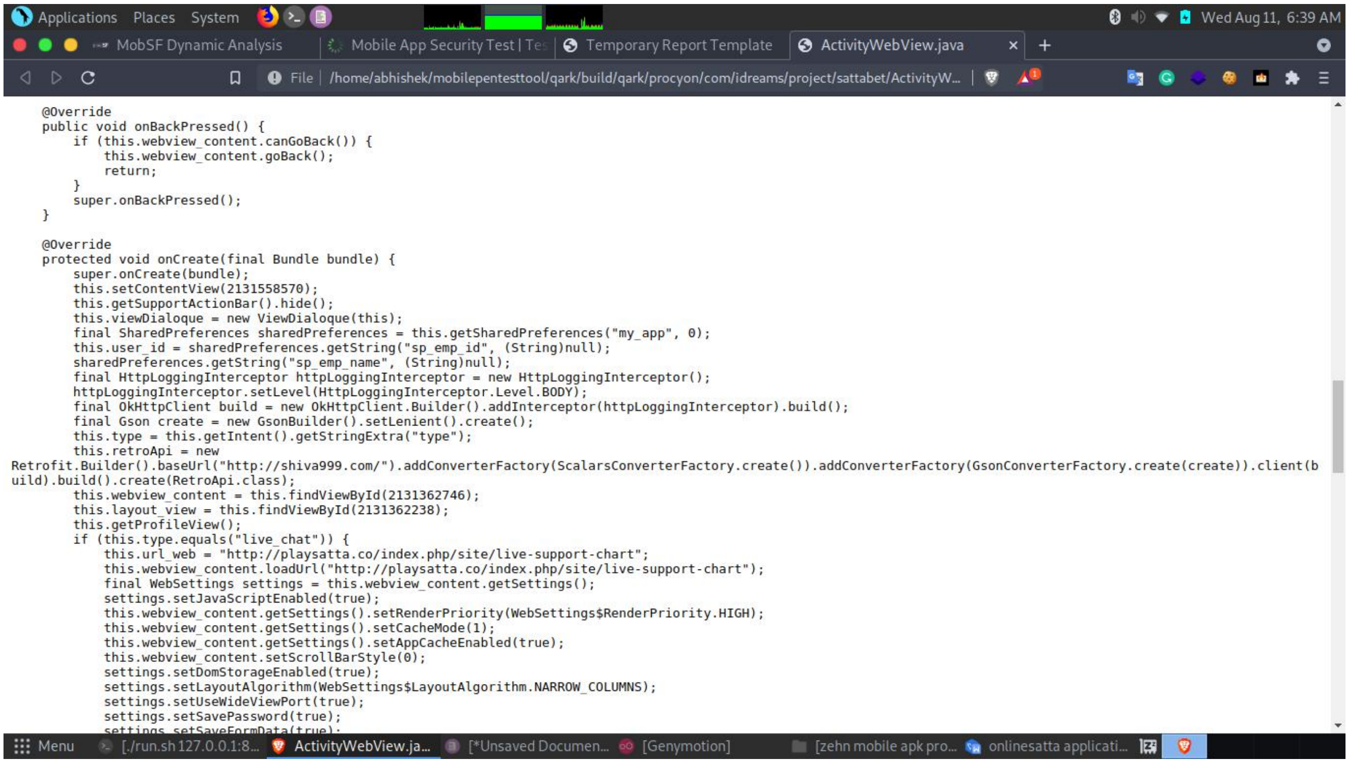
```
public class ActivityWebView extends AppCompatActivity
{
    LinearLayout layout_view;
    Request request;
    RetroApi retroApi;
    RetroApi retroApiWeb;
    Root root;
    String type;
    String url_web;
    String user_id;
    ViewDialoque viewDialoque;
    WebView webview_content;

    public ActivityWebView() {
        this.url_web = "";
        this.type = "";
    }

    public static Intent getOpenFacebookIntent(final Context context) {
        try {
            context.getPackageManager().getPackageInfo("com.facebook.katana", 0);
            return new Intent("android.intent.action.VIEW", Uri.parse("fb://profile/254175194653125"));
        }
        catch (Exception ex) {
            return new Intent("android.intent.action.VIEW", Uri.parse("https://www.facebook.com/arkverse"));
        }
    }

    private void getProfileView() {
        this.layout_view.setVisibility(0);
        this.webview_content.setVisibility(8);
        this.retroApi.getProfileView(this.getSharedPreferences("my_app", 0).getString("sp_emp_id", (String)null)).enqueue(new Callback<String>() {
            @Override
            public void onFailure(final Call<String> call, final Throwable t) {
                final ActivityWebView this$0 = ActivityWebView.this;
                final StringBuilder sb = new StringBuilder();
                sb.append("");
                sb.append(t.getMessage());
                Toast.makeText((Context)this$0, (CharSequence)sb.toString(), 0).show();
            }

            @Override
            public void onResponse(final Call<String> call, final Response<String> response) {
```



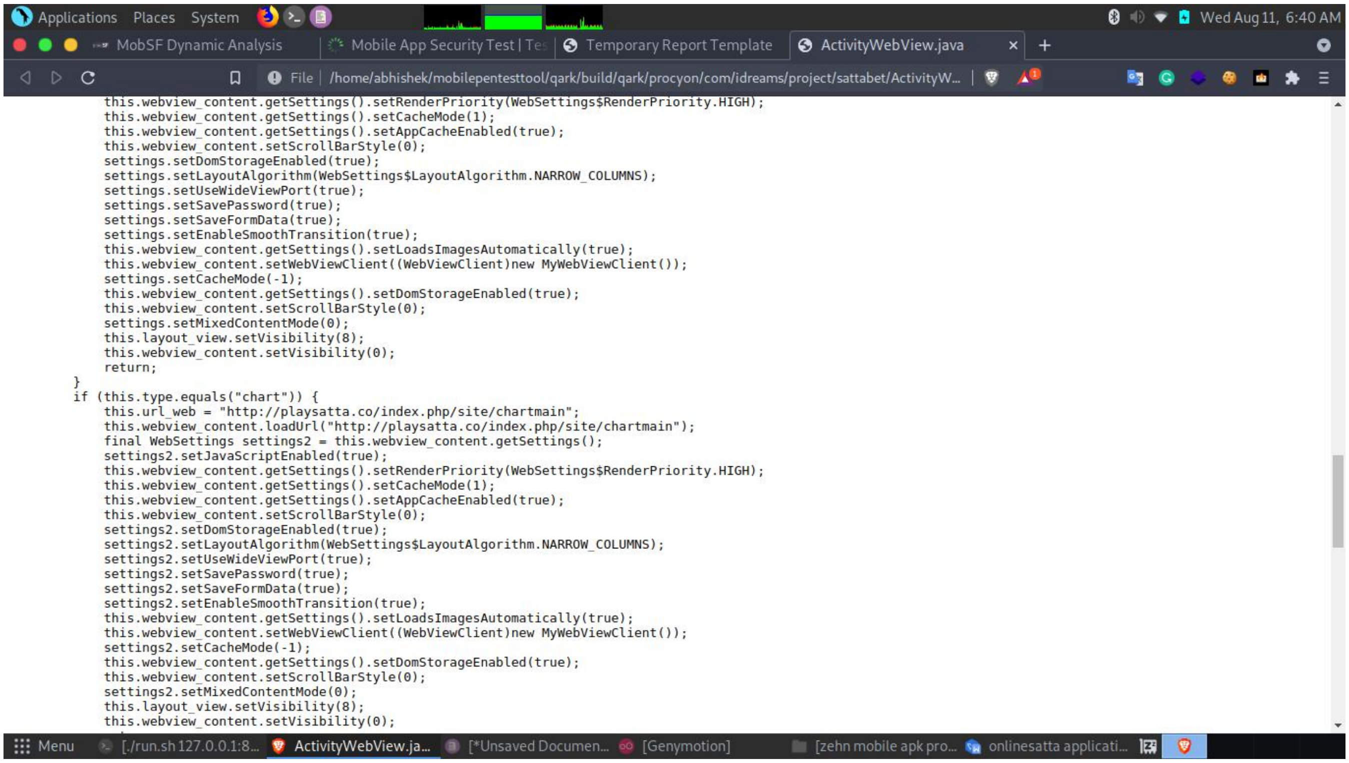
```
        @Override
        public void onResponse(final Call<String> call, final Response<String> response) {
            if (response.isSuccessful()) {
                try {
                    final JSONObject jsonObject = new JSONObject((String)response.body());
                    final StringBuilder sb = new StringBuilder();
                    sb.append("onResponse: ");
                    sb.append(jsonObject);
                    Log.d("TAG", sb.toString());
                    if (jsonObject.getString("Code").equals("200")) {
                        final JSONObject jsonObject2 = jsonObject.getJSONObject("data");
                        jsonObject2.getString("name");
                        jsonObject2.getString("mobile");
                        return;
                    }
                    jsonObject.getString("Code").equals("204");
                }
                catch (JSONException ex) {
                    ex.printStackTrace();
                }
            }
        }
    });
}

public static Intent newFacebookIntent(final PackageManager packageManager, final String s) {
    Uri uri = Uri.parse(s);
    try {
        if (packageManager.getApplicationInfo("com.facebook.katana", 0).enabled) {
            final StringBuilder sb = new StringBuilder();
            sb.append("fb://facewebmodal/f?href=");
            sb.append(s);
            uri = Uri.parse(sb.toString());
        }
        return new Intent("android.intent.action.VIEW", uri);
    }
    catch (PackageManager$NameNotFoundException ex) {
        uri = uri;
        return new Intent("android.intent.action.VIEW", uri);
    }
}
```



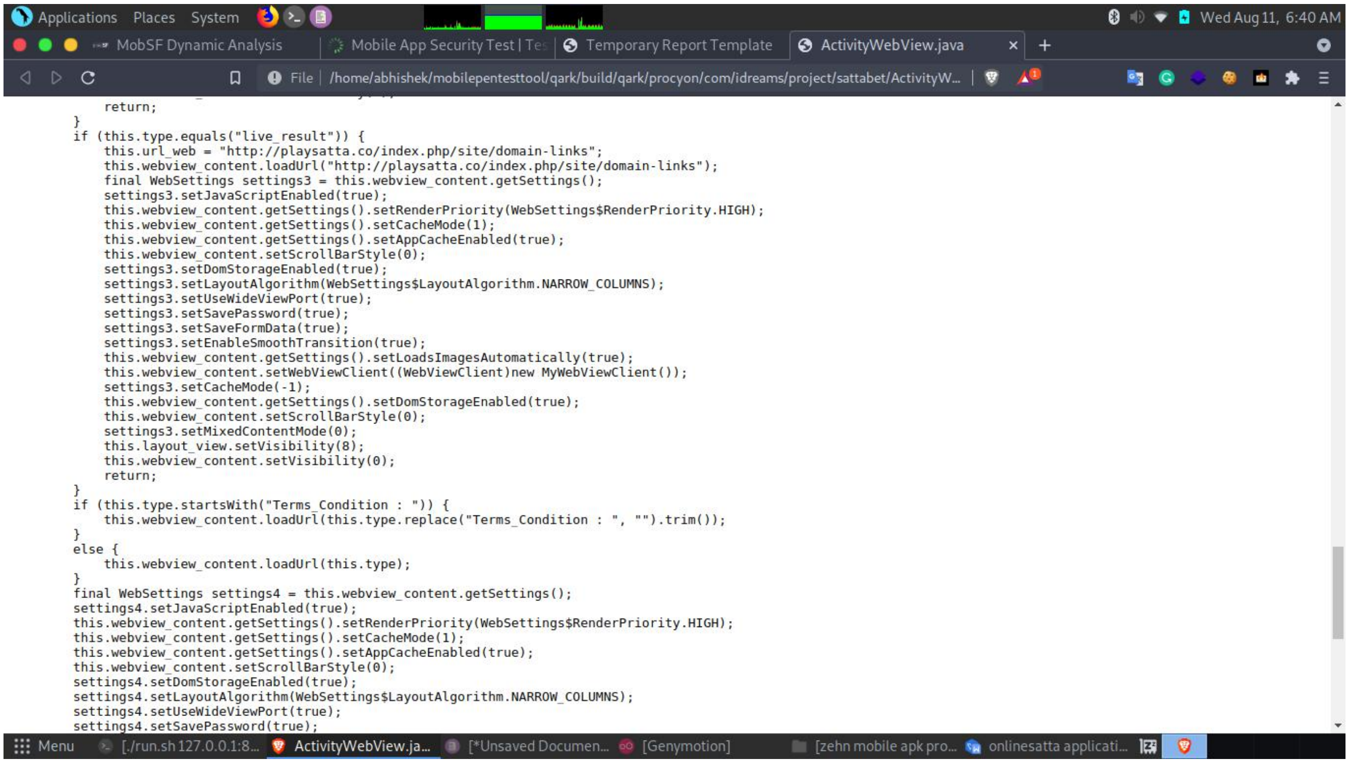
```
    @Override
    public void onBackPressed() {
        if (this.webview_content.canGoBack()) {
            this.webview_content.goBack();
            return;
        }
        super.onBackPressed();
    }

    @Override
    protected void onCreate(final Bundle bundle) {
        super.onCreate(bundle);
        this.setContentView(2131558570);
        this.getSupportActionBar().hide();
        this.viewDialoque = new ViewDialoque(this);
        final SharedPreferences sharedPreferences = this.getSharedPreferences("my_app", 0);
        this.user_id = sharedPreferences.getString("sp_emp_id", (String)null);
        sharedPreferences.getString("sp_emp_name", (String)null);
        final HttpLoggingInterceptor httpLoggingInterceptor = new HttpLoggingInterceptor();
        httpLoggingInterceptor.setLevel(HttpLoggingInterceptor.Level.BODY);
        final OkHttpClient build = new OkHttpClient.Builder().addInterceptor(httpLoggingInterceptor).build();
        final Gson create = new GsonBuilder().setLenient().create();
        this.type = this.getIntent().getStringExtra("type");
        this.retroApi = new
Retrofit.Builder().baseUrl("http://shiva999.com/").addConverterFactory(ScalarsConverterFactory.create()).addConverterFactory(GsonConverterFactory.create(create)).client(b
uild).build().create(RetroApi.class);
        this.webview_content = this.findViewById(2131362746);
        this.layout_view = this.findViewById(2131362238);
        this.getProfileView();
        if (this.type.equals("live_chat")) {
            this.url_web = "http://playsatta.co/index.php/site/live-support-chart";
            this.webview_content.loadUrl("http://playsatta.co/index.php/site/live-support-chart");
            final WebSettings settings = this.webview_content.getSettings();
            settings.setJavaScriptEnabled(true);
            this.webview_content.getSettings().setRenderPriority(WebSettings$RenderPriority.HIGH);
            this.webview_content.getSettings().setCacheMode(1);
            this.webview_content.getSettings().setAppCacheEnabled(true);
            this.webview_content.setScrollBarStyle(0);
            settings.setDomStorageEnabled(true);
            settings.setLayoutAlgorithm(WebSettings$LayoutAlgorithm.NARROW_COLUMNS);
            settings.setUseWideViewPort(true);
            settings.setSavePassword(true);
            settings.setSaveFormData(true);
```



