ImmuniWeb®
Community Edition

Summary of Mobile Application Security Test

Provided "as is" without any warranty of any kind.

This application was tested 2 times during the last 12 months.

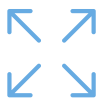|	
App version	1.0.0
App ID	com.example.slt_field_app
Device type	android
Test started	Aug 1st, 2024 04:12:57 GMT+0
Test finished	Aug 1st, 2024 04:14:16 GMT+0
Test runtime	1 minute
APK source	User upload

Mobile App Permissions and Privacy	OWASP Mobile Top 10 Security Test	Mobile App External Communications	Software Composition Analysis
8 PERMISSIONS	**1 MAJOR RISK FOUND**	**NOT FOUND**	**4 COMPONENTS FOUND**

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

Meet Regulatory and Compliance Requirements

Looking for a comprehensive security audit and compliance-ready report? You are at the right place.

Mobile Security Scanning	Mobile Penetration Testing	Cybersecurity Compliance

Trusted by 1,000+ customers from over 50 countries

50+ international awards and industry recognitions

FREE DEMO

Because prevention is better

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

Mobile Application Permissions and Privacy Test

Privacy Policy

Privacy Policy was not found in application	Misconfiguration or weakness

Mobile Application Permissions

The mobile application requests the following permissions that may endanger user's privacy under certain circumstances:

ACCESS_BACKGROUND_LOCATION	dangerous

Allows an app to access location in the background.

ACCESS_COARSE_LOCATION	dangerous

Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.

ACCESS_FINE_LOCATION	dangerous

Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

CAMERA	dangerous

Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.

ACCESS_NETWORK_STATE	normal

Allows an application to view the status of all networks.

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

FLASHLIGHT	normal

Allows the application to control the flashlight.

FOREGROUND_SERVICE	normal

Allows a regular application to use Service.startForeground.

INTERNET	normal

Allows an application to create network sockets.

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

OWASP Mobile Top 10 Security Test

The automated audit revealed the following security flaws and weaknesses that may impact the application:

0	**1**	**0**	**3**	**7**
CRITICAL RISK	HIGH RISK	MEDIUM RISK	LOW RISK	WARNING

EXTERNAL DATA IN SQL QUERIES   [M7] [CWE-89]   HIGH

Description:

Inclusion of input into raw SQL queries can potentially lead to a local SQL injection vulnerability in the mobile application, resuting in the compromise of any sensitive information stored within databse files.
The correct approach is to use prepared SQL statements beyond user's control.

Example of secure code:

```
PreparedStatement pstmt = con.prepareStatement("UPDATE EMPLOYEES SET SALARY = ?
WHERE ID = ?");
            pstmt.setBigDecimal(1, 153833.00)
            pstmt.setInt(2, 110592)
```

Example of insecure code:

```
db.rawQuery("SELECT username FROM users_table WHERE id = '"+ input_id +"'");
            db.execSQL("SELECT username FROM users_table WHERE id = '"+
input_id +"'");
```

There is **'execSQL()'** found in file 'q2/i.java':

```
[line 589:          try {]
[line 590:              C().execSQL(d5.c(), d5.d());]
[line 591:              u(f5);]
```

CVSSv3 Base Score:

7.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L)

Reference:

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

- https://developer.android.com/reference/android/database/sqlite/SQLiteDatabase.html
- https://developer.android.com/reference/java/sql/PreparedStatement.html

HARDCODED DATA   [M2] [CWE-200]   LOW

Description:

The mobile application contains debugging or potentially sensitive hardcoded data. An attacker with an access to the mobile application can easily extract this data from the application and use it in any further attacks.

https:// with value https://plus.google.com/ in following files:

- y0/k1.java:

```
[line 12: Uri parse = Uri.parse("https://plus.google.com/");]
```

CVSSv3 Base Score:

3.3 (AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N)

MISSING TAPJACKING PROTECTION   [M1] [CWE-451]   LOW

Description:

By default on Android 6.0 and lower, Android allows applications to overlaydraw over some portions of the phone screen and permits touch events to be sent to underlying activities. This can be used by an attacker to trick application users into performing some sensitive actions in a legitimate application (e.g. send a payment) that they do not otherwise intend doing.

