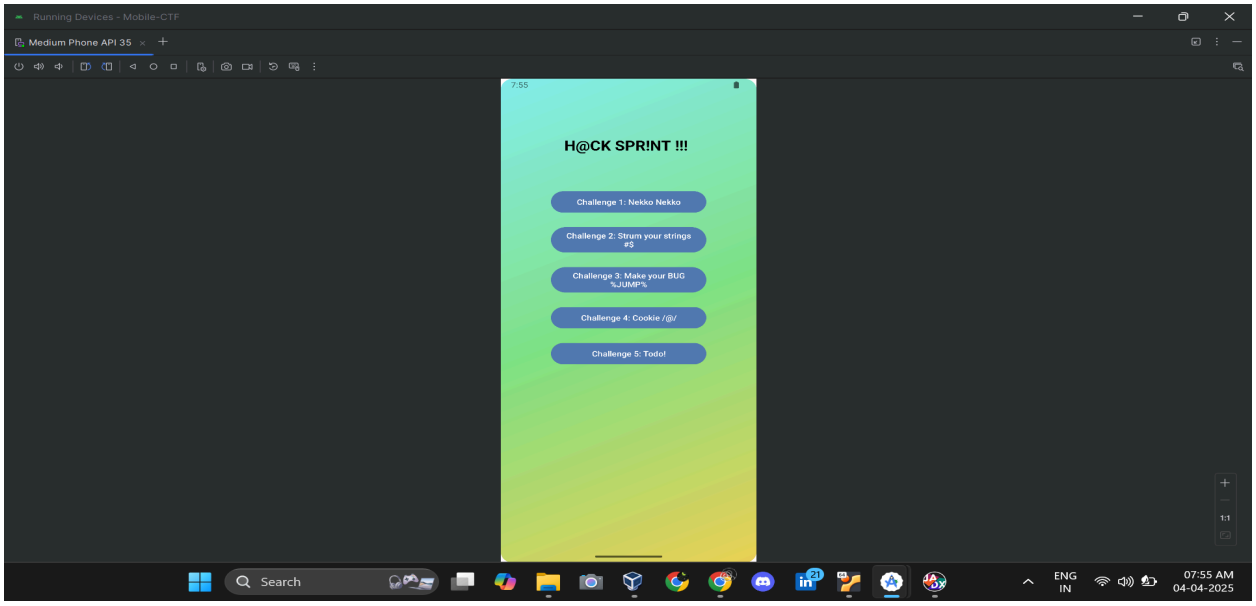
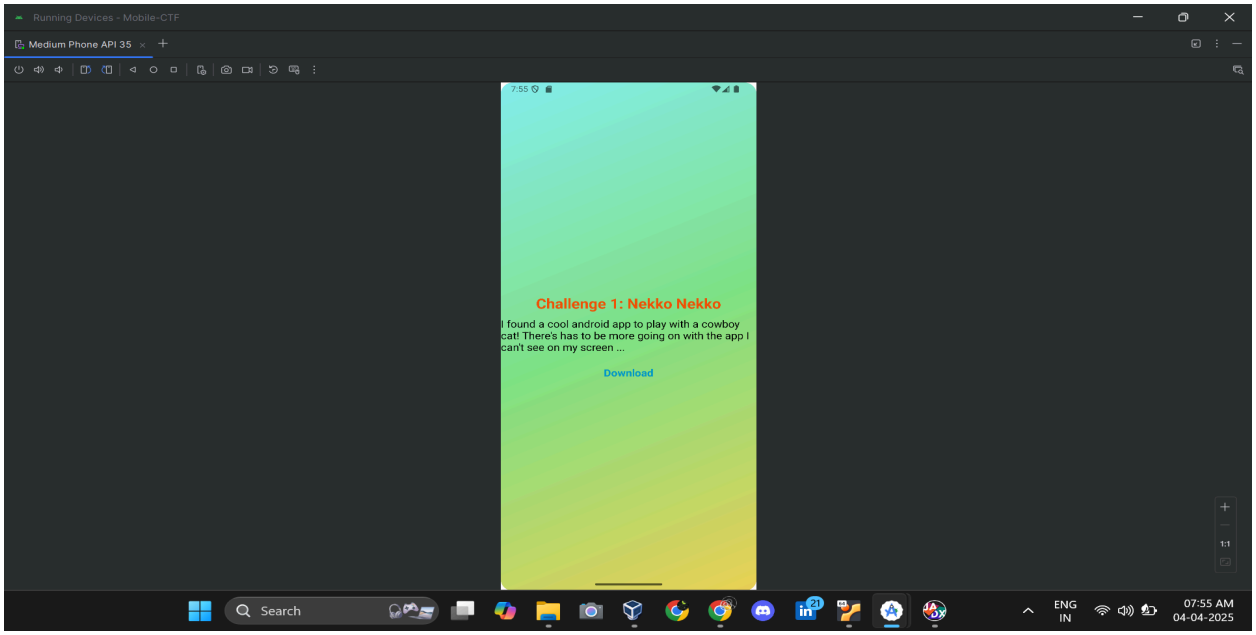
Mobile Security Lab