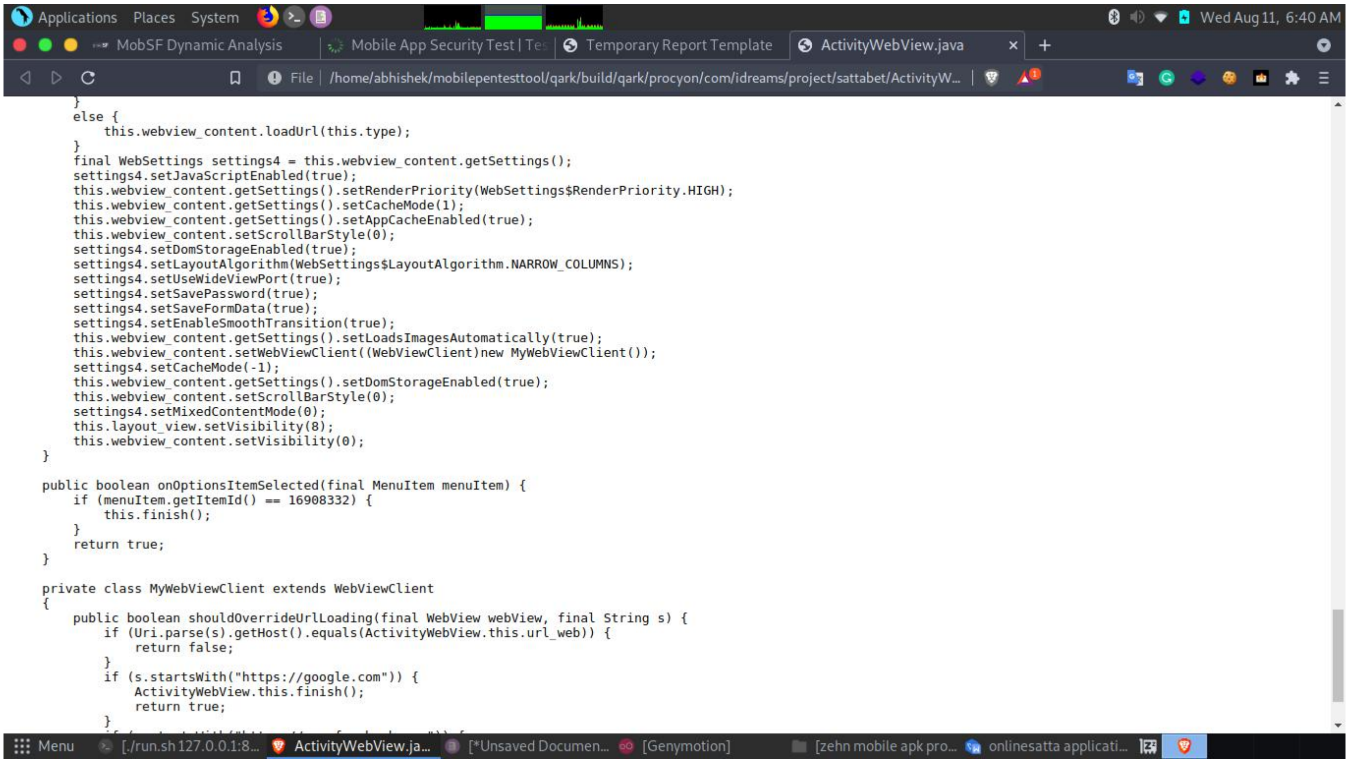
```
    @Override
    public void onBackPressed() {
        if (this.webview_content.canGoBack()) {
            this.webview_content.goBack();
            return;
        }
        super.onBackPressed();
    }

    @Override
    protected void onCreate(final Bundle bundle) {
        super.onCreate(bundle);
        this.setContentView(2131558570);
        this.getSupportActionBar().hide();
        this.viewDialoque = new ViewDialoque(this);
        final SharedPreferences sharedPreferences = this.getSharedPreferences("my_app", 0);
        this.user_id = sharedPreferences.getString("sp_emp_id", (String)null);
        sharedPreferences.getString("sp_emp_name", (String)null);
        final HttpLoggingInterceptor httpLoggingInterceptor = new HttpLoggingInterceptor();
        httpLoggingInterceptor.setLevel(HttpLoggingInterceptor.Level.BODY);
        final OkHttpClient build = new OkHttpClient.Builder().addInterceptor(httpLoggingInterceptor).build();
        final Gson create = new GsonBuilder().setLenient().create();
        this.type = this.getIntent().getStringExtra("type");
        this.retroApi = new
Retrofit.Builder().baseUrl("http://shiva999.com/").addConverterFactory(ScalarsConverterFactory.create()).addConverterFactory(GsonConverterFactory.create(create)).client(b
uild).build().create(RetroApi.class);
        this.webview_content = this.findViewById(2131362746);
        this.layout_view = this.findViewById(2131362238);
        this.getProfileView();
        if (this.type.equals("live_chat")) {
            this.url_web = "http://playsatta.co/index.php/site/live-support-chart";
            this.webview_content.loadUrl("http://playsatta.co/index.php/site/live-support-chart");
            final WebSettings settings = this.webview_content.getSettings();
            settings.setJavaScriptEnabled(true);
            this.webview_content.getSettings().setRenderPriority(WebSettings$RenderPriority.HIGH);
            this.webview_content.getSettings().setCacheMode(1);
            this.webview_content.getSettings().setAppCacheEnabled(true);
            this.webview_content.setScrollBarStyle(0);
            settings.setDomStorageEnabled(true);
            settings.setLayoutAlgorithm(WebSettings$LayoutAlgorithm.NARROW_COLUMNS);
            settings.setUseWideViewPort(true);
            settings.setSavePassword(true);
            settings.setSaveFormData(true);
```



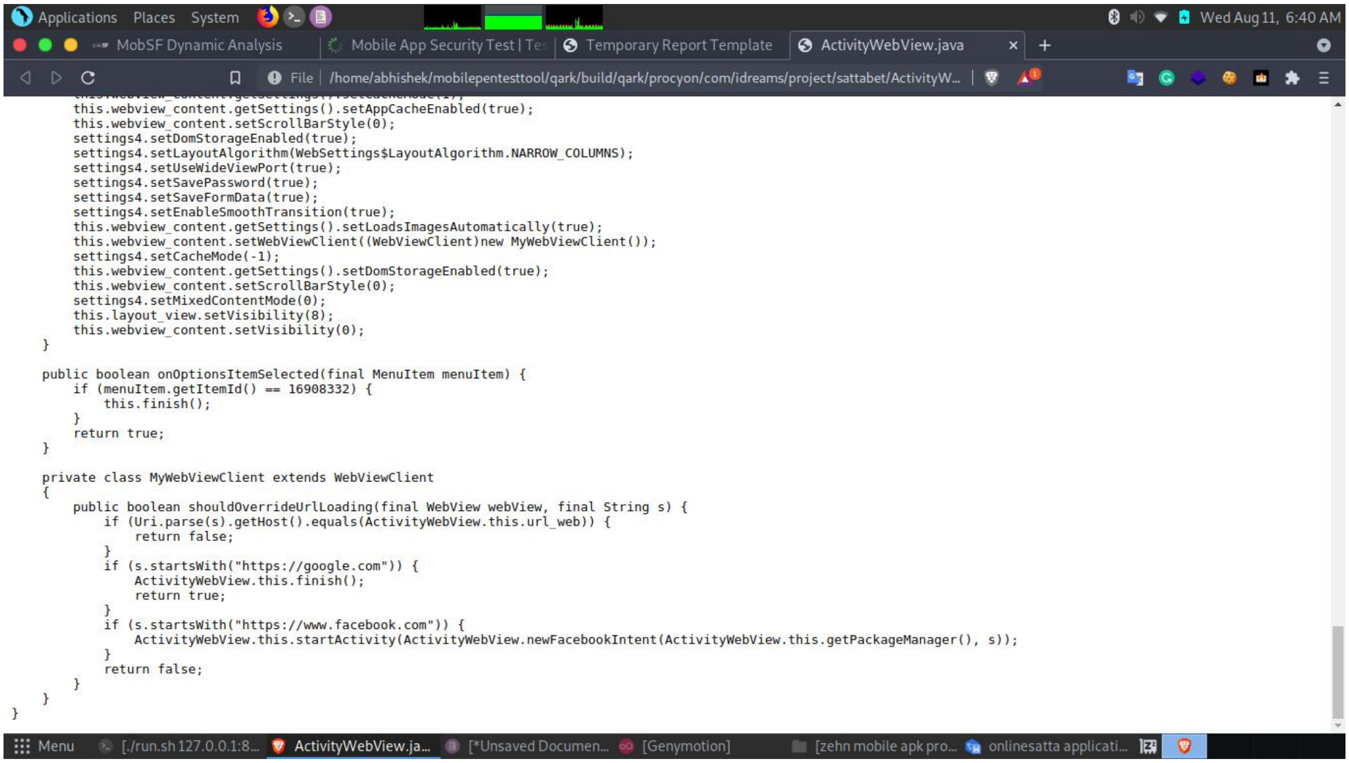
```
        this.webview_content.getSettings().setRenderPriority(WebSettings$RenderPriority.HIGH);
        this.webview_content.getSettings().setCacheMode(1);
        this.webview_content.getSettings().setAppCacheEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings.setDomStorageEnabled(true);
        settings.setLayoutAlgorithm(WebSettings$LayoutAlgorithm.NARROW_COLUMNS);
        settings.setUseWideViewPort(true);
        settings.setSavePassword(true);
        settings.setSaveFormData(true);
        settings.setEnableSmoothTransition(true);
        this.webview_content.getSettings().setLoadsImagesAutomatically(true);
        this.webview_content.setWebViewClient((WebViewClient)new MyWebViewClient());
        settings.setCacheMode(-1);
        this.webview_content.getSettings().setDomStorageEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings.setMixedContentMode(0);
        this.layout_view.setVisibility(8);
        this.webview_content.setVisibility(0);
        return;
    }
    if (this.type.equals("chart")) {
        this.url_web = "http://playsatta.co/index.php/site/chartmain";
        this.webview_content.loadUrl("http://playsatta.co/index.php/site/chartmain");
        final WebSettings settings2 = this.webview_content.getSettings();
        settings2.setJavaScriptEnabled(true);
        this.webview_content.getSettings().setRenderPriority(WebSettings$RenderPriority.HIGH);
        this.webview_content.getSettings().setCacheMode(1);
        this.webview_content.getSettings().setAppCacheEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings2.setDomStorageEnabled(true);
        settings2.setLayoutAlgorithm(WebSettings$LayoutAlgorithm.NARROW_COLUMNS);
        settings2.setUseWideViewPort(true);
        settings2.setSavePassword(true);
        settings2.setSaveFormData(true);
        settings2.setEnableSmoothTransition(true);
        this.webview_content.getSettings().setLoadsImagesAutomatically(true);
        this.webview_content.setWebViewClient((WebViewClient)new MyWebViewClient());
        settings2.setCacheMode(-1);
        this.webview_content.getSettings().setDomStorageEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings2.setMixedContentMode(0);
        this.layout_view.setVisibility(8);
        this.webview_content.setVisibility(0);
```



```
        return;
    }
    if (this.type.equals("live_result")) {
        this.url_web = "http://playsatta.co/index.php/site/domain-links";
        this.webview_content.loadUrl("http://playsatta.co/index.php/site/domain-links");
        final WebSettings settings3 = this.webview_content.getSettings();
        settings3.setJavaScriptEnabled(true);
        this.webview_content.getSettings().setRenderPriority(WebSettings$RenderPriority.HIGH);
        this.webview_content.getSettings().setCacheMode(1);
        this.webview_content.getSettings().setAppCacheEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings3.setDomStorageEnabled(true);
        settings3.setLayoutAlgorithm(WebSettings$LayoutAlgorithm.NARROW_COLUMNS);
        settings3.setUseWideViewPort(true);
        settings3.setSavePassword(true);
        settings3.setSaveFormData(true);
        settings3.setEnableSmoothTransition(true);
        this.webview_content.getSettings().setLoadsImagesAutomatically(true);
        this.webview_content.setWebViewClient((WebViewClient)new MyWebViewClient());
        settings3.setCacheMode(-1);
        this.webview_content.getSettings().setDomStorageEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings3.setMixedContentMode(0);
        this.layout_view.setVisibility(8);
        this.webview_content.setVisibility(0);
        return;
    }
    if (this.type.startsWith("Terms_Condition : ")) {
        this.webview_content.loadUrl(this.type.replace("Terms_Condition : ", "").trim());
    }
    else {
        this.webview_content.loadUrl(this.type);
    }
    final WebSettings settings4 = this.webview_content.getSettings();
    settings4.setJavaScriptEnabled(true);
    this.webview_content.getSettings().setRenderPriority(WebSettings$RenderPriority.HIGH);
    this.webview_content.getSettings().setCacheMode(1);
    this.webview_content.getSettings().setAppCacheEnabled(true);
    this.webview_content.setScrollBarStyle(0);
    settings4.setDomStorageEnabled(true);
    settings4.setLayoutAlgorithm(WebSettings$LayoutAlgorithm.NARROW_COLUMNS);
    settings4.setUseWideViewPort(true);
    settings4.setSavePassword(true);
```



```
        }
        else {
            this.webview_content.loadUrl(this.type);
        }
        final WebSettings settings4 = this.webview_content.getSettings();
        settings4.setJavaScriptEnabled(true);
        this.webview_content.getSettings().setRenderPriority(WebSettings$RenderPriority.HIGH);
        this.webview_content.getSettings().setCacheMode(1);
        this.webview_content.getSettings().setAppCacheEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings4.setDomStorageEnabled(true);
        settings4.setLayoutAlgorithm(WebSettings$LayoutAlgorithm.NARROW_COLUMNS);
        settings4.setUseWideViewPort(true);
        settings4.setSavePassword(true);
        settings4.setSaveFormData(true);
        settings4.setEnableSmoothTransition(true);
        this.webview_content.getSettings().setLoadsImagesAutomatically(true);
        this.webview_content.setWebViewClient((WebViewClient)new MyWebViewClient());
        settings4.setCacheMode(-1);
        this.webview_content.getSettings().setDomStorageEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings4.setMixedContentMode(0);
        this.layout_view.setVisibility(8);
        this.webview_content.setVisibility(0);
    }

    public boolean onOptionsItemSelected(final MenuItem menuItem) {
        if (menuItem.getItemId() == 16908332) {
            this.finish();
        }
        return true;
    }

    private class MyWebViewClient extends WebViewClient
    {
        public boolean shouldOverrideUrlLoading(final WebView webView, final String s) {
            if (Uri.parse(s).getHost().equals(ActivityWebView.this.url_web)) {
                return false;
            }
            if (s.startsWith("https://google.com")) {
                ActivityWebView.this.finish();
                return true;
            }
```



```
        this.webview_content.getSettings().setAppCacheEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings4.setDomStorageEnabled(true);
        settings4.setLayoutAlgorithm(WebSettings$LayoutAlgorithm.NARROW_COLUMNS);
        settings4.setUseWideViewPort(true);
        settings4.setSavePassword(true);
        settings4.setSaveFormData(true);
        settings4.setEnableSmoothTransition(true);
        this.webview_content.getSettings().setLoadsImagesAutomatically(true);
        this.webview_content.setWebViewClient((WebViewClient)new MyWebViewClient());
        settings4.setCacheMode(-1);
        this.webview_content.getSettings().setDomStorageEnabled(true);
        this.webview_content.setScrollBarStyle(0);
        settings4.setMixedContentMode(0);
        this.layout_view.setVisibility(8);
        this.webview_content.setVisibility(0);
    }

    public boolean onOptionsItemSelected(final MenuItem menuItem) {
        if (menuItem.getItemId() == 16908332) {
            this.finish();
        }
        return true;
    }

    private class MyWebViewClient extends WebViewClient
    {
        public boolean shouldOverrideUrlLoading(final WebView webView, final String s) {
            if (Uri.parse(s).getHost().equals(ActivityWebView.this.url_web)) {
                return false;
            }
            if (s.startsWith("https://google.com")) {
                ActivityWebView.this.finish();
                return true;
            }
```

```
            if (s.startsWith("https://www.facebook.com")) {
                ActivityWebView.this.startActivity(ActivityWebView.newFacebookIntent(ActivityWebView.this.getPackageManager(), s));
            }
            return false;
        }
    }
}
```