Example of secure code:

```
public class MyActivity extends Activity {
                protected void onCreate(Bundle bundle) {
                    super.onCreate(bundle);

                    final Button myButton =
(Button)findViewById(R.id.button_id);
                    myButton.setFilterTouchesWhenObscured(true);

                    myButton.setOnClickListener(new View.OnClickListener() {
                        // Perform action on click
                    }
                }
            }

            <Button
```

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
                                android:layout_height="wrap_content"
                                android:layout_width="wrap_content"
                                android:text="@string/self_destruct"
                                android:onClick="selfDestruct"
                                android:filterTouchesWhenObscured="true" />
```

There is **android:filterTouchesWhenObscured="true"** missing in files:

- android/res/layout-land/material_clock_period_toggle_land.xml

- android/res/layout-land/material_timepicker.xml

- android/res/layout-land/mtrl_picker_header_dialog.xml

- android/res/layout-ldrtl/material_textinput_timepicker.xml

- android/res/layout-sw600dp/design_layout_snackbar.xml

- android/res/layout-sw600dp/mtrl_layout_snackbar.xml

- android/res/layout-v22/abc_alert_dialog_button_bar_material.xml

- android/res/layout-v22/material_timepicker_dialog.xml

- android/res/layout-v22/mtrl_alert_dialog_actions.xml

- android/res/layout-v26/abc_screen_toolbar.xml

- android/res/layout-v26/mtrl_calendar_month.xml

- android/res/layout-watch/abc_alert_dialog_button_bar_material.xml

- android/res/layout-watch/abc_alert_dialog_title_material.xml

- android/res/layout/abc_action_bar_title_item.xml

- android/res/layout/abc_action_bar_up_container.xml

- android/res/layout/abc_action_menu_item_layout.xml

- android/res/layout/abc_action_menu_layout.xml

- android/res/layout/abc_action_mode_bar.xml

- android/res/layout/abc_action_mode_close_item_material.xml

- android/res/layout/abc_activity_chooser_view.xml

- android/res/layout/abc_activity_chooser_view_list_item.xml

- android/res/layout/abc_alert_dialog_button_bar_material.xml

- android/res/layout/abc_alert_dialog_material.xml

- android/res/layout/abc_alert_dialog_title_material.xml

- android/res/layout/abc_cascading_menu_item_layout.xml

- android/res/layout/abc_dialog_title_material.xml

- android/res/layout/abc_expanded_menu_layout.xml

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

- android/res/layout/abc_list_menu_item_checkbox.xml
- android/res/layout/abc_list_menu_item_icon.xml
- android/res/layout/abc_list_menu_item_layout.xml
- android/res/layout/abc_list_menu_item_radio.xml
- android/res/layout/abc_popup_menu_header_item_layout.xml
- android/res/layout/abc_popup_menu_item_layout.xml
- android/res/layout/abc_screen_content_include.xml
- android/res/layout/abc_screen_simple.xml
- android/res/layout/abc_screen_simple_overlay_action_mode.xml
- android/res/layout/abc_screen_toolbar.xml
- android/res/layout/abc_search_dropdown_item_icons_2line.xml
- android/res/layout/abc_search_view.xml
- android/res/layout/abc_select_dialog_material.xml
- android/res/layout/abc_tooltip.xml
- android/res/layout/barcode_capture.xml
- android/res/layout/custom_dialog.xml
- android/res/layout/design_bottom_navigation_item.xml
- android/res/layout/design_bottom_sheet_dialog.xml
- android/res/layout/design_layout_snackbar.xml
- android/res/layout/design_layout_snackbar_include.xml
- android/res/layout/design_layout_tab_icon.xml
- android/res/layout/design_layout_tab_text.xml
- android/res/layout/design_menu_item_action_area.xml
- android/res/layout/design_navigation_item.xml
- android/res/layout/design_navigation_item_header.xml
- android/res/layout/design_navigation_item_separator.xml
- android/res/layout/design_navigation_item_subheader.xml
- android/res/layout/design_navigation_menu.xml
- android/res/layout/design_navigation_menu_item.xml
- android/res/layout/design_text_input_end_icon.xml
- android/res/layout/design_text_input_start_icon.xml
- android/res/layout/material_chip_input_combo.xml