21PC35 - Smrithi P

21PC37 - Tharageshwaran S

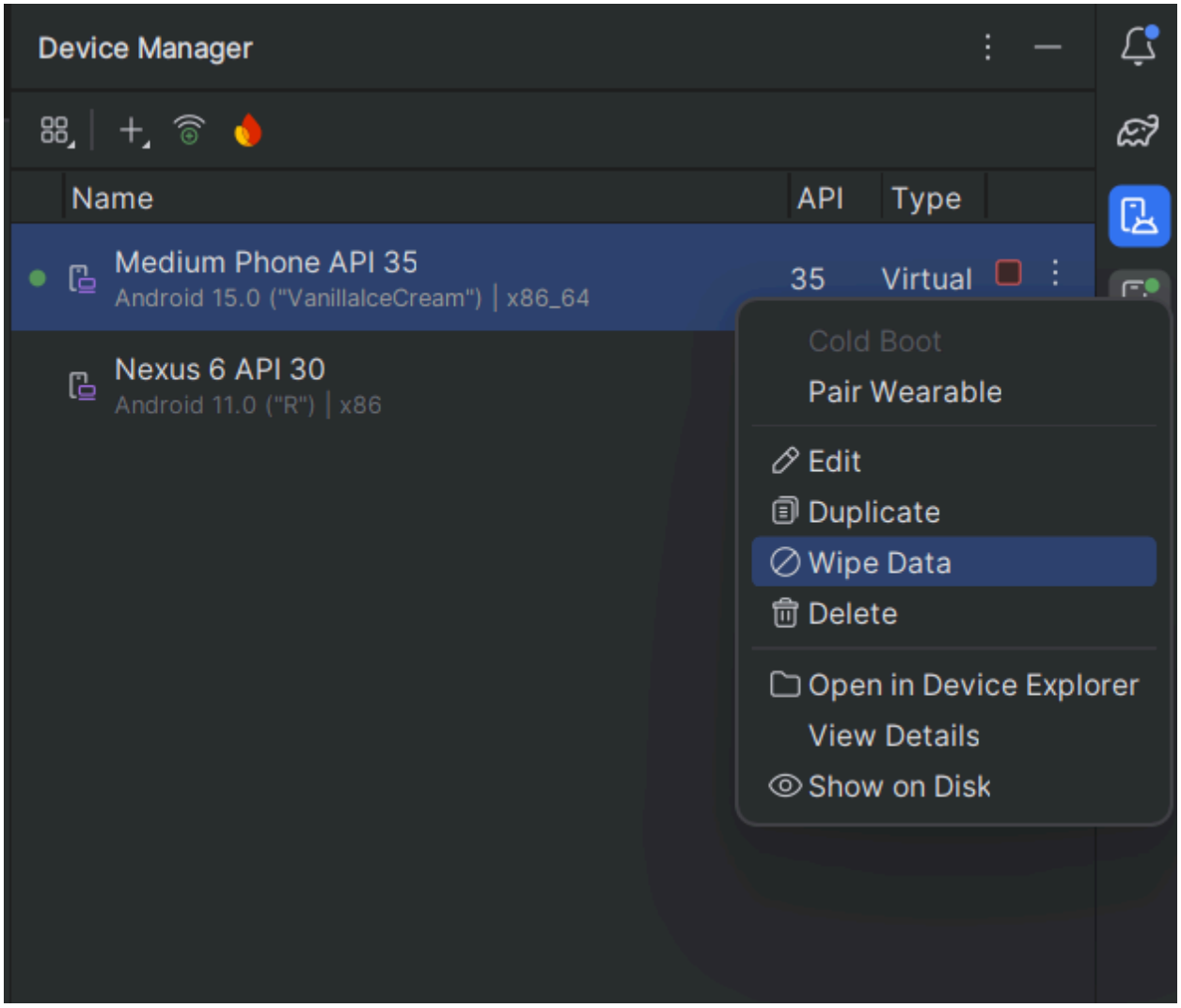
Mobile CTF





Note:

If the app doesn’t responds properly then we have to wipe the data to work without any interruptions.

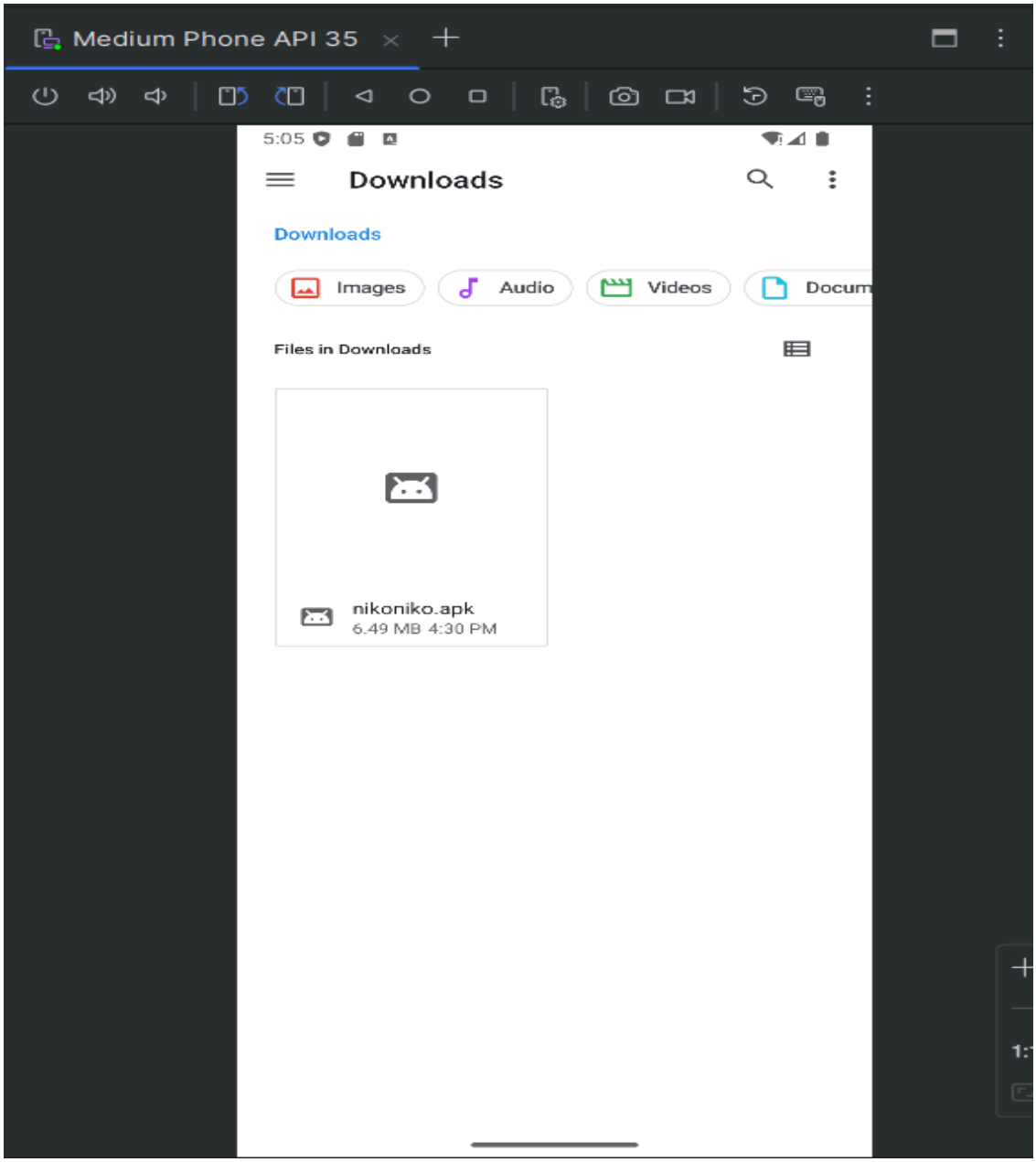


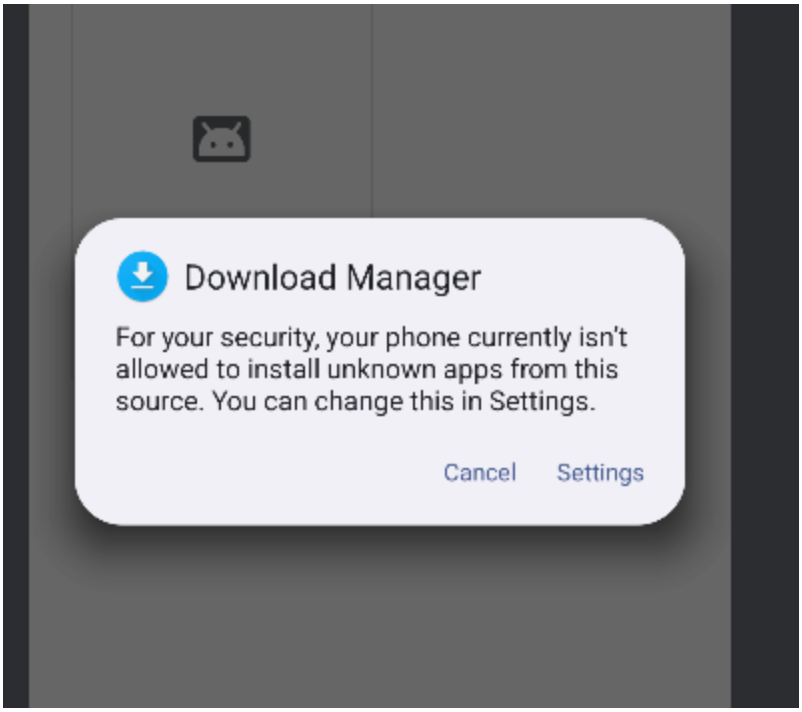
Challenge 1:

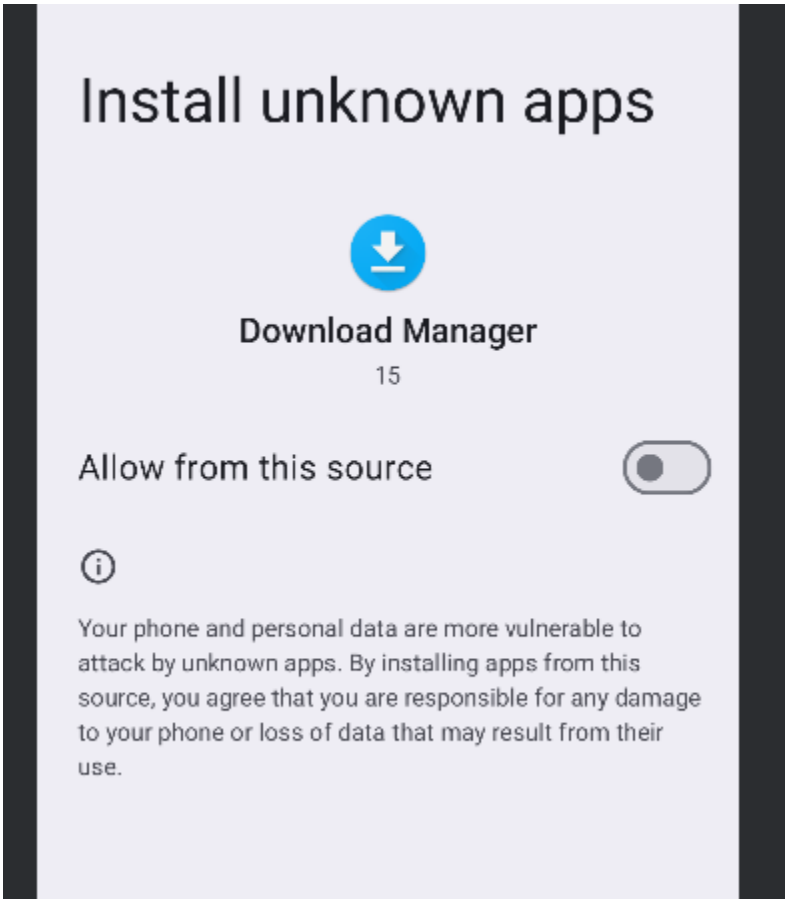
We are provided with the apk file for the challenge. I'll start by loading it into jadx-gui decompiler. Looking at the Android Manifest we see app info such as the package name, activity etc.

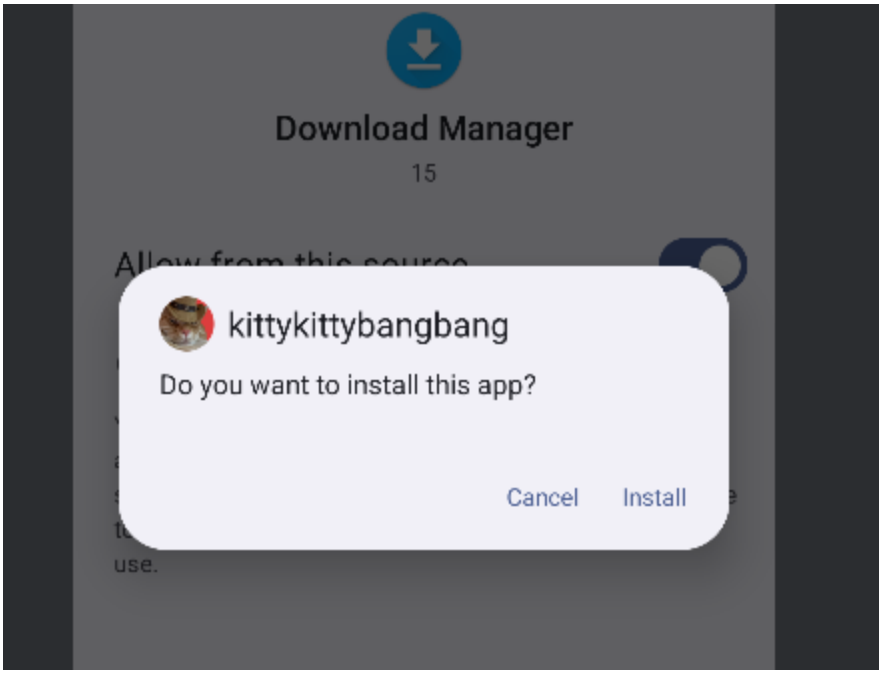
Navigating to the MainActivity and looking at the decompiled code, we note that the application logs several information including the flag.

With the logs streaming in, we tap on the picture of the cat. We then get the flag in the logs.