Remediation:

Who:	online satta
Vector:	Information disclosuer
Action:	Do not disclouse any type of information

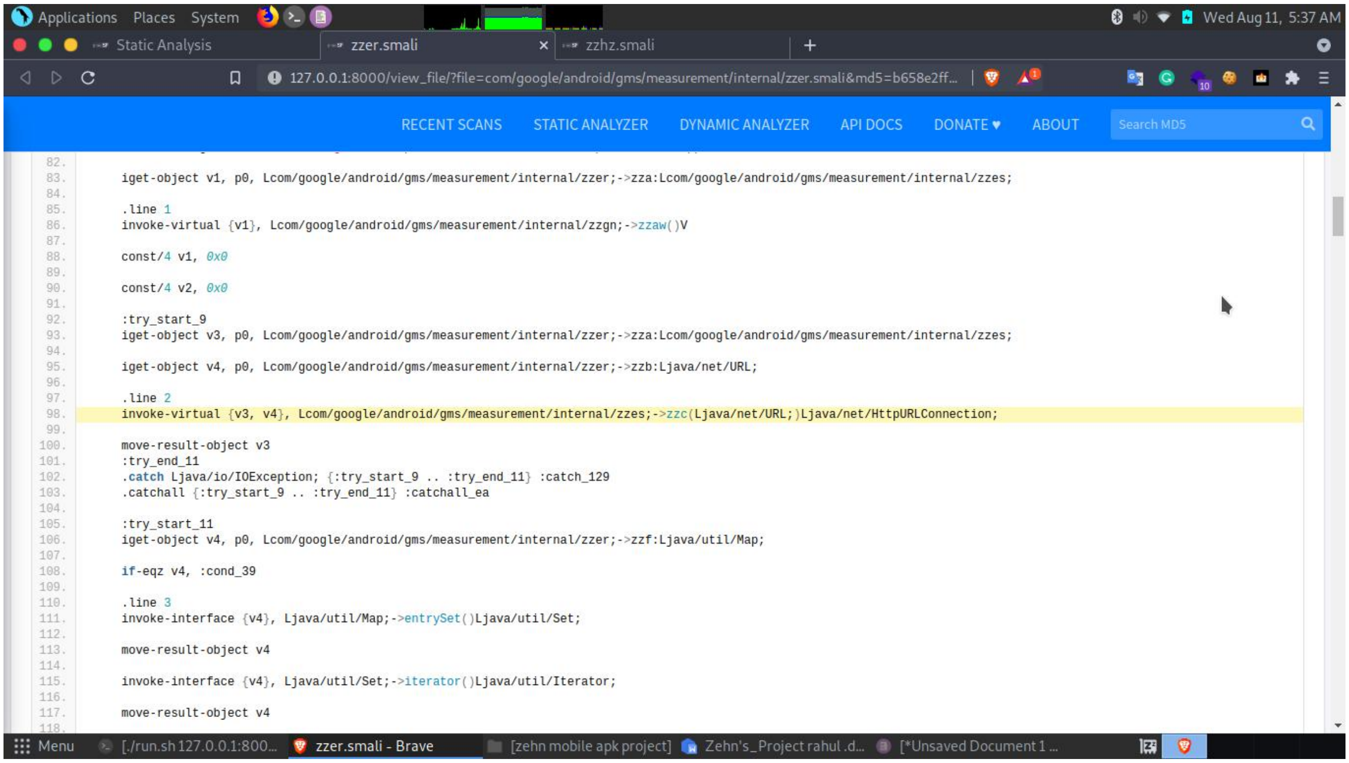
PENETRATION TEST FINDINGS QUARK

Connect to a URL and read data from it(Low)

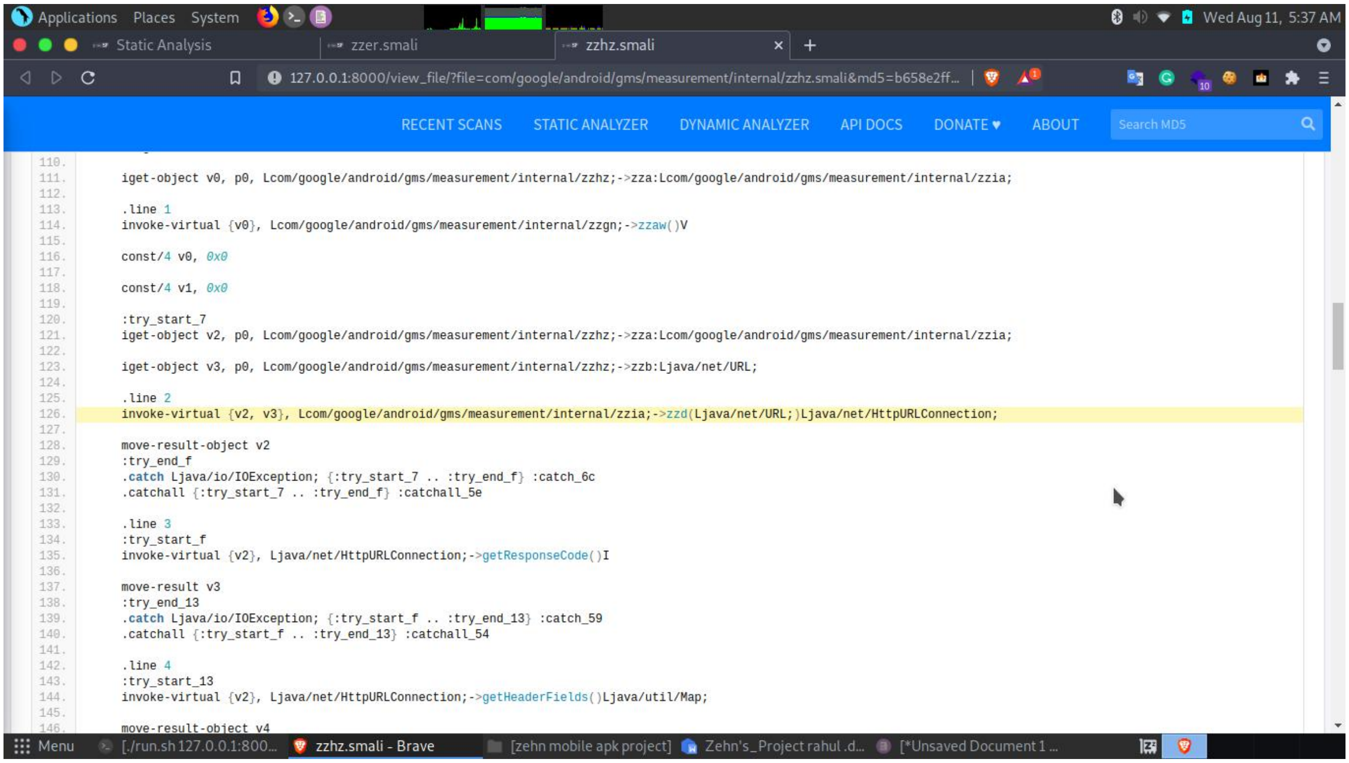
Description:	app can connect the url and read the data
Impact:	mainly impact on user privacy
Path:	com/google/android/gms/measurement/internal/zzer.smali -> run()V com/google/android/gms/measurement/internal/zzhz.smali -> run()V
References:	https://blog.codavel.com/how-to-integrate-httpurlconnection

Exploitation Proof of Concept

Abhishek Joshi gathered this vulnerability from Manual testing using testing tools with proper path and parameters.



```
    iget-object v1, p0, Lcom/google/android/gms/measurement/internal/zzer;->zza:Lcom/google/android/gms/measurement/internal/zzes;

    .line 1
    invoke-virtual {v1}, Lcom/google/android/gms/measurement/internal/zzgn;->zzaw()V

    const/4 v1, 0x0

    const/4 v2, 0x0

    :try_start_9
    iget-object v3, p0, Lcom/google/android/gms/measurement/internal/zzer;->zza:Lcom/google/android/gms/measurement/internal/zzes;

    iget-object v4, p0, Lcom/google/android/gms/measurement/internal/zzer;->zzb:Ljava/net/URL;

    .line 2
    invoke-virtual {v3, v4}, Lcom/google/android/gms/measurement/internal/zzes;->zzc(Ljava/net/URL;)Ljava/net/HttpURLConnection;

    move-result-object v3
    :try_end_11
    .catch Ljava/io/IOException; {:try_start_9 .. :try_end_11} :catch_129
    .catchall {:try_start_9 .. :try_end_11} :catchall_ea

    :try_start_11
    iget-object v4, p0, Lcom/google/android/gms/measurement/internal/zzer;->zzf:Ljava/util/Map;

    if-eqz v4, :cond_39

    .line 3
    invoke-interface {v4}, Ljava/util/Map;->entrySet()Ljava/util/Set;

    move-result-object v4

    invoke-interface {v4}, Ljava/util/Set;->iterator()Ljava/util/Iterator;

    move-result-object v4
```



```
    iget-object v0, p0, Lcom/google/android/gms/measurement/internal/zzhz;->zza:Lcom/google/android/gms/measurement/internal/zzia;

    .line 1
    invoke-virtual {v0}, Lcom/google/android/gms/measurement/internal/zzgn;->zzaw()V

    const/4 v0, 0x0

    const/4 v1, 0x0

    :try_start_7
    iget-object v2, p0, Lcom/google/android/gms/measurement/internal/zzhz;->zza:Lcom/google/android/gms/measurement/internal/zzia;

    iget-object v3, p0, Lcom/google/android/gms/measurement/internal/zzhz;->zzb:Ljava/net/URL;

    .line 2
    invoke-virtual {v2, v3}, Lcom/google/android/gms/measurement/internal/zzia;->zzd(Ljava/net/URL;)Ljava/net/HttpURLConnection;

    move-result-object v2
    :try_end_f
    .catch Ljava/io/IOException; {:try_start_7 .. :try_end_f} :catch_6c
    .catchall {:try_start_7 .. :try_end_f} :catchall_5e

    .line 3
    :try_start_f
    invoke-virtual {v2}, Ljava/net/HttpURLConnection;->getResponseCode()I

    move-result v3
    :try_end_13
    .catch Ljava/io/IOException; {:try_start_f .. :try_end_13} :catch_59
    .catchall {:try_start_f .. :try_end_13} :catchall_54

    .line 4
    :try_start_13
    invoke-virtual {v2}, Ljava/net/HttpURLConnection;->getHeaderFields()Ljava/util/Map;

    move-result-object v4
```

Remediation :