- android/res/layout/material_clock_display.xml

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

- android/res/layout/material_clock_display_divider.xml
- android/res/layout/material_clock_period_toggle.xml
- android/res/layout/material_clockface_textview.xml
- android/res/layout/material_clockface_view.xml
- android/res/layout/material_radial_view_group.xml
- android/res/layout/material_textinput_timepicker.xml
- android/res/layout/material_time_chip.xml
- android/res/layout/material_time_input.xml
- android/res/layout/material_timepicker.xml
- android/res/layout/material_timepicker_dialog.xml
- android/res/layout/material_timepicker_textinput_display.xml
- android/res/layout/mtrl_alert_dialog.xml
- android/res/layout/mtrl_alert_dialog_actions.xml
- android/res/layout/mtrl_alert_dialog_title.xml
- android/res/layout/mtrl_alert_select_dialog_item.xml
- android/res/layout/mtrl_alert_select_dialog_multichoice.xml
- android/res/layout/mtrl_alert_select_dialog_singlechoice.xml
- android/res/layout/mtrl_calendar_day.xml
- android/res/layout/mtrl_calendar_day_of_week.xml
- android/res/layout/mtrl_calendar_days_of_week.xml
- android/res/layout/mtrl_calendar_horizontal.xml
- android/res/layout/mtrl_calendar_month.xml
- android/res/layout/mtrl_calendar_month_labeled.xml
- android/res/layout/mtrl_calendar_month_navigation.xml
- android/res/layout/mtrl_calendar_months.xml
- android/res/layout/mtrl_calendar_vertical.xml
- android/res/layout/mtrl_calendar_year.xml
- android/res/layout/mtrl_layout_snackbar.xml
- android/res/layout/mtrl_layout_snackbar_include.xml
- android/res/layout/mtrl_picker_actions.xml
- android/res/layout/mtrl_picker_dialog.xml
- android/res/layout/mtrl_picker_fullscreen.xml
- android/res/layout/mtrl_picker_header_dialog.xml

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

- android/res/layout/mtrl_picker_header_fullscreen.xml
- android/res/layout/mtrl_picker_header_selection_text.xml
- android/res/layout/mtrl_picker_header_title_text.xml
- android/res/layout/mtrl_picker_header_toggle.xml
- android/res/layout/mtrl_picker_text_input_date.xml
- android/res/layout/mtrl_picker_text_input_date_range.xml
- android/res/layout/notification_action.xml
- android/res/layout/notification_action_tombstone.xml
- android/res/layout/notification_media_action.xml
- android/res/layout/notification_media_cancel_action.xml
- android/res/layout/notification_template_big_media.xml
- android/res/layout/notification_template_big_media_custom.xml
- android/res/layout/notification_template_big_media_narrow.xml
- android/res/layout/notification_template_big_media_narrow_custom.xml
- android/res/layout/notification_template_custom_big.xml
- android/res/layout/notification_template_icon_group.xml
- android/res/layout/notification_template_lines_media.xml
- android/res/layout/notification_template_media.xml
- android/res/layout/notification_template_media_custom.xml
- android/res/layout/notification_template_part_chronometer.xml
- android/res/layout/notification_template_part_time.xml
- android/res/layout/select_dialog_item_material.xml
- android/res/layout/select_dialog_multichoice_material.xml
- android/res/layout/select_dialog_singlechoice_material.xml
- android/res/layout/support_simple_spinner_dropdown_item.xml
- android/res/layout/test_action_chip.xml
- android/res/layout/test_chip_zero_corner_radius.xml
- android/res/layout/test_design_checkbox.xml
- android/res/layout/test_design_radiobutton.xml
- android/res/layout/test_reflow_chipgroup.xml
- android/res/layout/test_toolbar.xml
- android/res/layout/test_toolbar_custom_background.xml
- android/res/layout/test_toolbar_elevation.xml

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

- android/res/layout/test_toolbar_surface.xml

- android/res/layout/text_view_with_line_height_from_appearance.xml

- android/res/layout/text_view_with_line_height_from_layout.xml

- android/res/layout/text_view_with_line_height_from_style.xml

- android/res/layout/text_view_with_theme_line_height.xml

- android/res/layout/text_view_without_line_height.xml

- android/res/layout/toast_custom.xml

Details:

There is 'extends FrameLayout' found in file 'a2/b.java':