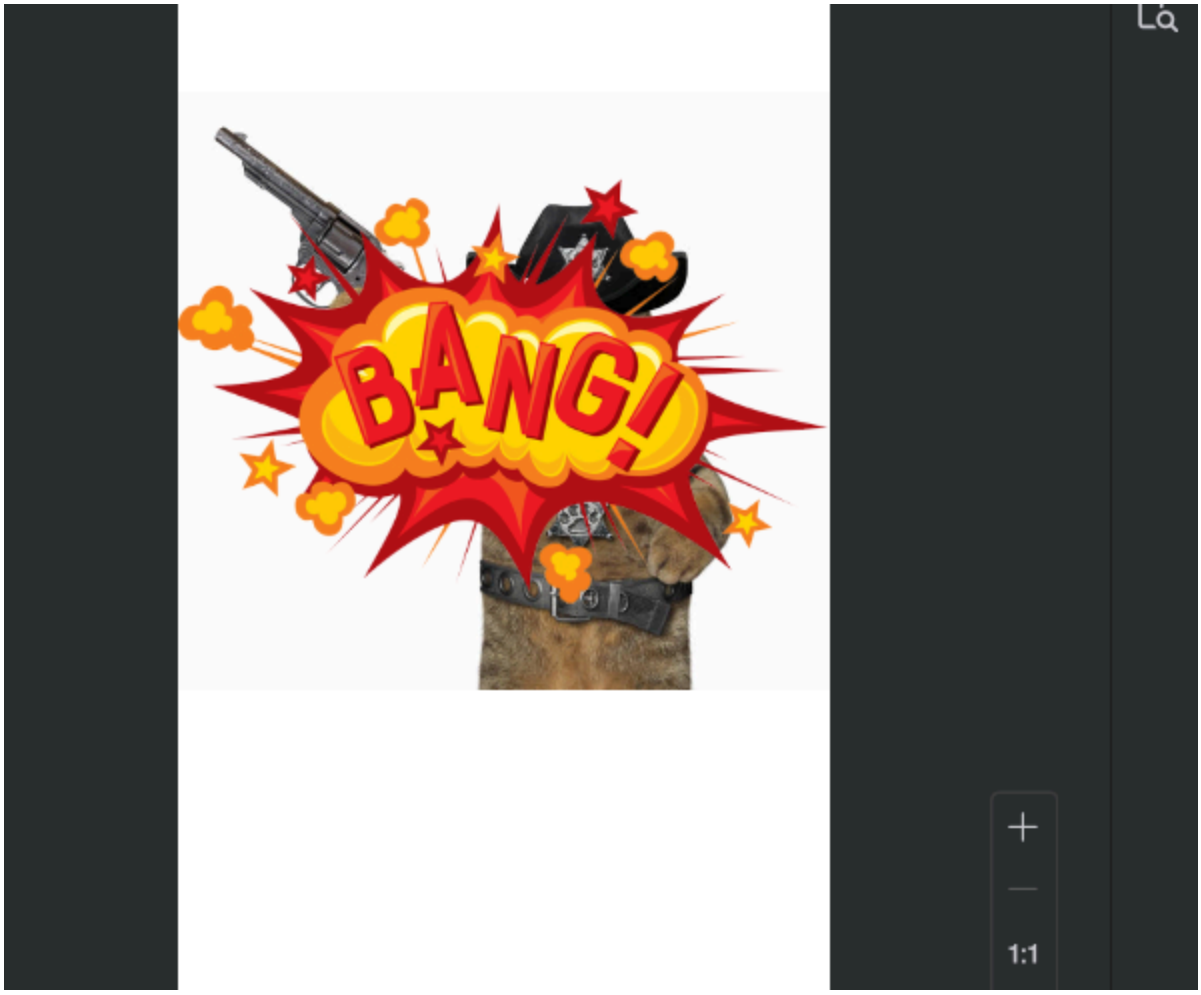


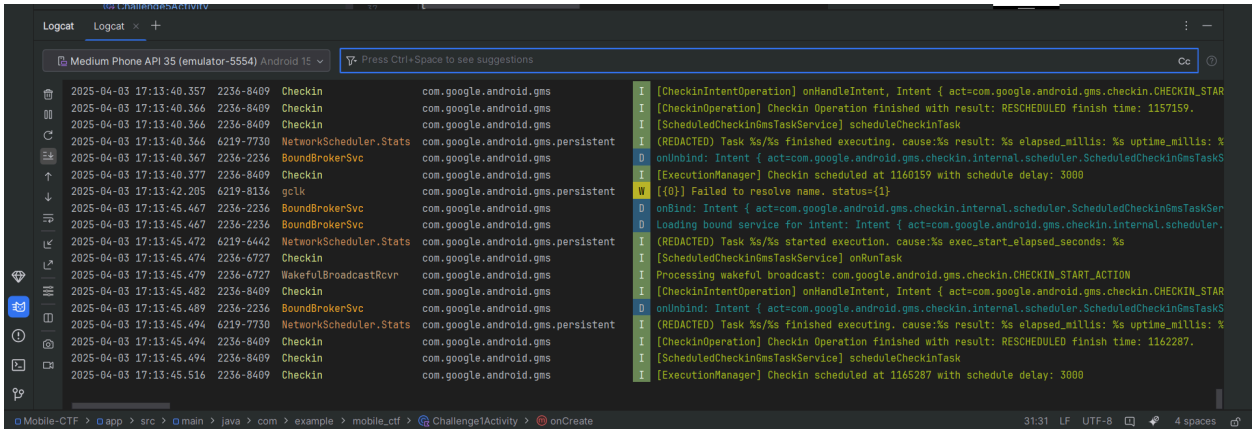

Download Manager
For your security, your phone currently isn't allowed to install unknown apps from this source. You can change this in Settings.
Cancel
Settings

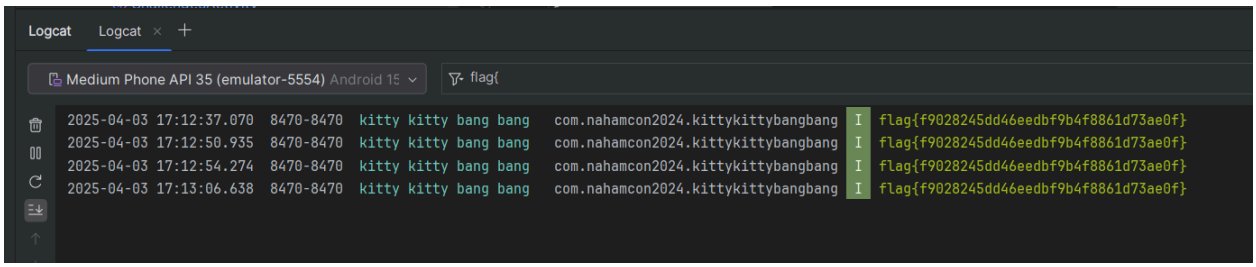

Install unknown apps
Download Manager
15
Allow from this source
Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.


Download Manager
15
kittykittybangbang
Do you want to install this app?
Cancel
Install