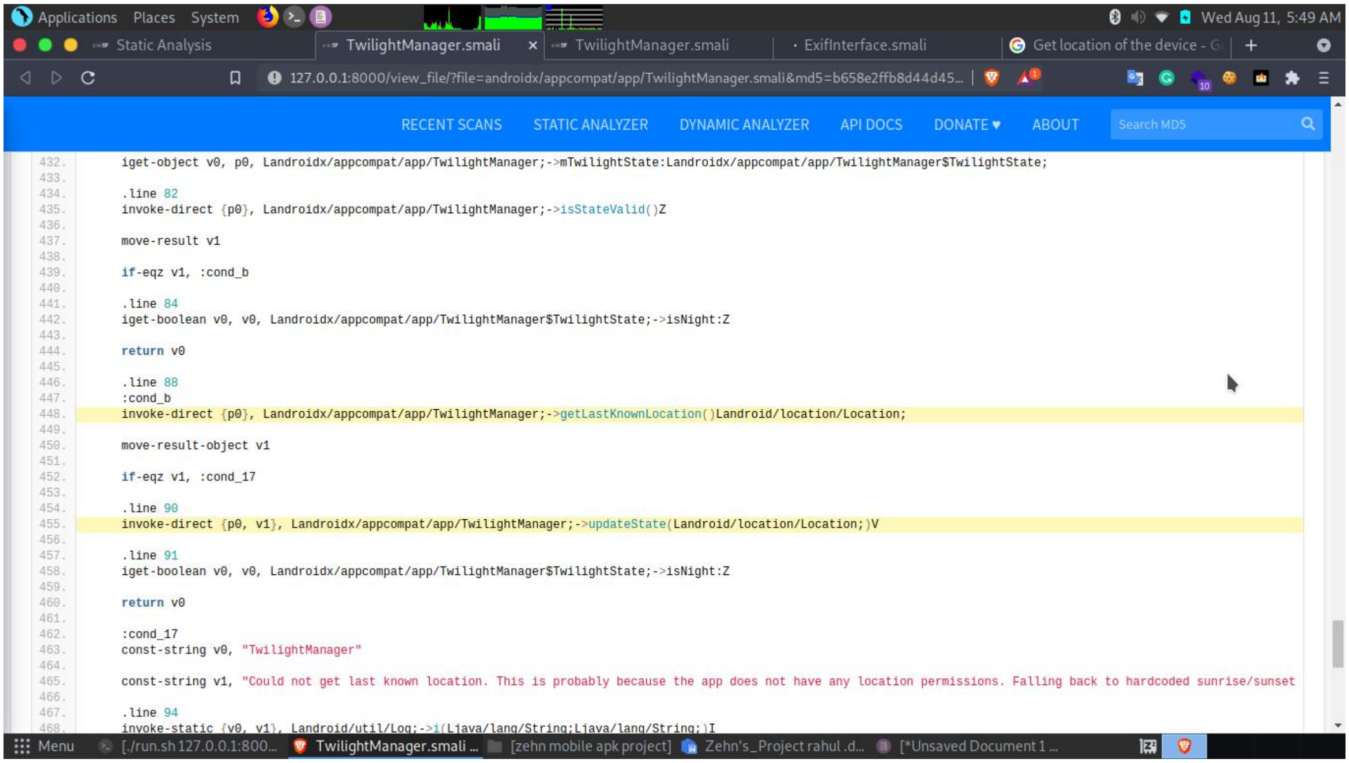
Who:	online satta
Vector:	privacy
Action:	-App connect the url and read the data -you can allow the filter and sanitize the code -you can use alternative method to solve this issues

Get last known location of the device(High)

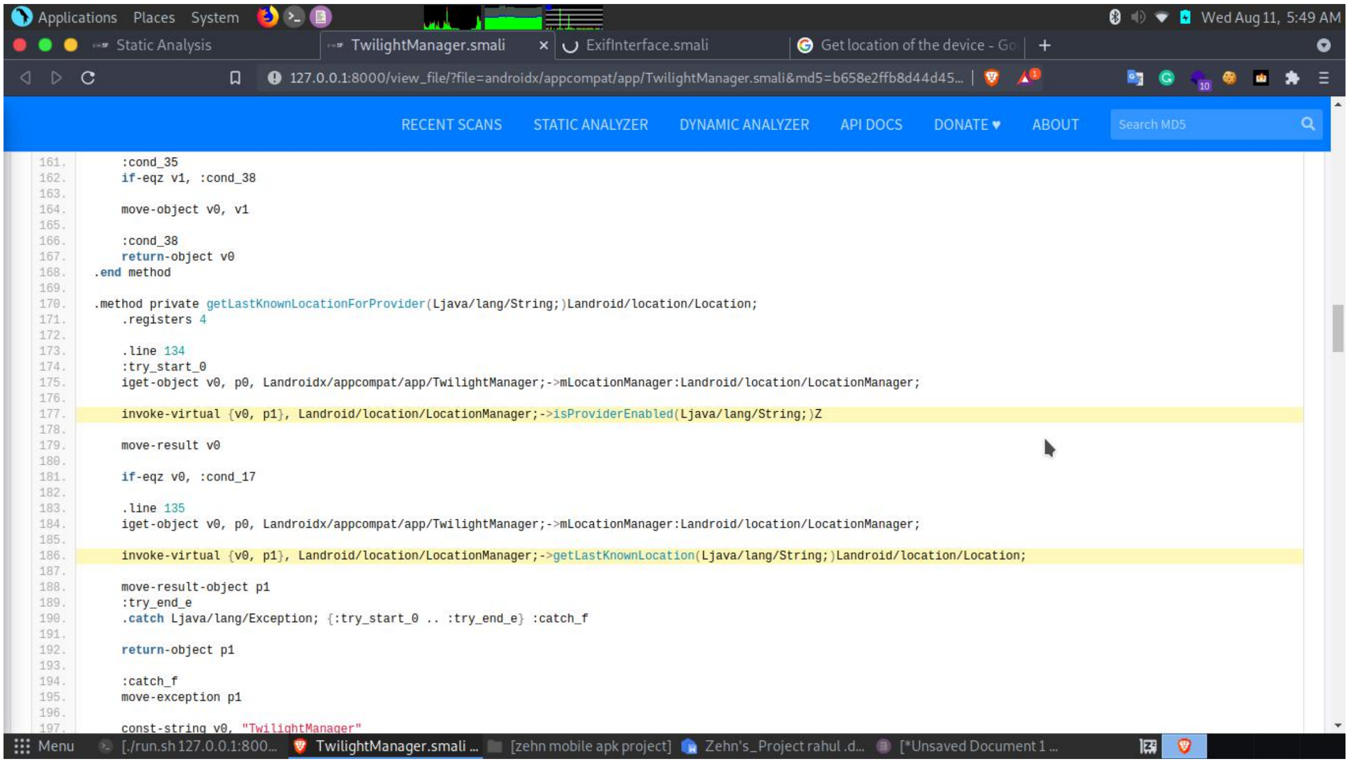
Description:	Get last known location of the device now days privacy should be matter many application banned because of privacy you canot allow and capture the location
Impact:	location of the device should gather the last known location
Path:	androidx/appcompat/app/TwilightManager.smali -> isNight()Z androidx/appcompat/app/TwilightManager.smali -> getLastKnownLocationForProvider(Ljava/lang/String;)Landroid/location/Location;
References:	https://developer.android.com/training/location/retrieve-current https://developers.google.com/maps/documentation/javascript/geolocation

Exploitation Proof of Concept

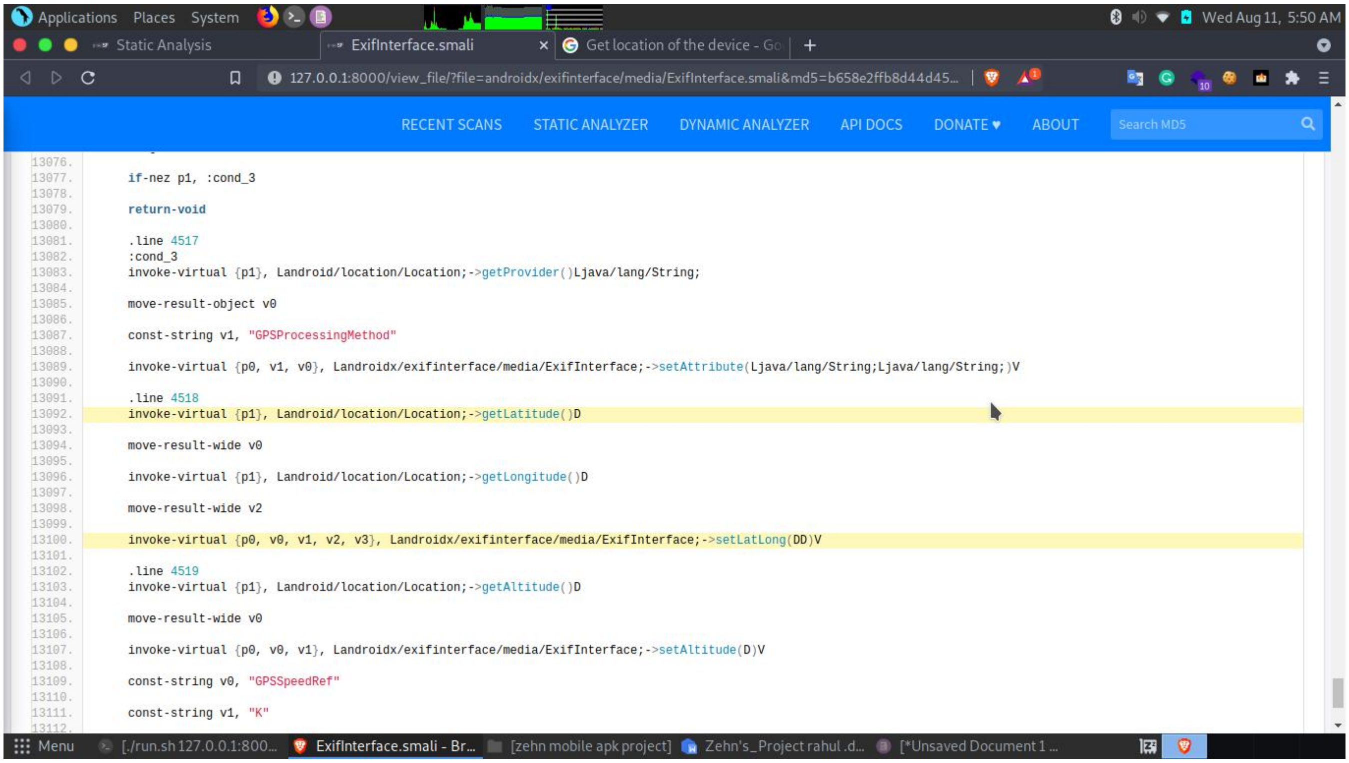
Abhishek Joshi gathered this vulnerability from Manual testing using testing tools with proper path and parameters.


Applications
Places
System
Wed Aug 11, 5:49 AM
Static Analysis
TwilightManager.smali
TwilightManager.smali
ExifInterface.smali
Get location of the device - G
127.0.0.1:8000/view_file/?file=androidx/appcompat/app/TwilightManager.smali&md5=b658e2ffb8d44d45...
RECENT SCANS
STATIC ANALYZER
DYNAMIC ANALYZER
API DOCS
DONATE ♥
ABOUT
Search MD5
Menu
[./run.sh 127.0.0.1:800...
TwilightManager.smali ...
[zehn mobile apk project]
Zehn's_Project rahul .d...
[*Unsaved Document 1 ...

```
    iget-object v0, p0, Landroidx/appcompat/app/TwilightManager;->mTwilightState:Landroidx/appcompat/app/TwilightManager$TwilightState;

    .line 82
    invoke-direct {p0}, Landroidx/appcompat/app/TwilightManager;->isStateValid()Z

    move-result v1

    if-eqz v1, :cond_b

    .line 84
    iget-boolean v0, v0, Landroidx/appcompat/app/TwilightManager$TwilightState;->isNight:Z

    return v0

    .line 88
    :cond_b
    invoke-direct {p0}, Landroidx/appcompat/app/TwilightManager;->getLastKnownLocation()Landroid/location/Location;

    move-result-object v1

    if-eqz v1, :cond_17

    .line 90
    invoke-direct {p0, v1}, Landroidx/appcompat/app/TwilightManager;->updateState(Landroid/location/Location;)V

    .line 91
    iget-boolean v0, v0, Landroidx/appcompat/app/TwilightManager$TwilightState;->isNight:Z

    return v0

    :cond_17
    const-string v0, "TwilightManager"

    const-string v1, "Could not get last known location. This is probably because the app does not have any location permissions. Falling back to hardcoded sunrise/sunset

    .line 94
    invoke-static {v0, v1}, Landroid/util/Log;->i(Ljava/lang/String;Ljava/lang/String;)I
```


Applications
Places
System
Wed Aug 11, 5:49 AM
Static Analysis
TwilightManager.smali
ExifInterface.smali
Get location of the device - Go
127.0.0.1:8000/view_file/?file=androidx/appcompat/app/TwilightManager.smali&md5=b658e2ffb8d44d45...
RECENT SCANS
STATIC ANALYZER
DYNAMIC ANALYZER
API DOCS
DONATE ♥
ABOUT
Search MD5
Menu
[./run.sh 127.0.0.1:800...
TwilightManager.smali ...
[zehn mobile apk project]
Zehn's_Project rahul .d...
[*Unsaved Document 1 ...

```
    :cond_35
    if-eqz v1, :cond_38

    move-object v0, v1

    :cond_38
    return-object v0
.end method

.method private getLastKnownLocationForProvider(Ljava/lang/String;)Landroid/location/Location;
    .registers 4

    .line 134
    :try_start_0
    iget-object v0, p0, Landroidx/appcompat/app/TwilightManager;->mLocationManager:Landroid/location/LocationManager;

    invoke-virtual {v0, p1}, Landroid/location/LocationManager;->isProviderEnabled(Ljava/lang/String;)Z

    move-result v0

    if-eqz v0, :cond_17

    .line 135
    iget-object v0, p0, Landroidx/appcompat/app/TwilightManager;->mLocationManager:Landroid/location/LocationManager;

    invoke-virtual {v0, p1}, Landroid/location/LocationManager;->getLastKnownLocation(Ljava/lang/String;)Landroid/location/Location;

    move-result-object p1
    :try_end_e
    .catch Ljava/lang/Exception; {:try_start_0 .. :try_end_e} :catch_f

    return-object p1

    :catch_f
    move-exception p1

    const-string v0, "TwilightManager"
```


Applications
Places
System
Wed Aug 11, 5:50 AM
Static Analysis
ExifInterface.smali
Get location of the device - Go
127.0.0.1:8000/view_file/?file=androidx/exifinterface/media/ExifInterface.smali&md5=b658e2ffb8d44d45...
RECENT SCANS
STATIC ANALYZER
DYNAMIC ANALYZER
API DOCS
DONATE ♥
ABOUT
Search MD5
Menu
[./run.sh 127.0.0.1:800...
ExifInterface.smali - Br...
[zehn mobile apk project]
Zehn's_Project rahul .d...
[*Unsaved Document 1 ...

```
    if-nez p1, :cond_3

    return-void

    .line 4517
    :cond_3
    invoke-virtual {p1}, Landroid/location/Location;->getProvider()Ljava/lang/String;

    move-result-object v0

    const-string v1, "GPSProcessingMethod"

    invoke-virtual {p0, v1, v0}, Landroidx/exifinterface/media/ExifInterface;->setAttribute(Ljava/lang/String;Ljava/lang/String;)V

    .line 4518
    invoke-virtual {p1}, Landroid/location/Location;->getLatitude()D

    move-result-wide v0

    invoke-virtual {p1}, Landroid/location/Location;->getLongitude()D

    move-result-wide v2

    invoke-virtual {p0, v0, v1, v2, v3}, Landroidx/exifinterface/media/ExifInterface;->setLatLong(DD)V

    .line 4519
    invoke-virtual {p1}, Landroid/location/Location;->getAltitude()D

    move-result-wide v0

    invoke-virtual {p0, v0, v1}, Landroidx/exifinterface/media/ExifInterface;->setAltitude(D)V

    const-string v0, "GPSSpeedRef"

    const-string v1, "K"
```

Remediation

Who:	online satta
Vector:	privacy
Action:	-dont violate the use privacy.