```
[line 8: /* loaded from: classes.dex */]
[line 9: public class b extends FrameLayout implements d {]
[line 10:     @Override // a2.d]
```

There is 'extends FrameLayout' found in file 'i/c.java':

```
[line 100:      /* loaded from: classes.dex */]
[line 101:      static class C0071c extends FrameLayout implements h.c {]
[line 102:]
```

There is 'extends FrameLayout' found in file 'io/flutter/embedding/android/q.java':

```
[line 47: /* loaded from: classes.dex */]
[line 48: public class q extends FrameLayout implements b.c, y.e {]
[line 49:     private final androidx.core.util.a<WindowLayoutInfo> A;]
```

There is 'extends FrameLayout' found in file 'io/flutter/plugin/platform/o.java':

```
[line 20: /* loaded from: classes.dex */]
[line 21: public class o extends FrameLayout {]
[line 22:]
```

There is 'extends FrameLayout' found in file 'l/a.java':

```
[line 7: /* loaded from: classes.dex */]
[line 8: public class a extends FrameLayout {]
[line 9:]
```

There is 'extends FrameLayout' found in file 'z2/a.java':

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
[line 17: /* loaded from: classes.dex */]
[line 18: public class a extends FrameLayout {]
[line 19:]
```

Details:

There is 'extends SurfaceView' found in file 'io/flutter/embedding/android/j.java':

```
[line 9: /* loaded from: classes.dex */]
[line 10: public class j extends SurfaceView implements
io.flutter.embedding.engine.renderer.b {]
[line 11:]
```

Details:

There is 'extends TextureView' found in file 'io/flutter/embedding/android/k.java':

```
[line 10: /* loaded from: classes.dex */]
[line 11: public class k extends TextureView implements b {]
[line 12:]
```

Details:

There is 'extends View' found in file 'com/amolg/flutterbarcodescanner/camera/GraphicOverlay.java':

```
[line 19: /* loaded from: classes.dex */]
[line 20: public class GraphicOverlay<T extends a> extends View {]
[line 21:]
```

There is 'extends View' found in file 'io/flutter/embedding/android/i.java':

```
[line 20: /* loaded from: classes.dex */]
[line 21: public class i extends View implements
io.flutter.embedding.engine.renderer.b {]
[line 22:]
```

Details:

There is 'extends ViewGroup' found in file
'com/amolg/flutterbarcodescanner/camera/CameraSourcePreview.java':

```
[line 10: /* loaded from: classes.dex */]
[line 11: public class CameraSourcePreview extends ViewGroup {]
```

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
[line 12:]
```

There is 'extends ViewGroup' found in file 'io/flutter/plugin/platform/SingleViewPresentation.java':

```
[line 61:      /* loaded from: classes.dex */]
[line 62:      public static class b extends ViewGroup {]
[line 63:]
```

CVSSv3 Base Score:

3.3 (AV:L/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N)

Reference:

- https://developer.android.com/guide/topics/ui/declaring-layout.html

- https://developer.android.com/guide/topics/resources/layout-resource.html

- https://blog.lookout.com/blog/2010/12/09/android-touch-event-hijacking/

EXPORTED ACTIVITIES   [M1] [CWE-926]   LOW

Description:

The mobile application contains exported activities that can be invoked by other applications residing on the mobile device, including malicious ones, to trigger a legitimate application activity in order to perform potentially sensitive actions.

Example of secure code:

```
<activity
                android:name=".SomeActivity"
                ....
                android:exported="false" />
```

Example of insecure code:

```
<activity
                android:name=".SomeActivity"
                ....
                android:exported="true" />
```

There is '**MainActivity**' found in file 'android/AndroidManifest.xml':

```
[line 40:          <activity
android:configChanges="density|fontScale|keyboard|keyboardHidden|layoutDirection
|locale|orientation|screenLayout|screenSize|smallestScreenSize|uiMode"
android:exported="true" android:hardwareAccelerated="true"
android:launchMode="singleTop"
android:name="com.example.slt_field_app.MainActivity"
android:theme="@style/LaunchTheme" android:windowSoftInputMode="adjustResize">]
```

CVSSv3 Base Score:

3.6 (AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N)

Reference:

- https://developer.android.com/reference/android/app/Activity.html
- https://developer.android.com/guide/topics/manifest/activity-element.html

ACTIVITY MISSING SECURE FLAG   WARNING

Description:

An Activity is missing the secure flag LayoutParams.FLAG_SECURE. As a result, any sensitive information on the screen will be saved in screenshots which can then be viewed by a malicious application on the same device, or by an attacker with physical access

There is **'setContentView('** found in file 'com/amolg/flutterbarcodescanner/BarcodeCaptureActivity.java':

```
[line 290:          try {]
[line 291:          setContentView(f.a_res_0x7f0b001c);]
[line 292:          try {]
```

There is **'setContentView('** found in file 'd/b.java':

```
[line 265:      @Override // android.app.Activity]
[line 266:      public void setContentView(int i5) {]
[line 267:         y().A(i5);]
```

```
[line 270:      @Override // android.app.Activity]
[line 271:      public void setContentView(View view) {]
[line 272:         y().B(view);]
```

```
[line 275:      @Override // android.app.Activity]
[line 276:      public void setContentView(View view, ViewGroup.LayoutParams
```

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
layoutParams) {]
[line 277:          y().C(view, layoutParams);]
```