5:12


BANG!
1:1

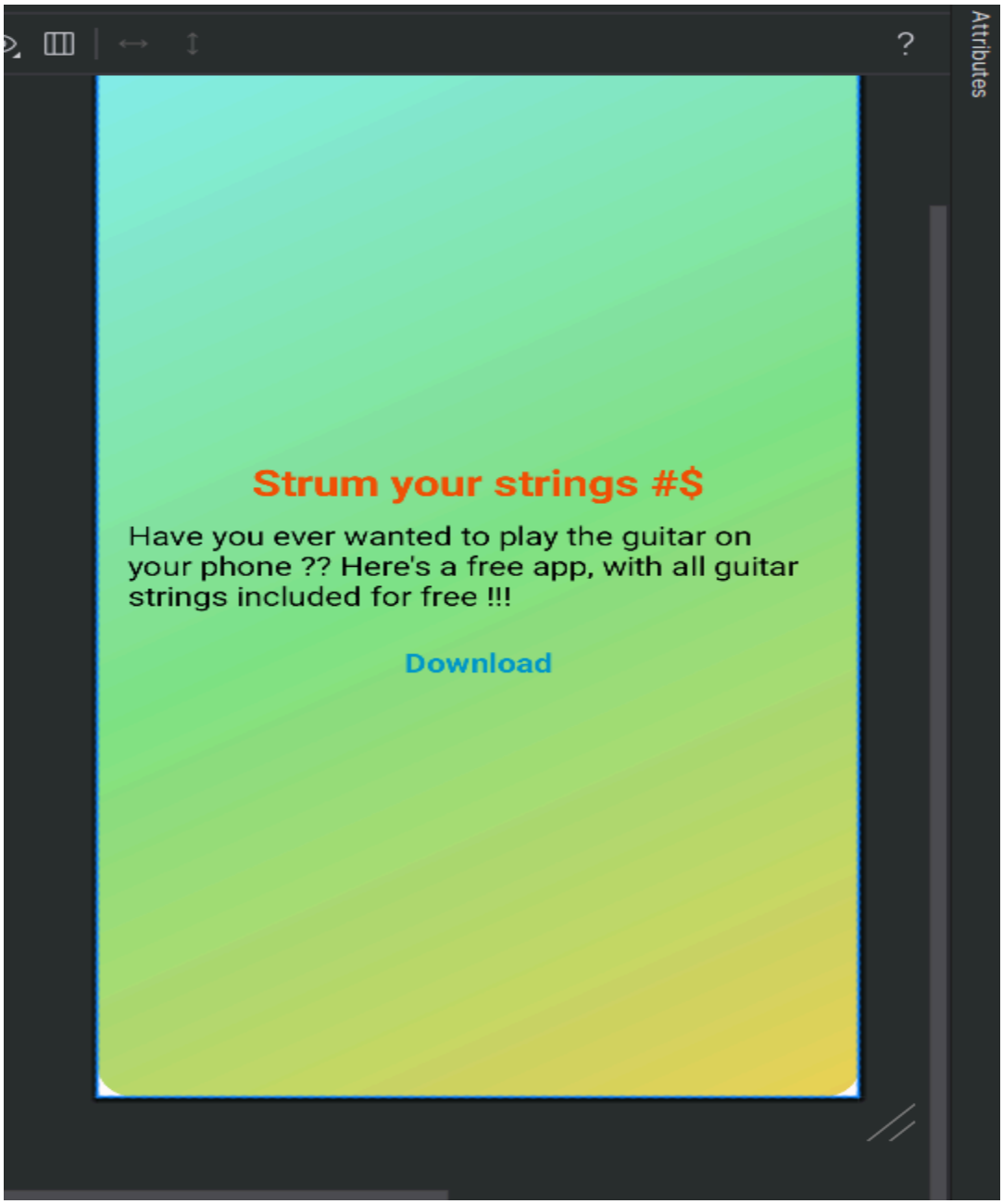

Logcat
Logcat
Medium Phone API 35 (emulator-5554) Android 15
Press Ctrl+Space to see suggestions
2025-04-03 17:13:40.357 2236-8409 Checkin com.google.android.gms I [CheckinIntentOperation] onHandleIntent, Intent { act=com.google.android.gms.checkin.CHECKIN_STAR
2025-04-03 17:13:40.366 2236-8409 Checkin com.google.android.gms I [CheckinOperation] Checkin Operation finished with result: RESCHEDULED finish time: 1157159.
2025-04-03 17:13:40.366 2236-8409 Checkin com.google.android.gms I [ScheduledCheckinGmsTaskService] scheduleCheckinTask
2025-04-03 17:13:40.366 6219-7730 NetworkScheduler.Stats com.google.android.gms.persistent I (REDACTED) Task %s/%s finished executing. cause:%s result: %s elapsed_millis: %s uptime_millis: %
2025-04-03 17:13:40.367 2236-2236 BoundBrokerSvc com.google.android.gms D onUnbind: Intent { act=com.google.android.gms.checkin.internal.scheduler.ScheduledCheckinGmsTaskS
2025-04-03 17:13:40.377 2236-8409 Checkin com.google.android.gms I [ExecutionManager] Checkin scheduled at 1160159 with schedule delay: 3000
2025-04-03 17:13:42.205 6219-8136 gclk com.google.android.gms.persistent W [{0}] Failed to resolve name. status={1}
2025-04-03 17:13:45.467 2236-2236 BoundBrokerSvc com.google.android.gms D onBind: Intent { act=com.google.android.gms.checkin.internal.scheduler.ScheduledCheckinGmsTaskSer
2025-04-03 17:13:45.467 2236-2236 BoundBrokerSvc com.google.android.gms D Loading bound service for intent: Intent { act=com.google.android.gms.checkin.internal.scheduler.
2025-04-03 17:13:45.472 6219-6442 NetworkScheduler.Stats com.google.android.gms.persistent I (REDACTED) Task %s/%s started execution. cause:%s exec_start_elapsed_seconds: %s
2025-04-03 17:13:45.474 2236-6727 Checkin com.google.android.gms I [ScheduledCheckinGmsTaskService] onRunTask
2025-04-03 17:13:45.479 2236-6727 WakefulBroadcastRcvr com.google.android.gms I Processing wakeful broadcast: com.google.android.gms.checkin.CHECKIN_START_ACTION
2025-04-03 17:13:45.482 2236-8409 Checkin com.google.android.gms I [CheckinIntentOperation] onHandleIntent, Intent { act=com.google.android.gms.checkin.CHECKIN_STAR
2025-04-03 17:13:45.489 2236-2236 BoundBrokerSvc com.google.android.gms D onUnbind: Intent { act=com.google.android.gms.checkin.internal.scheduler.ScheduledCheckinGmsTaskS
2025-04-03 17:13:45.494 6219-7730 NetworkScheduler.Stats com.google.android.gms.persistent I (REDACTED) Task %s/%s finished executing. cause:%s result: %s elapsed_millis: %s uptime_millis: %
2025-04-03 17:13:45.494 2236-8409 Checkin com.google.android.gms I [CheckinOperation] Checkin Operation finished with result: RESCHEDULED finish time: 1162287.
2025-04-03 17:13:45.494 2236-8409 Checkin com.google.android.gms I [ScheduledCheckinGmsTaskService] scheduleCheckinTask
2025-04-03 17:13:45.516 2236-8409 Checkin com.google.android.gms I [ExecutionManager] Checkin scheduled at 1165287 with schedule delay: 3000
Mobile-CTF > app > src > main > java > com > example > mobile_ctf > Challenge1Activity > onCreate
31:31 LF UTF-8 4 spaces