Read sensitive data(SMS, CALLLOG, etc (High)

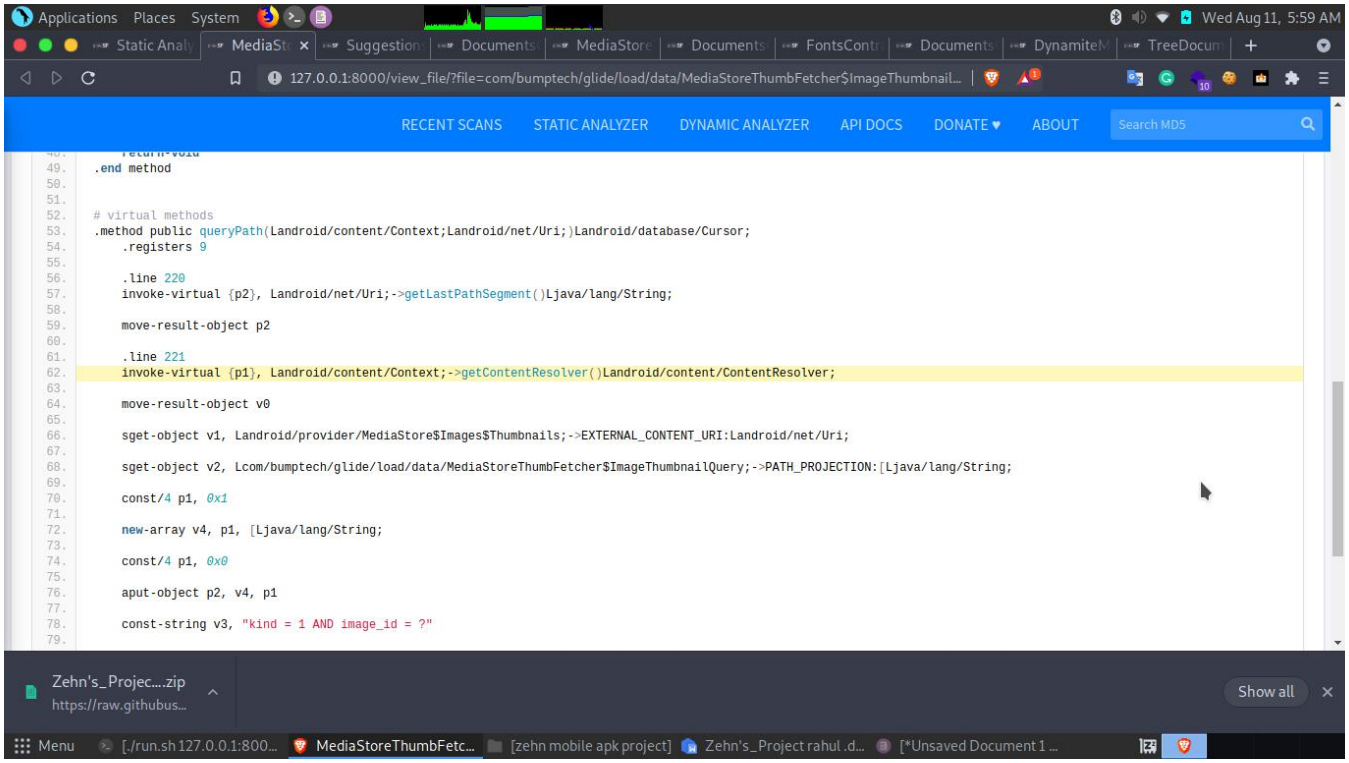
Description:	Read sensitive data SMS,Callog etc
Impact:	directly impact to the user privacy

Path:	com/bumptech/glide/load/data/MediaStoreThumbFetcher$ImageThumbnailQuery.smali -> queryPath(Landroid/content/Context;Landroid/net/Uri;)Landroid/database/Cursor;
	androidx/appcompat/widget/SuggestionsAdapter.smali -> getSearchManagerSuggestions(Landroid/app/SearchableInfo;Ljava/lang/String;I)Landroid/database/Cursor;
	androidx/documentfile/provider/DocumentsContractApi19.smali -> queryForString(Landroid/content/Context;Landroid/net/Uri;Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String;
	com/bumptech/glide/load/data/MediaStoreThumbFetcher$VideoThumbnailQuery.smali -> queryPath(Landroid/content/Context;Landroid/net/Uri;)Landroid/database/Cursor;
	androidx/documentfile/provider/DocumentsContractApi19.smali -> queryForLong(Landroid/content/Context;Landroid/net/Uri;Ljava/lang/String;J)J
	androidx/core/provider/FontsContractCompat.smali -> getFontFromProvider(Landroid/content/Context;Landroidx/core/provider/FontRequest;Ljava/lang/String;Landroid/os/CancellationSignal;)[Landroidx/core/provider/FontsContractCompat$FontInfo;
	androidx/documentfile/provider/DocumentsContractApi19.smali -> exists(Landroid/content/Context;Landroid/net/Uri;)Z
	com/google/android/gms/dynamite/DynamiteModule.smali -> zzc(Landroid/content/Context;Ljava/lang/String;Z)I
	androidx/documentfile/provider/TreeDocumentFile.smali -> listFiles()[Landroidx/documentfile/provider/DocumentFile;

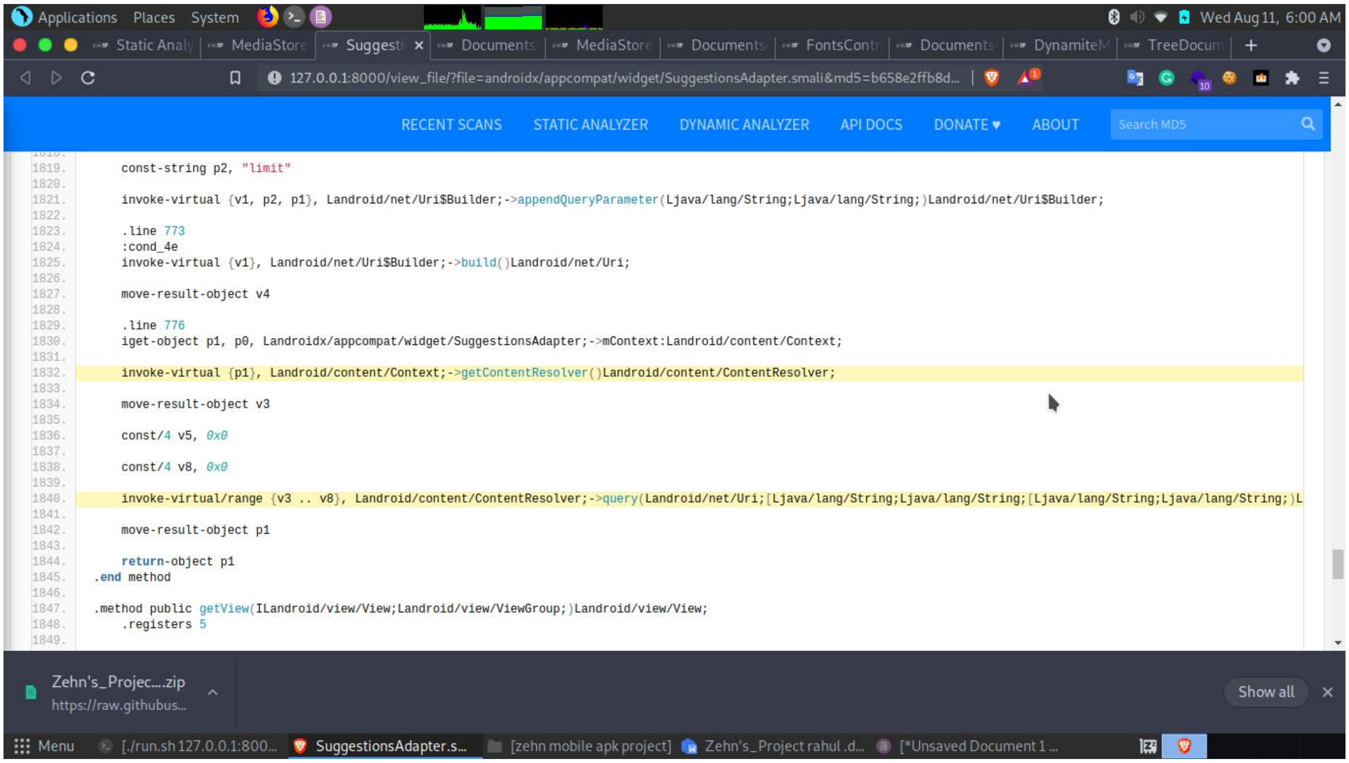
References:	

Exploitation Proof of Concept

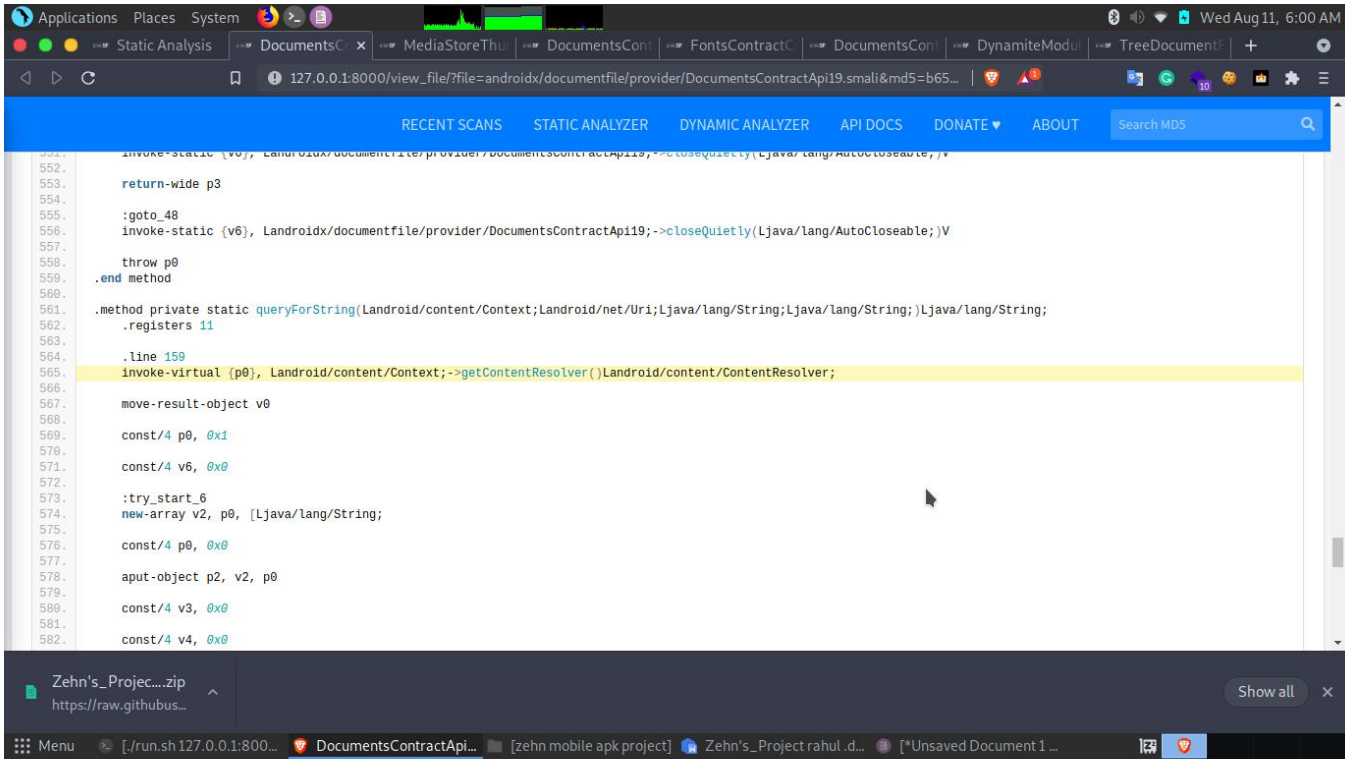
Abhishek Joshi gathered this vulnerability from Manual testing using testing tools with proper path and parameters.



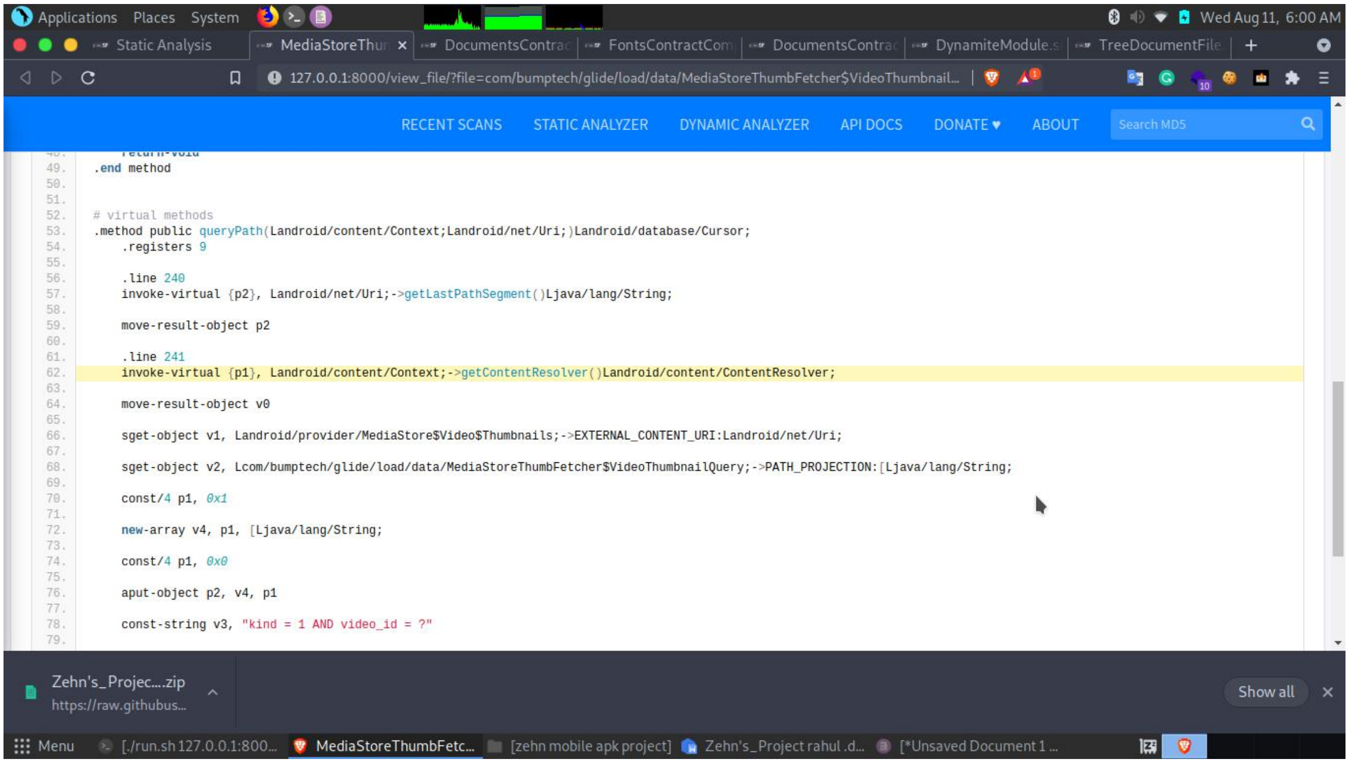
```
    return-void
.end method


# virtual methods
.method public queryPath(Landroid/content/Context;Landroid/net/Uri;)Landroid/database/Cursor;
    .registers 9

    .line 220
    invoke-virtual {p2}, Landroid/net/Uri;->getLastPathSegment()Ljava/lang/String;

    move-result-object p2

    .line 221
    invoke-virtual {p1}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v0

    sget-object v1, Landroid/provider/MediaStore$Images$Thumbnails;->EXTERNAL_CONTENT_URI:Landroid/net/Uri;

    sget-object v2, Lcom/bumptech/glide/load/data/MediaStoreThumbFetcher$ImageThumbnailQuery;->PATH_PROJECTION:[Ljava/lang/String;

    const/4 p1, 0x1

    new-array v4, p1, [Ljava/lang/String;

    const/4 p1, 0x0

    aput-object p2, v4, p1

    const-string v3, "kind = 1 AND image_id = ?"