There is **'setContentView('** found in file 'd/f.java':

```
[line 1305:                 }]
[line 1306:                 this.f5206j.setContentView(viewGroup);]
[line 1307:                 contentFrameLayout.setAttachListener(new c());]
```

There is **'setContentView('** found in file 'd/i.java':

```
[line 116:     @Override // android.app.Dialog]
[line 117:     public void setContentView(int i5) {]
[line 118:         a().A(i5);]
```

```
[line 121:     @Override // android.app.Dialog]
[line 122:     public void setContentView(View view) {]
[line 123:         a().B(view);]
```

```
[line 126:     @Override // android.app.Dialog]
[line 127:     public void setContentView(View view, ViewGroup.LayoutParams
layoutParams) {]
[line 128:         a().C(view, layoutParams);]
```

There is **'setContentView('** found in file 'io/flutter/embedding/android/c.java':

```
[line 292:     G();]
[line 293:     setContentView(H());]
[line 294:     F();]
```

There is **'setContentView('** found in file 'io/flutter/plugin/platform/SingleViewPresentation.java':

```
[line 363:          }]
[line 364:          setContentView(this.rootView);]
[line 365:      }]
```

OBJECT DESERIALIZATION FOUND   [M7] [CWE-502]   WARNING

Description:

Object deserialization performed on an untrusted resource (e.g. user-supplied input or external storage), can be dangerous if the data for deserialization is tampered with by an attacker.

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

Example of secure code:

```
// Use only serialization when you have the control over data
```

Example of insecure code:

```
bundle.putSerializable("exampleClass", exampleOfSerializabledClass);
            exampleOfSerializabledClass =
bundle.getSerializable("exampleClass");
```

There is **'getSerializableExtra()'** found in file 'io/flutter/embedding/android/c.java':

```
[line 249:       public List<String> l() {]
[line 250:          return (List)
getIntent().getSerializableExtra("dart_entrypoint_args");]
[line 251:       }]
```

There is **'implements Serializable'** found in file 'a4/c.java':

```
[line 15:      /* loaded from: classes.dex */]
[line 16:      public static final class a extends c implements Serializable {]
[line 17:          private a() {]
```

There is **'implements Serializable'** found in file 'android/icu/util/TimeZone.java':

```
[line 4: /* loaded from: classes.dex */]
[line 5: public /* synthetic */ class TimeZone implements Serializable,
Cloneable, Freezable {]
[line 6:      static {]
```

There is **'implements Serializable'** found in file 'kotlin/jvm/internal/a.java':

```
[line 22:      /* loaded from: classes.dex */]
[line 23:      private static class C0089a implements Serializable {]
[line 24:]
```

There is **'implements Serializable'** found in file 'm1/p0.java':

```
[line 9: /* loaded from: classes.dex */]
[line 10: public abstract class p0 extends AbstractCollection implements
```

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
Serializable {]
[line 11:]
```

There is **'implements Serializable'** found in file 'q3/j.java':

```
[line 5: /* loaded from: classes.dex */]
[line 6: public final class j<A, B> implements Serializable {]
[line 7:]
```

There is **'implements Serializable'** found in file 'q3/k.java':

```
[line 6: /* loaded from: classes.dex */]
[line 7: public final class k<T> implements Serializable {]
[line 8:]
```

```
[line 22:      /* loaded from: classes.dex */]
[line 23:      public static final class b implements Serializable {]
[line 24:]
```

Reference:

- https://developer.android.com/reference/android/os/Bundle.html

DYNAMIC LOAD OF CODE   [M7] [CWE-94]   WARNING

Description:

The mobile application uses dynamic load of executable code. Under certain circumstances, dynamic load of code can be dangerous. For example, if the code is located on an external storage (e.g. SD card), this can lead to code injection vulnerability if the external storage is world readable and/or writable and an attacker can access it.

Example of secure code:

```
// If you are using code from unsafe place (like external storage),
        // you should sign and cryptographically verify your code.
```

Example of insecure code:

```
Object test = loader.loadClass("Test", true).newInstance();
```

There is **'ClassLoader'** found in file 'android/app/AppComponentFactory.java':

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
[line 14:       @NonNull]
[line 15:      public native /* synthetic */ Activity
instantiateActivity(@NonNull ClassLoader ClassLoader, @NonNull String str,
@Nullable Intent intent) throws ClassNotFoundException, IllegalAccessException,
InstantiationException;]
[line 16: ]
[line 17:       @NonNull]
[line 18:      public native /* synthetic */ Application
instantiateApplication(@NonNull ClassLoader ClassLoader, @NonNull String str)
throws ClassNotFoundException, IllegalAccessException, InstantiationException;]
[line 19: ]
[line 20:       @NonNull]
[line 21:      public native /* synthetic */ ContentProvider
instantiateProvider(@NonNull ClassLoader ClassLoader, @NonNull String str)
throws ClassNotFoundException, IllegalAccessException, InstantiationException;]
[line 22: ]
[line 23:       @NonNull]
[line 24:      public native /* synthetic */ BroadcastReceiver
instantiateReceiver(@NonNull ClassLoader ClassLoader, @NonNull String str,
@Nullable Intent intent) throws ClassNotFoundException, IllegalAccessException,
InstantiationException;]
[line 25: ]
[line 26:       @NonNull]
[line 27:      public native /* synthetic */ Service instantiateService(@NonNull
ClassLoader ClassLoader, @NonNull String str, @Nullable Intent intent) throws
ClassNotFoundException, IllegalAccessException, InstantiationException;]
[line 28: }]
```

There is '**ClassLoader**' found in file 'd/j.java':

```
[line 129:               }]
[line 130:               constructor = Class.forName(str3, false,
context.getClassLoader()).asSubclass(View.class).getConstructor(f5265b);]
[line 131:               gVar.put(str, constructor);]
```

There is '**ClassLoader**' found in file 'e1/b.java':

```
[line 29:                  try {]
[line 30:
context.getClassLoader().loadClass("com.google.android.instantapps.supervisor.In
stantAppsRuntime");]
[line 31:                  f5474b = Boolean.TRUE;]
```

There is '**ClassLoader**' found in file 'g1/b.java':

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
[line 8:      /* renamed from: a  reason: collision with root package name */]
[line 9:      private static volatile ClassLoader f5612a;]
[line 10:]
```

```
[line 13: ]
[line 14:      public static synchronized ClassLoader a() {]
[line 15:          ClassLoader ClassLoader;]
[line 16:          synchronized (b.class) {]
```

```
[line 24: ]
[line 25:      private static synchronized ClassLoader b() {]
[line 26:          synchronized (b.class) {]
[line 27:              ClassLoader ClassLoader = null;]
[line 28:              if (f5613b == null) {]
```

```
[line 35:                  try {]
[line 36:                      classLoader = f5613b.getContextClassLoader();]
[line 37:                  } catch (SecurityException e5) {]
```

```
[line 97:                          try {]
[line 98:                              thread.setContextClassLoader(null);]
[line 99:                              thread.start();]
```

There is 'ClassLoader' found in file 'g4/g0.java':

```
[line 18:          List<CoroutineExceptionHandler> e5;]
[line 19:          a5 = f.a(ServiceLoader.load(CoroutineExceptionHandler.class,
CoroutineExceptionHandler.class.getClassLoader()).iterator());]
[line 20:          e5 = h.e(a5);]
```

There is 'ClassLoader' found in file 'h/g.java':

```
[line 189:             try {]
[line 190:                 Constructor<?> constructor = Class.forName(str,
false, g.this.f5735c.getClassLoader()).getConstructor(clsArr);]
[line 191:                 constructor.setAccessible(true);]
```

There is 'ClassLoader' found in file 'io/flutter/plugin/platform/SingleViewPresentation.java':

```
[line 234:         public WindowManager b() {]
[line 235:             return (WindowManager)
```

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
Proxy.newProxyInstance(WindowManager.class.getClassLoader(), new Class[]
{WindowManager.class}, this);]
[line 236:         }]
```

There is **'ClassLoader'** found in file 'j1/c.java':

```
[line 10:      /* renamed from: a  reason: collision with root package name */]
[line 11:      private static final ClassLoader f6805a =
c.class.getClassLoader();]
[line 12:]
```

There is **'ClassLoader'** found in file 'k1/c.java':

```
[line 10:      /* renamed from: a  reason: collision with root package name */]
[line 11:      private static final ClassLoader f6849a =
c.class.getClassLoader();]
[line 12:]
```

There is **'ClassLoader'** found in file 'kotlin/coroutines/jvm/internal/i.java':

```
[line 41:          try {]
[line 42:          a aVar2 = new a(Class.class.getDeclaredMethod("getModule",
new Class[0]),
aVar.getClass().getClassLoader().loadClass("java.lang.Module").getDeclaredMethod
("getDescriptor", new Class[0]),
aVar.getClass().getClassLoader().loadClass("java.lang.module.ModuleDescriptor").
getDeclaredMethod("name", new Class[0]));]
[line 43:          f6885c = aVar2;]
```