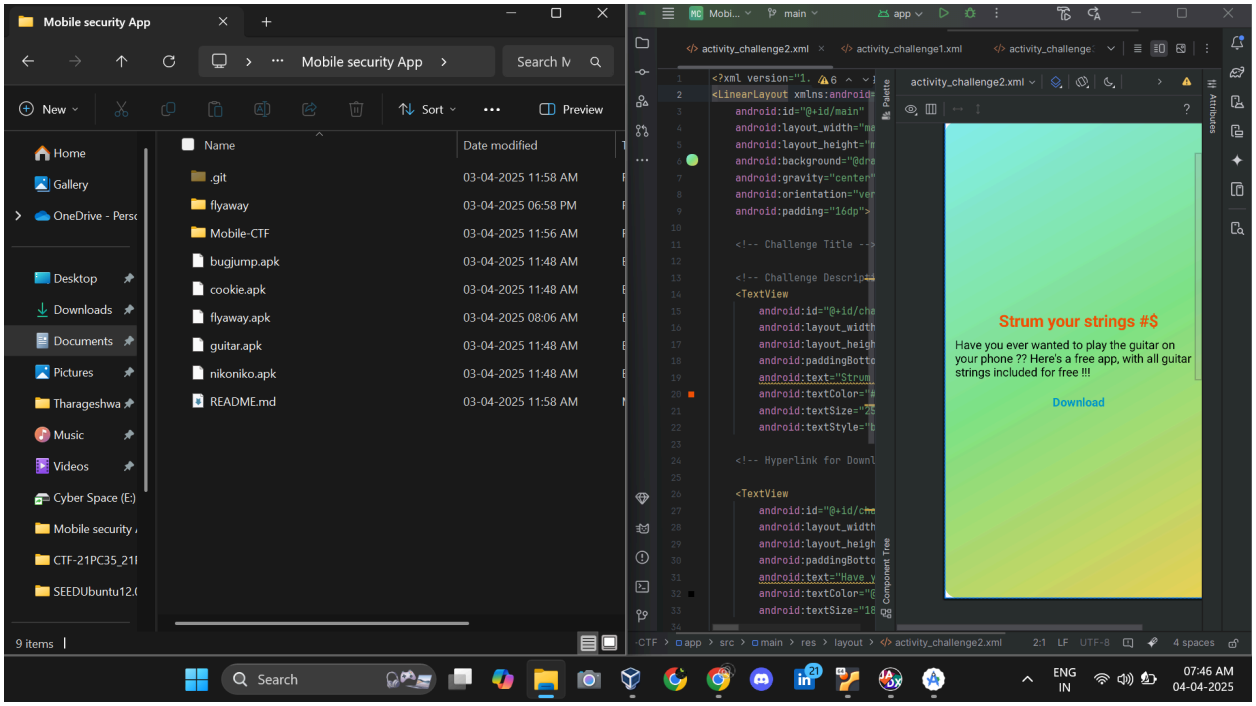

Logcat
Logcat
Medium Phone API 35 (emulator-5554) Android 15
flag{
2025-04-03 17:12:37.070 8470-8470 kitty kitty bang bang com.nahamcon2024.kittykittybangbang I flag{f9028245dd46eedbf9b4f8861d73ae0f}
2025-04-03 17:12:50.935 8470-8470 kitty kitty bang bang com.nahamcon2024.kittykittybangbang I flag{f9028245dd46eedbf9b4f8861d73ae0f}
2025-04-03 17:12:54.274 8470-8470 kitty kitty bang bang com.nahamcon2024.kittykittybangbang I flag{f9028245dd46eedbf9b4f8861d73ae0f}
2025-04-03 17:13:06.638 8470-8470 kitty kitty bang bang com.nahamcon2024.kittykittybangbang I flag{f9028245dd46eedbf9b4f8861d73ae0f}

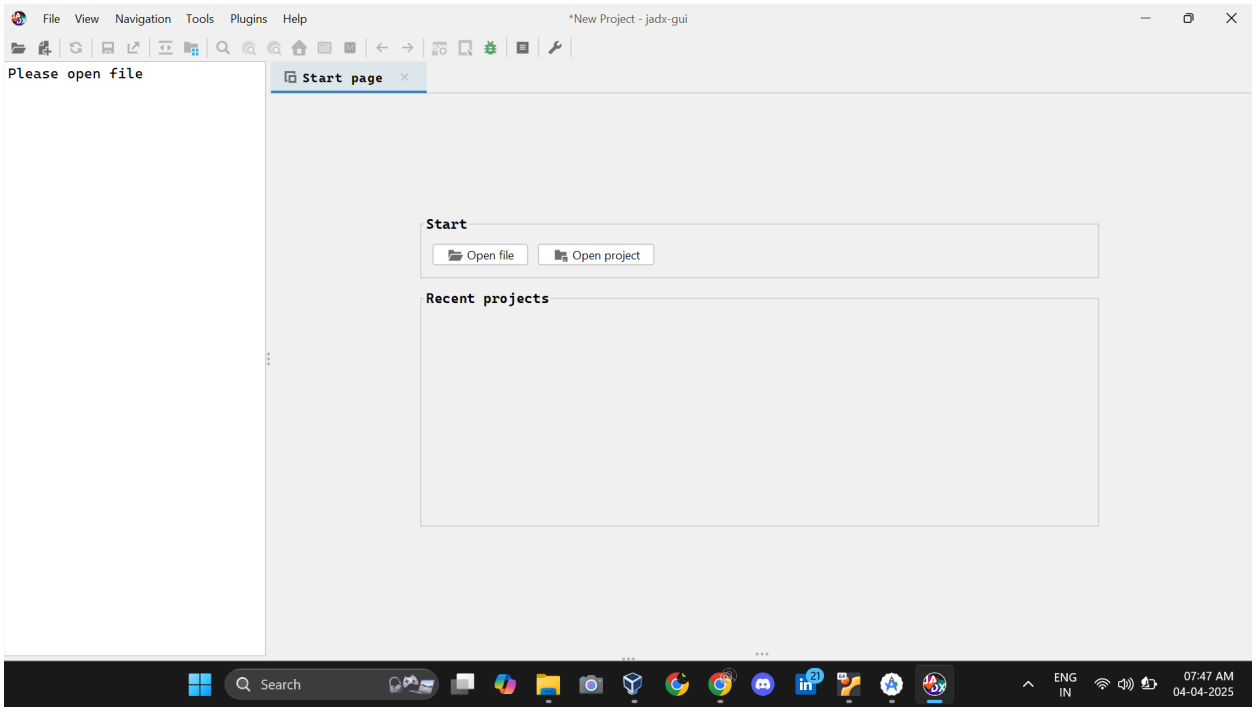
Challenge 2:

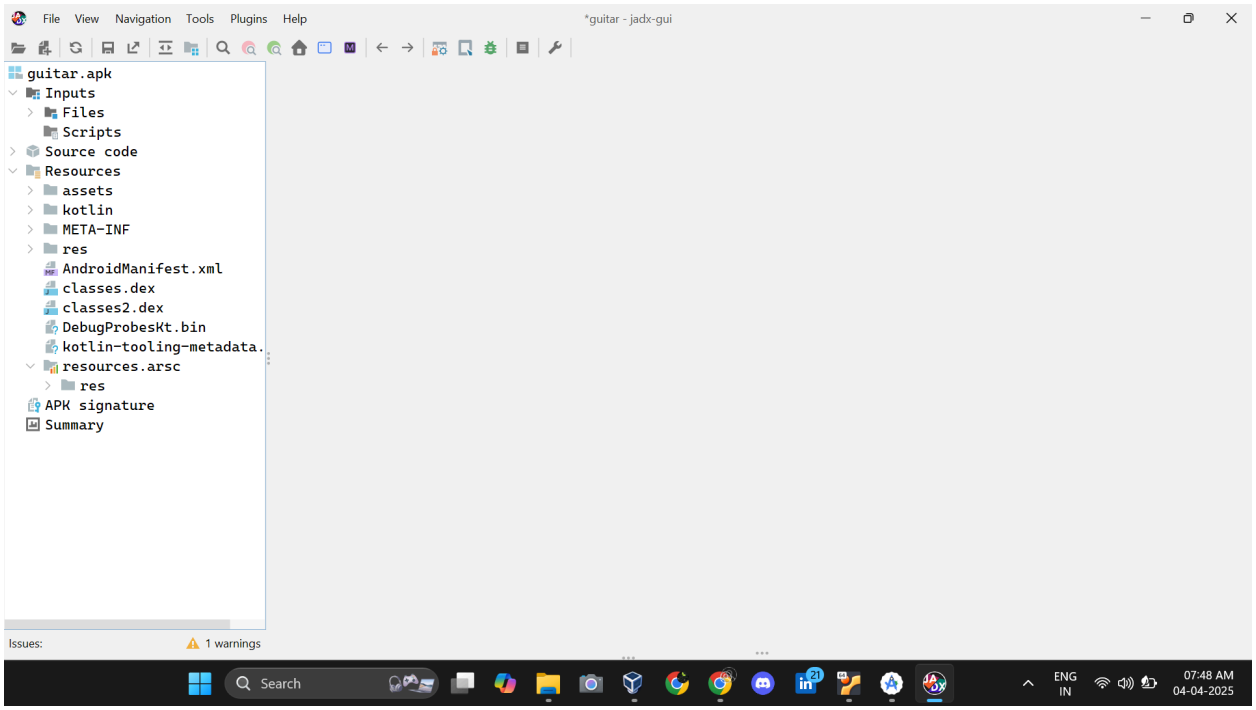
We are provided with the apk which I'll load into jadx.