```



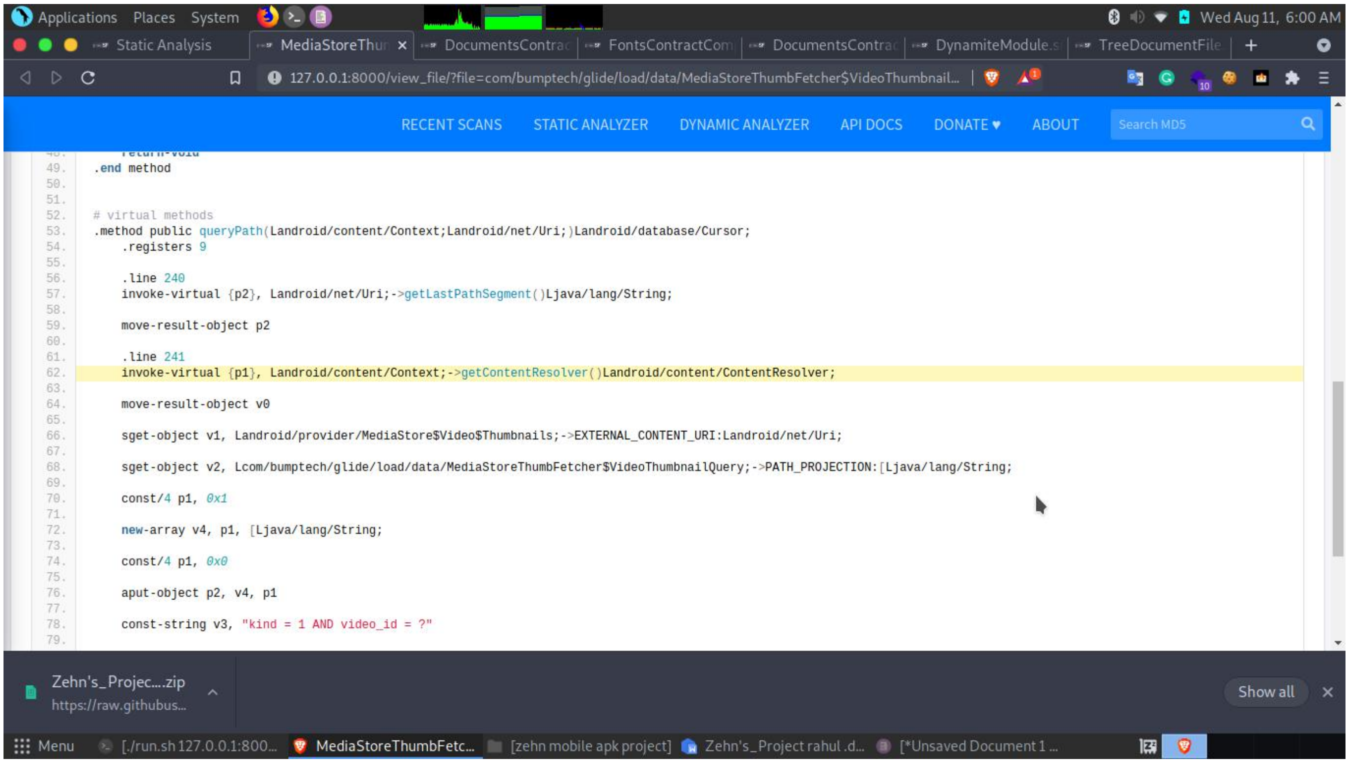
```
    const-string p2, "limit"

    invoke-virtual {v1, p2, p1}, Landroid/net/Uri$Builder;->appendQueryParameter(Ljava/lang/String;Ljava/lang/String;)Landroid/net/Uri$Builder;

    .line 773
    :cond_4e
    invoke-virtual {v1}, Landroid/net/Uri$Builder;->build()Landroid/net/Uri;

    move-result-object v4

    .line 776
    iget-object p1, p0, Landroidx/appcompat/widget/SuggestionsAdapter;->mContext:Landroid/content/Context;

    invoke-virtual {p1}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v3

    const/4 v5, 0x0

    const/4 v8, 0x0

    invoke-virtual/range {v3 .. v8}, Landroid/content/ContentResolver;->query(Landroid/net/Uri;[Ljava/lang/String;Ljava/lang/String;[Ljava/lang/String;Ljava/lang/String;)L

    move-result-object p1

    return-object p1
.end method

.method public getView(ILandroid/view/View;Landroid/view/ViewGroup;)Landroid/view/View;
    .registers 5

```



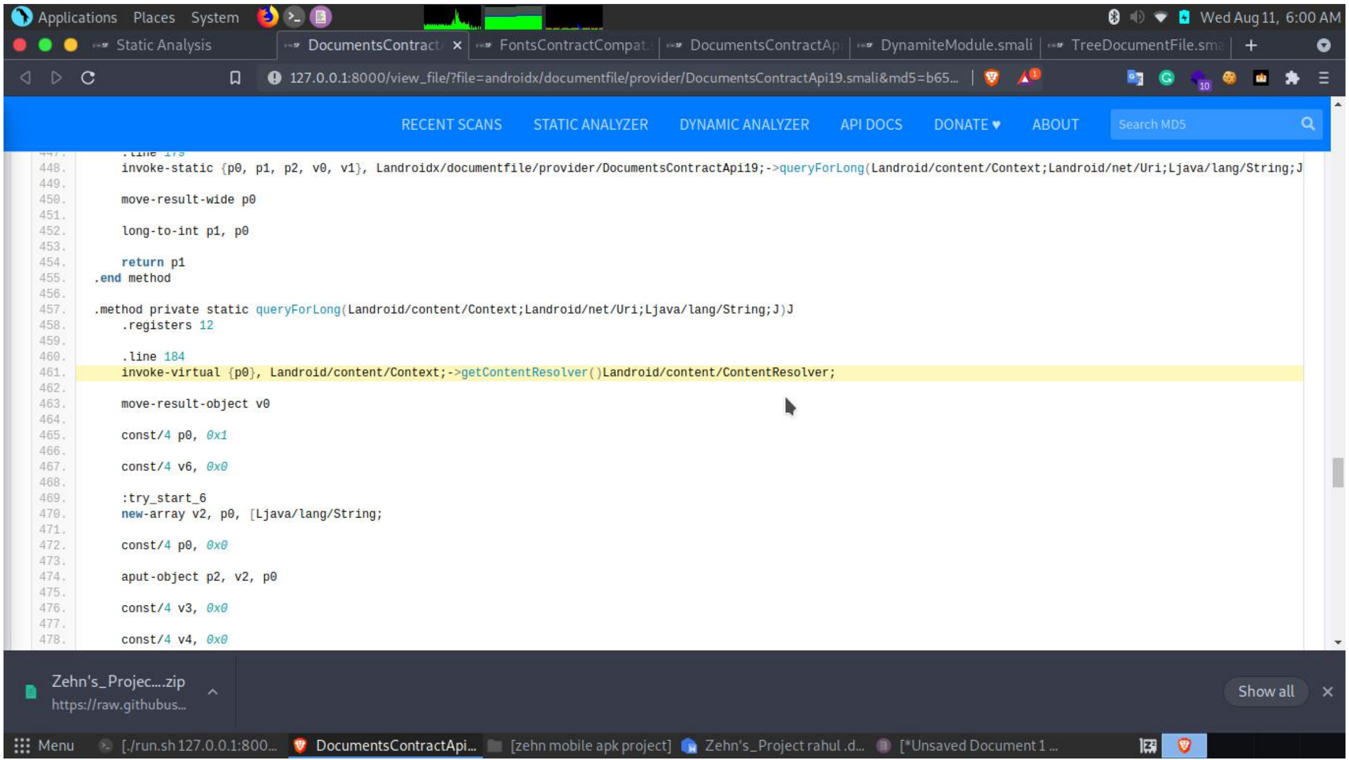
```
    invoke-static {v0}, Landroidx/documentfile/provider/DocumentsContractApi19;->closeQuietly(Ljava/lang/AutoCloseable;)V

    return-wide p3

    :goto_48
    invoke-static {v6}, Landroidx/documentfile/provider/DocumentsContractApi19;->closeQuietly(Ljava/lang/AutoCloseable;)V

    throw p0
.end method

.method private static queryForString(Landroid/content/Context;Landroid/net/Uri;Ljava/lang/String;Ljava/lang/String;)Ljava/lang/String;
    .registers 11

    .line 159
    invoke-virtual {p0}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v0

    const/4 p0, 0x1

    const/4 v6, 0x0

    :try_start_6
    new-array v2, p0, [Ljava/lang/String;

    const/4 p0, 0x0

    aput-object p2, v2, p0

    const/4 v3, 0x0

    const/4 v4, 0x0
```



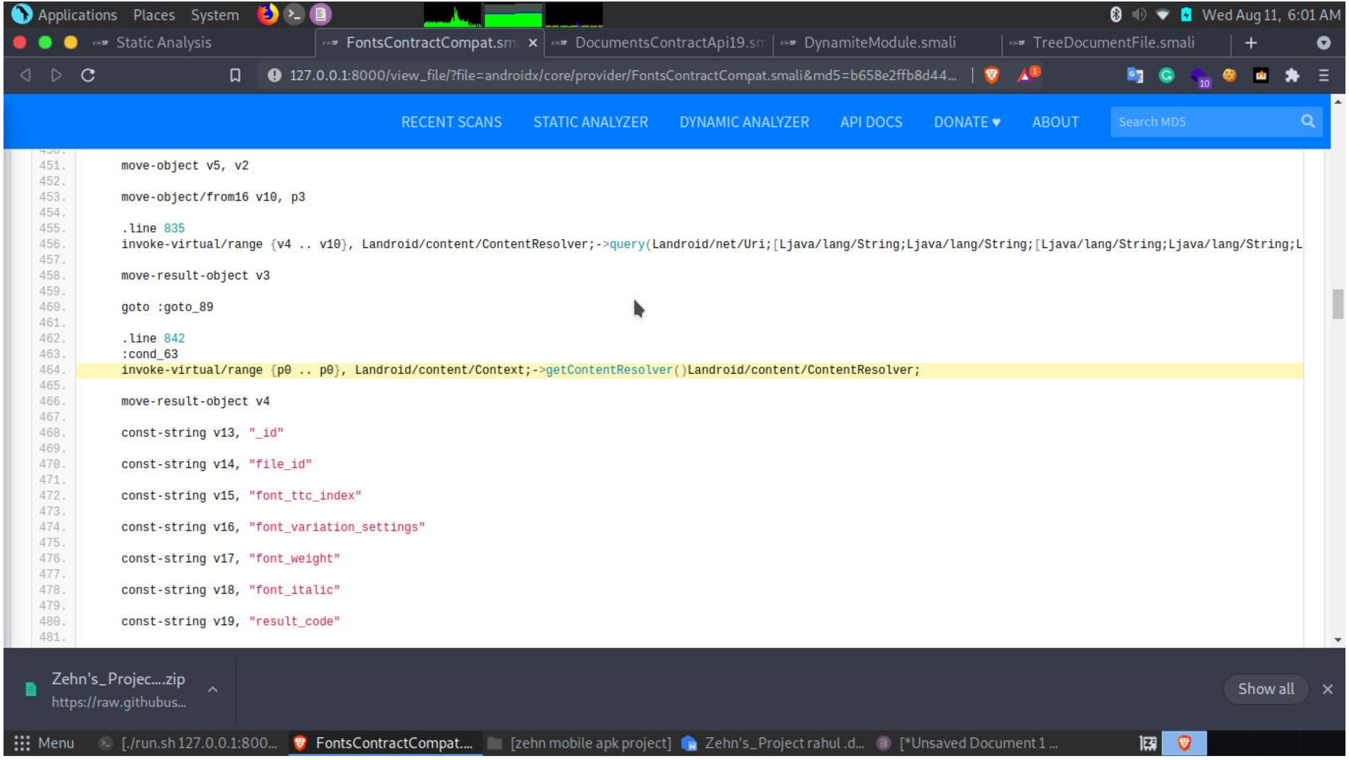
```
    return-void
.end method


# virtual methods
.method public queryPath(Landroid/content/Context;Landroid/net/Uri;)Landroid/database/Cursor;
    .registers 9

    .line 240
    invoke-virtual {p2}, Landroid/net/Uri;->getLastPathSegment()Ljava/lang/String;

    move-result-object p2

    .line 241
    invoke-virtual {p1}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v0

    sget-object v1, Landroid/provider/MediaStore$Video$Thumbnails;->EXTERNAL_CONTENT_URI:Landroid/net/Uri;

    sget-object v2, Lcom/bumptech/glide/load/data/MediaStoreThumbFetcher$VideoThumbnailQuery;->PATH_PROJECTION:[Ljava/lang/String;

    const/4 p1, 0x1

    new-array v4, p1, [Ljava/lang/String;

    const/4 p1, 0x0

    aput-object p2, v4, p1

    const-string v3, "kind = 1 AND video_id = ?"