There is **'ClassLoader'** found in file 'l1/c.java':

```
[line 7:     /* renamed from: a  reason: collision with root package name */]
[line 8:     private static final ClassLoader f7046a =
c.class.getClassLoader();]
[line 9:]
```

There is **'ClassLoader'** found in file 'm1/n.java':

```
[line 10:      /* renamed from: a  reason: collision with root package name */]
[line 11:      private static final ClassLoader f7274a =
n.class.getClassLoader();]
[line 12:]
```

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

There is **'ClassLoader'** found in file 'm2/a.java':

```
[line 15:        /* loaded from: classes.dex */]
[line 16:        static class C0092a implements Parcelable.ClassLoaderCreator<a> {]
[line 17:            C0092a() {]
```

```
[line 25:            /* renamed from: b */]
[line 26:            public a createFromParcel(Parcel parcel, ClassLoader
ClassLoader) {]
[line 27:                return new a(parcel, ClassLoader, null);]
```

```
[line 35: ]
[line 36:        private a(Parcel parcel, ClassLoader ClassLoader) {]
[line 37:            super(parcel, ClassLoader);]
```

```
[line 48: ]
[line 49:        /* synthetic */ a(Parcel parcel, ClassLoader ClassLoader, C0092a
aVar) {]
[line 50:            this(parcel, ClassLoader);]
```

There is **'ClassLoader'** found in file 'u3/b.java':

```
[line 23:                    } catch (ClassCastException e5) {]
[line 24:                        ClassLoader classLoader =
newInstance.getClass().getClassLoader();]
[line 25:                        ClassLoader classLoader2 =
a.class.getClassLoader();]
[line 26:                        if (!i.a(classLoader, ClassLoader2)) {]
```

```
[line 42:                    } catch (ClassCastException e6) {]
[line 43:                        ClassLoader classLoader3 =
newInstance3.getClass().getClassLoader();]
[line 44:                        ClassLoader classLoader4 =
a.class.getClassLoader();]
[line 45:                        if (!i.a(classLoader3, ClassLoader4)) {]
```

```
[line 63:                    } catch (ClassCastException e7) {]
[line 64:                        ClassLoader classLoader5 =
newInstance2.getClass().getClassLoader();]
[line 65:                        ClassLoader classLoader6 =
a.class.getClassLoader();]
[line 66:                        if (!i.a(classLoader5, ClassLoader6)) {]
```

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
[line 80:                      } catch (ClassCastException e8) {]
[line 81:                   ClassLoader classLoader7 =
newInstance4.getClass().getClassLoader();]
[line 82:                   ClassLoader classLoader8 =
a.class.getClassLoader();]
[line 83:                   if (!i.a(classLoader7, ClassLoader8)) {]
```

There is **'ClassLoader'** found in file 'y/a.java':

```
[line 23:     /* loaded from: classes.dex */]
[line 24:     static class b implements Parcelable.ClassLoaderCreator<a> {]
[line 25:         b() {]
```

```
[line 33:     /* renamed from: b */]
[line 34:     public a createFromParcel(Parcel parcel, ClassLoader
ClassLoader) {]
[line 35:         if (parcel.readParcelable(ClassLoader) == null) {]
```

```
[line 51:     /* JADX INFO: Access modifiers changed from: protected */]
[line 52:     public a(Parcel parcel, ClassLoader ClassLoader) {]
[line 53:         Parcelable readParcelable =
parcel.readParcelable(ClassLoader);]
```

Reference:

- https://developer.android.com/reference/java/lang/ClassLoader.html

- https://developer.android.com/reference/dalvik/system/DexClassLoader.html

- https://developer.android.com/reference/java/security/SecureClassLoader.html

- https://developer.android.com/reference/java/net/URLClassLoader.html

MISSING ANTI-EMULATION   WARNING

Description:

The mobile application does not use any anti-emulation or anti-debugger techniques (e.g. detecting rooted devices or checking if contacts are authentic).
This can significantly facilitate application debugging and reverse-engineering processes.

Reference:

- https://github.com/strazzere/anti-emulator

NETWORK SECURITY CONFIGURATION IS NOT PRESENT   WARNING

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

Description:

The mobile application does not use Network Security Configuration to define which certificates and Certificate Authorities (CA) can be used for different environments (e.g. Development, Test and Production). The Network Security Configuration on Android feature lets application developers customize their network security settings in a safe, declarative configuration file without modifying the application code.

Reference:

- https://developer.android.com/training/articles/security-config.html

USAGE OF IMPLICIT INTENT   [M1] [CWE-927]   WARNING

Description:

The mobile application uses implicit intent that may be insecure under certain conditions.

Intents enable mobile applications to communicate with each other by requesting to perform different actions for which they are better suited. An implicit intent, however, does not specify to which particular application it sends a request to perform an action. If a malicious application is installed on victim's device, it may also receive the implicit intent, respond to it and perform some action instead, or in addition to, a legitimate application.

Example of secure code:

```
Intent downloadIntent = new Intent(this, DownloadService.class);
```

Example of insecure code:

```
Intent sendIntent = new Intent();
```

There is **'new Intent()'** found in file 'com/amolg/flutterbarcodescanner/BarcodeCaptureActivity.java':

```
[line 185:          }]
[line 186:          Intent intent = new Intent();]
[line 187:          intent.putExtra("Barcode", aVar);]
```

```
[line 241:          }]
[line 242:          Intent intent = new Intent();]
[line 243:          intent.putExtra("Barcode", aVar);]
```

There is **'new Intent()'** found in file 'p0/a.java':

```
[line 9:          try {]
[line 10:             Intent intent = new Intent();]
```

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

```
[line 11:
intent.setAction("android.settings.APPLICATION_DETAILS_SETTINGS");]
```

```
[line 25:          try {]
[line 26:              Intent intent = new Intent();]
[line 27:
intent.setAction("android.settings.LOCATION_SOURCE_SETTINGS");]
```

There is **'new Intent()'** found in file 'v0/g.java':

```
[line 96:          try {]
[line 97:              Intent intent = new Intent();]
[line 98:              ComponentName componentName = this.f8215c;]
```

There is **'new Intent()'** found in file 'y0/d1.java':

```
[line 49:          if (this.f8658a == null) {]
[line 50:              return new Intent().setComponent(this.f8660c);]
[line 51:          }]
```

Reference:

- https://developer.android.com/guide/components/intents-filters.html
- https://developer.android.com/training/articles/security-tips.html

USAGE OF INTENT FILTER   [M1] [CWE-927]   WARNING

Description:

The mobile application uses an intent filter.
Intent filters should not be used for security purposes because they place no restrictions on explicit intents sent to the component, and can allow other applications on the same device to directly interact with them.
Intent filters are defined in the Android Manifest file, they let developers choose which type of intents their application components are supposed to receive and handle.

Example of secure code:

```
// When you use intent-filter, you have to perform input validation in your
code.
```

Example of insecure code:

```
<intent-filter>
                    <action android:name="android.intent.action.VIEW" />
                    <action android:name="android.intent.action.EDIT" />
                    <action android:name="android.intent.action.PICK" />
                    <category android:name="android.intent.category.DEFAULT" />
                    <data mimeType:name="vnd.android.cursor.dir/vnd.google.note"
/>
                </intent-filter>
```

There is '**<intent-filter>**' found in file 'android/AndroidManifest.xml':

```
[line 41:             <meta-data
android:name="io.flutter.embedding.android.NormalTheme"
android:resource="@style/NormalTheme"/>]
[line 42:             <intent-filter>]
[line 43:                 <action android:name="android.intent.action.MAIN"/>]
```

Reference:

- https://developer.android.com/guide/components/intents-filters.html

- https://developer.android.com/training/articles/security-tips.html

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

Software Composition Analysis

The mobile application uses the following external and native libraries:

External

- kotlinx.coroutines
- io.flutter
- com.baseflow
- com.amolg

Android Native

- androidx.core
- androidx.versionedparcelable
- androidx.activity
- androidx.vectordrawable
- androidx.lifecycle
- androidx.annotation
- androidx.fragment
- androidx.loader
- androidx.recyclerview
- androidx.window
- androidx.appcompat
- androidx.viewpager2
- androidx.coordinatorlayout
- androidx.savedstate
- androidx.constraintlayout
- androidx.media
- kotlin.jvm
- kotlin.coroutines
- android.hardware
- android.app
- android.widget
- android.location
- android.support
- android.view

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

- android.os
- android.text
- android.graphics
- android.icu

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/

Meet Regulatory and Compliance Requirements

Looking for a comprehensive security audit and compliance-ready report? You are at the right place.

Mobile Security Scanning	Mobile Penetration Testing	Cybersecurity Compliance

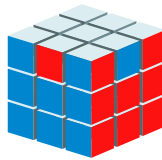**Trusted by 1,000+ customers from over 50 countries**

50+ international awards and industry recognitions

FREE DEMO

Because prevention is better

The End of Report

Upgrade from Free Community Edition to [ImmuniWeb® AI Platform](#)

Full Test Results: https://www.immuniweb.com/mobile/slt_field_app/8tLvEJkj/