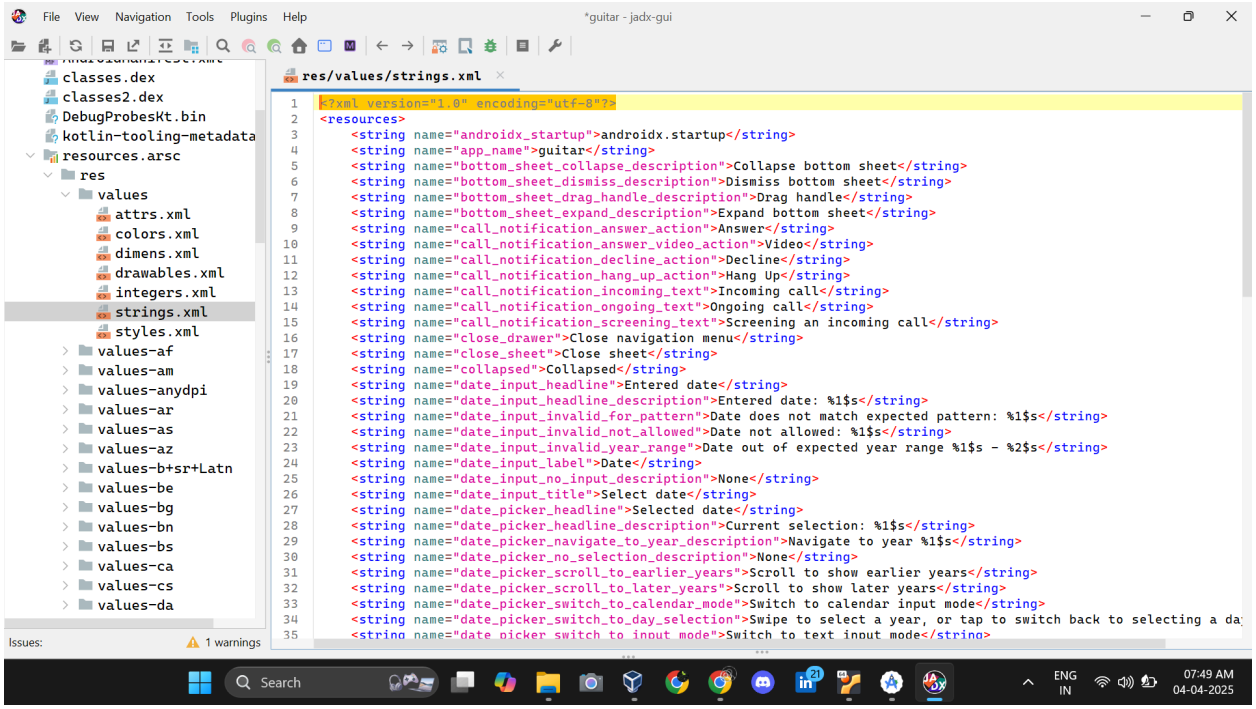
Looking through the Android Manifest and decompiled code, I eventually found the flag in the strings.xml file in base64 encoded format.