```



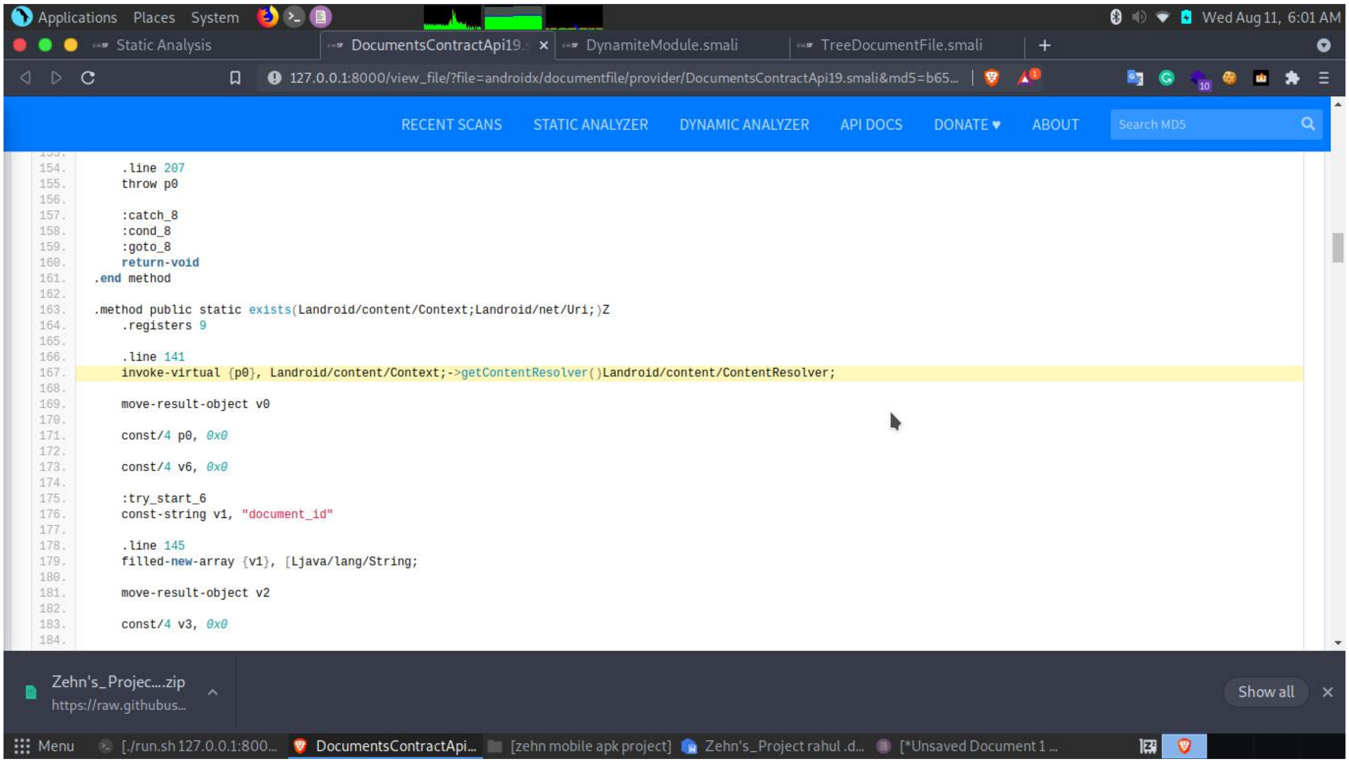
```
    return-void
.end method


# virtual methods
.method public queryPath(Landroid/content/Context;Landroid/net/Uri;)Landroid/database/Cursor;
    .registers 9

    .line 240
    invoke-virtual {p2}, Landroid/net/Uri;->getLastPathSegment()Ljava/lang/String;

    move-result-object p2

    .line 241
    invoke-virtual {p1}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v0

    sget-object v1, Landroid/provider/MediaStore$Video$Thumbnails;->EXTERNAL_CONTENT_URI:Landroid/net/Uri;

    sget-object v2, Lcom/bumptech/glide/load/data/MediaStoreThumbFetcher$VideoThumbnailQuery;->PATH_PROJECTION:[Ljava/lang/String;

    const/4 p1, 0x1

    new-array v4, p1, [Ljava/lang/String;

    const/4 p1, 0x0

    aput-object p2, v4, p1

    const-string v3, "kind = 1 AND video_id = ?"

```



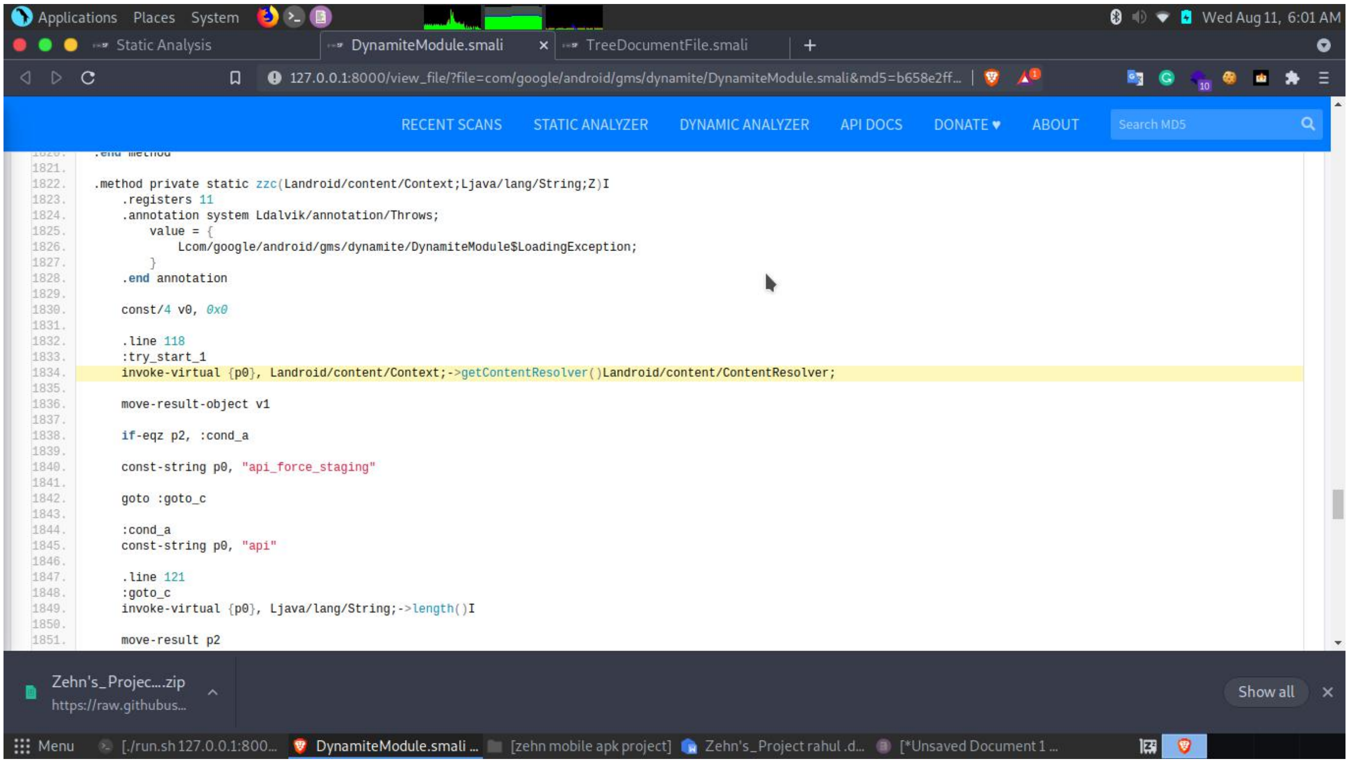
```
    .line 179
    invoke-static {p0, p1, p2, v0, v1}, Landroidx/documentfile/provider/DocumentsContractApi19;->queryForLong(Landroid/content/Context;Landroid/net/Uri;Ljava/lang/String;J

    move-result-wide p0

    long-to-int p1, p0

    return p1
.end method

.method private static queryForLong(Landroid/content/Context;Landroid/net/Uri;Ljava/lang/String;J)J
    .registers 12

    .line 184
    invoke-virtual {p0}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v0

    const/4 p0, 0x1

    const/4 v6, 0x0

    :try_start_6
    new-array v2, p0, [Ljava/lang/String;

    const/4 p0, 0x0

    aput-object p2, v2, p0

    const/4 v3, 0x0

    const/4 v4, 0x0
```



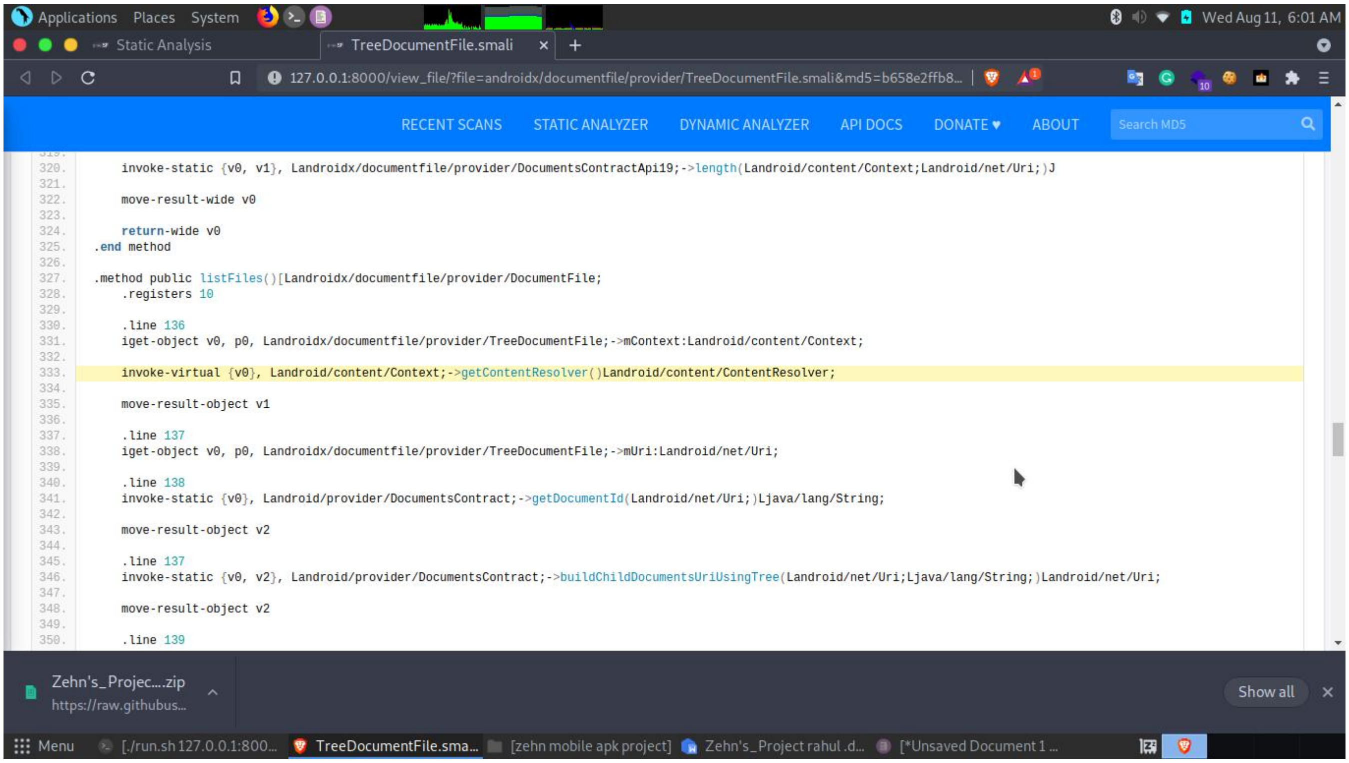
```
    move-object v5, v2

    move-object/from16 v10, p3

    .line 835
    invoke-virtual/range {v4 .. v10}, Landroid/content/ContentResolver;->query(Landroid/net/Uri;[Ljava/lang/String;Ljava/lang/String;[Ljava/lang/String;Ljava/lang/String;L

    move-result-object v3

    goto :goto_89

    .line 842
    :cond_63
    invoke-virtual/range {p0 .. p0}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v4

    const-string v13, "_id"

    const-string v14, "file_id"

    const-string v15, "font_ttc_index"

    const-string v16, "font_variation_settings"

    const-string v17, "font_weight"

    const-string v18, "font_italic"

    const-string v19, "result_code"
```



```
    .line 207
    throw p0

    :catch_8
    :cond_8
    :goto_8
    return-void
.end method

.method public static exists(Landroid/content/Context;Landroid/net/Uri;)Z
    .registers 9

    .line 141
    invoke-virtual {p0}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v0

    const/4 p0, 0x0

    const/4 v6, 0x0

    :try_start_6
    const-string v1, "document_id"

    .line 145
    filled-new-array {v1}, [Ljava/lang/String;

    move-result-object v2

    const/4 v3, 0x0

```



```
.end method

.method private static zzc(Landroid/content/Context;Ljava/lang/String;Z)I
    .registers 11
    .annotation system Ldalvik/annotation/Throws;
        value = {
            Lcom/google/android/gms/dynamite/DynamiteModule$LoadingException;
        }
    .end annotation

    const/4 v0, 0x0

    .line 118
    :try_start_1
    invoke-virtual {p0}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v1

    if-eqz p2, :cond_a

    const-string p0, "api_force_staging"

    goto :goto_c

    :cond_a
    const-string p0, "api"

    .line 121
    :goto_c
    invoke-virtual {p0}, Ljava/lang/String;->length()I

    move-result p2
```



```
    invoke-static {v0, v1}, Landroidx/documentfile/provider/DocumentsContractApi19;->length(Landroid/content/Context;Landroid/net/Uri;)J

    move-result-wide v0

    return-wide v0
.end method

.method public listFiles()[Landroidx/documentfile/provider/DocumentFile;
    .registers 10

    .line 136
    iget-object v0, p0, Landroidx/documentfile/provider/TreeDocumentFile;->mContext:Landroid/content/Context;

    invoke-virtual {v0}, Landroid/content/Context;->getContentResolver()Landroid/content/ContentResolver;

    move-result-object v1

    .line 137
    iget-object v0, p0, Landroidx/documentfile/provider/TreeDocumentFile;->mUri:Landroid/net/Uri;

    .line 138
    invoke-static {v0}, Landroid/provider/DocumentsContract;->getDocumentId(Landroid/net/Uri;)Ljava/lang/String;

    move-result-object v2

    .line 137
    invoke-static {v0, v2}, Landroid/provider/DocumentsContract;->buildChildDocumentsUriUsingTree(Landroid/net/Uri;Ljava/lang/String;)Landroid/net/Uri;

    move-result-object v2

    .line 139
```

INFORMATION GATHERING

SIGNER CERTIFICATE

```
APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=IN, ST=Maharastra, L=Nagpur, O=playsatta, OU=s/w, CN=ajay bagdi
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-12-11 09:54:25+00:00
Valid To: 2044-12-04 09:54:25+00:00
Issuer: C=IN, ST=Maharastra, L=Nagpur, O=playsatta, OU=s/w, CN=ajay bagdi
Serial Number: 0x4c925f8f
Hash Algorithm: sha256
```

```
md5: ae8b5ec62f353d52941d99cd70d0b4e1
sha1: ff6bda8ff0dcd376abf145f1098d1697a95f2aa4
sha256: 92c8f7b5d0772a2101fd35097b43c751044e23f06e1e8effc349521f45527ffe
sha512:
fe16d313076aa1191b00c07297fbdcfd20e825cabd8d152c5cbd900f319d642393647ac36f658eb
5a98528ae70716841f73a89a5c10410c45b92d0c25a46822e
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8eb91df7b271684820a0c52029d3e3b15eb1848cb12d4cabc6b924b06cc990c9
```

Activity:-->

com.idreams.project.onlinesatta.MyProfileActivity
com.idreams.project.onlinesatta.ActivityBankDetails
com.idreams.project.onlinesatta.ActivityWacGameProviderList
com.idreams.project.onlinesatta.ActivityWacGameList
com.idreams.project.onlinesatta.ActivitySsgGameList
com.idreams.project.onlinesatta.ActivityWacGameWebView
com.idreams.project.onlinesatta.OurUpiActivity
com.idreams.project.onlinesatta.SUpiGatewayActivity
com.idreams.project.onlinesatta.ActivityLiveChat
com.idreams.project.onlinesatta.ActivityFeedback
com.idreams.project.onlinesatta.ActivityXMLParser
com.idreams.project.onlinesatta.ActivityRemoveWallet
com.idreams.project.onlinesatta.PaymentDepositOptions
com.idreams.project.onlinesatta.ActivityWallet
com.idreams.project.onlinesatta.ActivityWinnerOfTheDay
com.idreams.project.onlinesatta.ActivityNoticeBoard
com.idreams.project.onlinesatta.ActivityDashboard
com.idreams.project.onlinesatta.ActivityChoicePanna
com.idreams.project.onlinesatta.ActivityDPMotor
com.idreams.project.onlinesatta.ActivitySPMotor
com.idreams.project.onlinesatta.ActivityDigitBasedJodi
com.idreams.project.onlinesatta.ActivityRedBracket
com.idreams.project.onlinesatta.ActivityGameHistory
com.idreams.project.onlinesatta.ActivityWebView
com.idreams.project.onlinesatta.ui.PaymentUiActivity
com.idreams.project.onlinesatta.ActivityGame1
com.idreams.project.onlinesatta.ActivityStarLineResults
com.idreams.project.onlinesatta.ActivityStarLineGame
com.idreams.project.onlinesatta.ActivityStarLineBazarList
com.idreams.project.onlinesatta.ActivityStarLineReports
com.idreams.project.onlinesatta.ActivityKingGameFirstDigit

```
com.idreams.project.onlinesatta.ActivityKingGameSecondDigit
com.idreams.project.onlinesatta.ActivityKingGameJodi
com.idreams.project.onlinesatta.ActivityStarLineGameSingleDigit
com.idreams.project.onlinesatta.ActivityStarLineGameSinglePatti
com.idreams.project.onlinesatta.ActivityStarLineGameTriplePatti
com.idreams.project.onlinesatta.ActivityKingBazarList
com.idreams.project.onlinesatta.ActivityKingGame
com.idreams.project.onlinesatta.ActivityKingGameSangam
com.idreams.project.onlinesatta.ActivityKingGameReports
com.idreams.project.onlinesatta.SplashScreen
com.idreams.project.onlinesatta.Sign_in
com.idreams.project.onlinesatta.Sign_Up
com.idreams.project.onlinesatta.MainActivity
com.idreams.project.onlinesatta.GuestLog
com.idreams.project.onlinesatta.DashBoard
com.idreams.project.onlinesatta.PlayGames
com.idreams.project.onlinesatta.GameAppC
com.idreams.project.onlinesatta.JodiGamesEX
com.idreams.project.onlinesatta.SangamGame
com.idreams.project.onlinesatta.TriplePattiGame
com.idreams.project.onlinesatta.ReportsFragment
com.idreams.project.onlinesatta.PayrollFragment
com.idreams.project.onlinesatta.DepositMoney
com.idreams.project.onlinesatta.PaymentWithdrawOption
com.idreams.project.onlinesatta.WalletsReport
com.idreams.project.onlinesatta.PaymentApcoDeposit
com.idreams.project.onlinesatta.PaymentApcoRedirectUrl
com.idreams.project.onlinesatta.PaymentRupeeDeposit
com.idreams.project.onlinesatta.PaymentRupeeRedirectUrl
com.idreams.project.onlinesatta.PaymentRupeeWithDraw
com.idreams.project.onlinesatta.PaymentYarDeposit
com.idreams.project.onlinesatta.PaymentYarRedirectUrl
com.idreams.project.onlinesatta.MoreFragment
com.idreams.project.onlinesatta.HowToPlay
com.idreams.project.onlinesatta.MyProfile
com.idreams.project.onlinesatta.MyMonthlyReports
com.idreams.project.onlinesatta.ContactUs
com.idreams.project.onlinesatta.DailyBhav
com.idreams.project.onlinesatta.Results
com.idreams.project.onlinesatta.JodiCharts
```

com.idreams.project.onlinesatta.PanelCharts
com.idreams.project.onlinesatta.SinglePattiGamesEX
com.idreams.project.onlinesatta.ResetPassword
com.idreams.project.onlinesatta.ForgetPassword
com.idreams.project.onlinesatta.OtpVerification
com.idreams.project.onlinesatta.OtpVerfications
com.idreams.project.onlinesatta.paymero.LiveResultActivity
com.idreams.project.onlinesatta.paymero.PaymeroGatewayActivity
com.idreams.project.onlinesatta.paymero.PaymeroWalletActivity
com.idreams.project.onlinesatta.paymero.PaymeroWalletSelectionActivity
com.idreams.project.onlinesatta.paymero.PaymeroUserDetailsActivity
com.idreams.project.onlinesatta.paymero.PaymeroUPIFormActivity
com.idreams.project.onlinesatta.paymero.PaymeroUPIActivity
com.idreams.project.onlinesatta.paymero.PaymeroBankSelectionActivity
com.idreams.project.onlinesatta.paymero.PaymeroNetBankingActivity
dev.shreyaspatil.easyupipayment.ui.PaymentUiActivity
com.razorpay.CheckoutActivity
com.cashfree.pg.ui.web_checkout.CFPaymentActivity
com.cashfree.pg.ui.upi.CFUPIPaymentActivity
com.cashfree.pg.ui.amazonpay.AmazonPayActivity
com.cashfree.pg.ui.gpay.GooglePayActivity
com.cashfree.pg.ui.phonepe.CFPhonePayActivity
com.google.android.gms.common.api.GoogleApiActivity

Services:-->

com.idreams.project.onlinesatta.FireBaseMessagingService
com.idreams.project.onlinesatta.FirebaseInstantId
com.idreams.project.onlinesatta.SessionService
com.google.firebase.messaging.FirebaseMessagingService
com.google.firebase.components.ComponentDiscoveryService
com.google.android.gms.measurement.AppMeasurementService
com.google.android.gms.measurement.AppMeasurementJobService
com.google.firebase.iid.FirebaseInstanceIdService
com.google.android.datatransport.runtime.backends.TransportBackendDiscovery
com.google.android.datatransport.runtime.scheduling.jobscheduling.JobInfoSchedulerService

Recevers:-->

com.razorpay.RzpTokenReceiver
com.google.android.gms.measurement.AppMeasurementReceiver

com.google.firebase.iid.FirebaseInstanceIdReceiver
com.google.android.datatransport.runtime.scheduling.jobscheduling.AlarmManagerSchedulerBroadcastReceiver

Emails Collected :
android.studio@android.com
photopecker@gmail.com

Telephony Identifiers Leakage
This application reads the MCC+MNC of the provider of the SIM
This application reads the SIM's serial number
This application reads the numeric name (MCC+MNC) of current registered operator
This application reads the operator name
This application reads the radio technology (network type) currently in use on the device for data transmission

Telephony Services Abuse
This application makes phone calls

Code Execution
This application executes a UNIX command

Permissions

```
Asked: ['android.permission.ACCESS_NETWORK_STATE',
'android.permission.INTERNET',
'android.permission.READ_EXTERNAL_STORAGE',
'android.permission.REQUEST_INSTALL_PACKAGES',
'android.permission.WAKE_LOCK',
'android.permission.WRITE_EXTERNAL_STORAGE',
'com.google.android.c2dm.permission.RECEIVE',
'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE']
Implied: []
Declared: []
```

apk leakes:-->

```
===================
[Google_API_Key]
- AIzaSyDFAO0clBOSZWrXuDDhc_6LeON1A2lRum4

[Google_Cloud_Platform_OAuth]
```

```
- 320227347610-fhdc0opdpf89n1prhlmirtehc2o2flm7.apps.googleusercontent.com

[IP_Address]
- 0.0.0.0
- 192.168.19.1

[LinkFinder]
- /...
- /10000000
- /OS1/OnlineSatta.apk
- /cancel?
- /cancel?platform=android_sdk
- /cmdline
- /index.html
- /index.php/api/yaar-pay-return
- /metadata
- /proc/
- /proc/meminfo
- /proc/self/fd/
- /proceed\
- /status?
- /system/app/Superuser.apk
- /system/xbin/su
- /system/xbin/which
- /topics/
- /v1/checkout
- AES/CBC/PKCS5Padding
- Asia/Calcutta
- activity_choser_model_history.xml
- amazonpayment/checkstatus
- config/app/
- content://com.google.android.gms.phenotype/
- content://com.google.android.gsf.gservices
- content://com.google.android.gsf.gservices/prefix
- data.xml
- http://playsatta.co/index.php/site/chartmain
- http://playsatta.co/index.php/site/domain-links
- http://playsatta.co/index.php/site/live-support-chart
- http://sattaresults.co/web/site/chartj
- http://sattaresults.co/web/site/chartp
- http://schemas.android.com/apk/res-auto
- http://schemas.android.com/apk/res/android
- http://www.youtube.com/watch?v=potzQ8jq8nY
- http://xmlpull.org/v1/doc/features.html#process-namespaces
- https://api.androidhive.info/pizza/?format=xml
- https://api.razorpay.com
- https://api.razorpay.com/v1/checkout/public
- https://api.razorpay.com/v1/payments/
- https://api.whatsapp.com/send?phone=
- https://api.whatsapp.com/send?phone=+
- https://app-measurement.com/a
- https://butler.razorpay.com/v1/settings
- https://cdn.razorpay.com/static/magic/
- https://cdn.razorpay.com/static/otpelf/
- https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings
```

- https://google.com
- https://lumberjack.razorpay.com/v1/track
- https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps
- https://payments.cashfree.com/
- https://plus.google.com/
- https://reports.crashlytics.com/sdk-api/v1/platforms/android/apps/%s/minidumps
- https://reports.crashlytics.com/spi/v1/platforms/android/apps/%s/reports
- https://test.cashfree.com/
- https://update.crashlytics.com/spi/v1/platforms/android/apps
- https://update.crashlytics.com/spi/v1/platforms/android/apps/%s
- https://www.cashfree.com/
- https://www.dpbossonline.com//OnlineSatta.apk
- https://www.facebook.com
- https://www.facebook.com/arkverse
- https://www.google.com
- https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s
- https://www.googleapis.com/auth/appstate
- https://www.googleapis.com/auth/datastoremobile
- https://www.googleapis.com/auth/drive
- https://www.googleapis.com/auth/drive.appdata
- https://www.googleapis.com/auth/drive.apps
- https://www.googleapis.com/auth/drive.file
- https://www.googleapis.com/auth/fitness.activity.read
- https://www.googleapis.com/auth/fitness.activity.write
- https://www.googleapis.com/auth/fitness.blood_glucose.read
- https://www.googleapis.com/auth/fitness.blood_glucose.write
- https://www.googleapis.com/auth/fitness.blood_pressure.read
- https://www.googleapis.com/auth/fitness.blood_pressure.write
- https://www.googleapis.com/auth/fitness.body.read
- https://www.googleapis.com/auth/fitness.body.write
- https://www.googleapis.com/auth/fitness.body_temperature.read
- https://www.googleapis.com/auth/fitness.body_temperature.write
- https://www.googleapis.com/auth/fitness.location.read
- https://www.googleapis.com/auth/fitness.location.write
- https://www.googleapis.com/auth/fitness.nutrition.read
- https://www.googleapis.com/auth/fitness.nutrition.write
- https://www.googleapis.com/auth/fitness.oxygen_saturation.read
- https://www.googleapis.com/auth/fitness.oxygen_saturation.write
- https://www.googleapis.com/auth/fitness.reproductive_health.read
- https://www.googleapis.com/auth/fitness.reproductive_health.write
- https://www.googleapis.com/auth/games
- https://www.googleapis.com/auth/games.firstparty
- https://www.googleapis.com/auth/games_lite
- https://www.googleapis.com/auth/plus.login
- https://www.googleapis.com/auth/plus.me
- https://www.satta.us/
- https://www.satta.us/index.php/api/yaarpay-deposit?amount=
- https://youtu.be/potzQ8jq8nY
- magic.js
- otpelf.js
- overrides.txt
- phonepepayment/checkstatus
- share_history.xml

- upi/checkStatusPayRequest
- upi/droppedUserStatus
- version.json

TOOL’S :

- MOBSF(Mobile Security Framework)
- ImmuniWeb
- QuickXXI
- Qark(Quick Android Review Kit)
- AndroBugs Framework
- AndroWarn
- APKLeaks
- RMS(Run-Time Mobile Security)