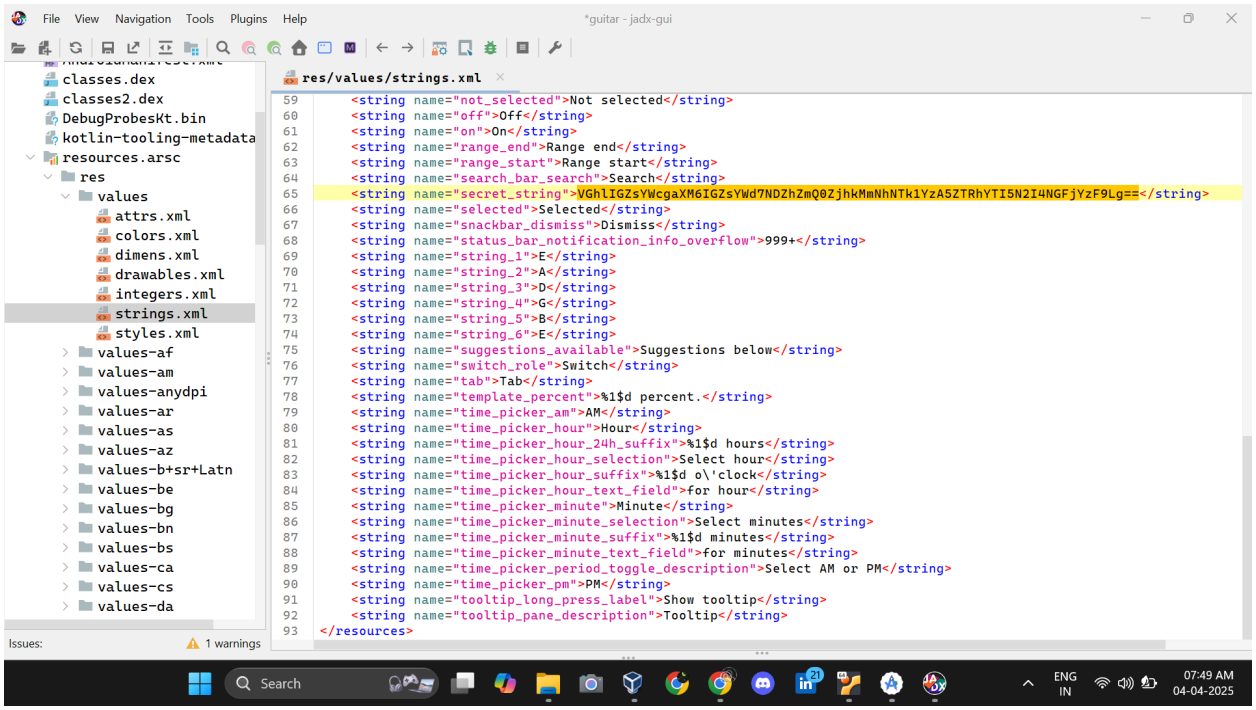


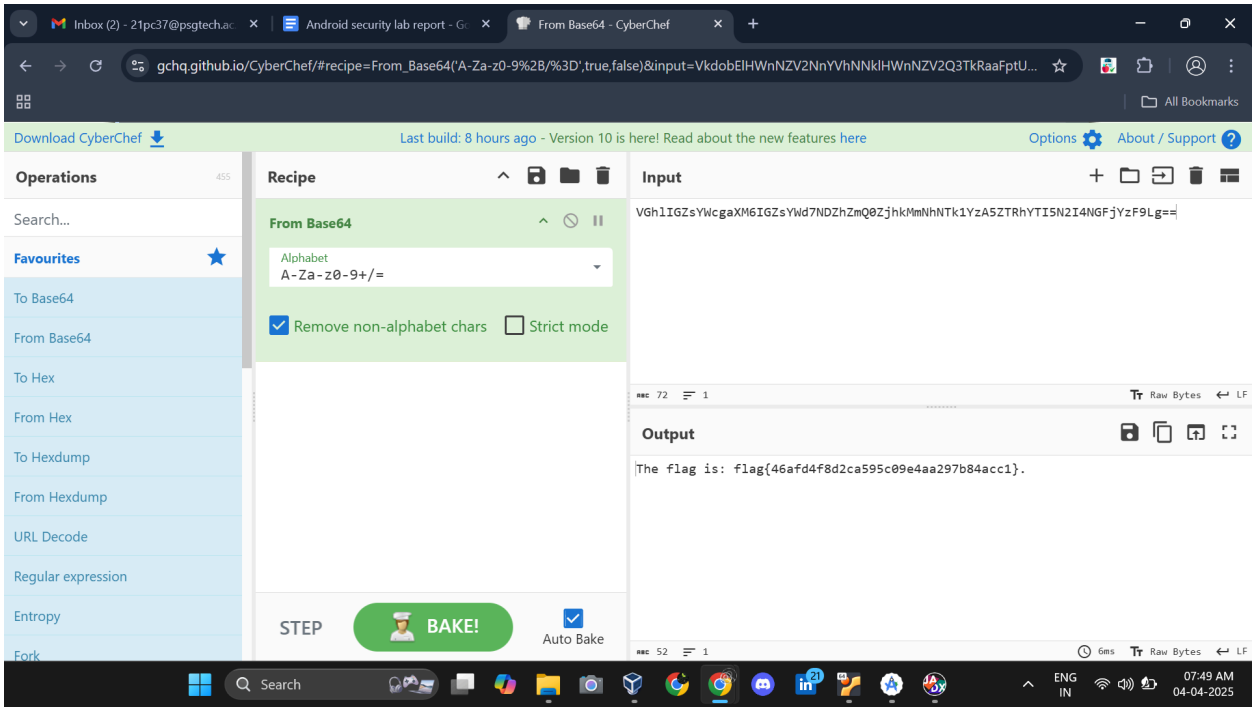

Mobile security App
Search Mobile security App
New
Sort
Preview
Home
Gallery
OneDrive - Perso
Desktop
Downloads
Documents
Pictures
Thirageshwa
Music
Videos
Cyber Space (E:)
Mobile security
CTF-21PC35_21I
SEEDUbuntu12.(
Name
Date modified
.git
03-04-2025 11:58 AM
flyaway
03-04-2025 06:58 PM
Mobile-CTF
03-04-2025 11:56 AM
bugjump.apk
03-04-2025 11:48 AM
cookie.apk
03-04-2025 11:48 AM
flyaway.apk
03-04-2025 08:06 AM
guitar.apk
03-04-2025 11:48 AM
nikoniko.apk
03-04-2025 11:48 AM
README.md
03-04-2025 11:58 AM
9 items
activity_challenge2.xml
activity_challenge1.xml
Strum your strings #$
Have you ever wanted to play the guitar on your phone ?? Here's a free app, with all guitar strings included for free !!!
Download
Search
ENG IN
07:46 AM
04-04-2025


File View Navigation Tools Plugins Help
*New Project - jadx-gui
Please open file
Start page
Start
Open file
Open project
Recent projects
Search
ENG IN
07:47 AM
04-04-2025


File View Navigation Tools Plugins Help
*guitar - jadx-gui
guitar.apk
Inputs
Files
Scripts
Source code
Resources
assets
kotlin
META-INF
res
AndroidManifest.xml
classes.dex
classes2.dex
DebugProbesKt.bin
kotlin-tooling-metadata.
resources.arsc
res
APK signature
Summary
Issues:
1 warnings
Search
ENG
IN
07:48 AM
04-04-2025

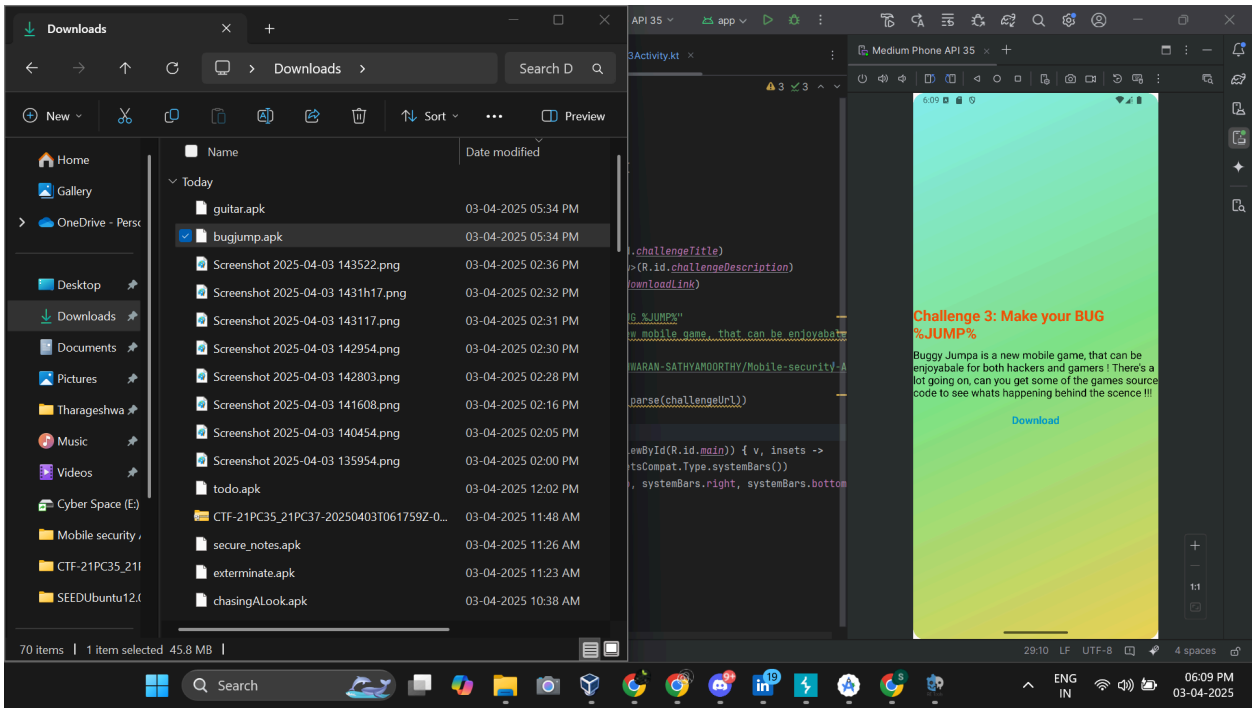

File View Navigation Tools Plugins Help
*guitar - jadx-gui
classes.dex
classes2.dex
DebugProbesKt.bin
kotlin-tooling-metadata
resources.arsc
res
values
attrs.xml
colors.xml
dimens.xml
drawables.xml
integers.xml
strings.xml
styles.xml
values-af
values-am
values-anydpi
values-ar
values-as
values-az
values-b+sr+Latn
values-be
values-bg
values-bn
values-bs
values-ca
values-cs
values-da
res/values/strings.xml
<?xml version="1.0" encoding="utf-8"?>
<resources>
<string name="androidx_startup">androidx.startup</string>
<string name="app_name">guitar</string>
<string name="bottom_sheet_collapse_description">Collapse bottom sheet</string>
<string name="bottom_sheet_dismiss_description">Dismiss bottom sheet</string>
<string name="bottom_sheet_drag_handle_description">Drag handle</string>
<string name="bottom_sheet_expand_description">Expand bottom sheet</string>
<string name="call_notification_answer_action">Answer</string>
<string name="call_notification_answer_video_action">Video</string>
<string name="call_notification_decline_action">Decline</string>
<string name="call_notification_hang_up_action">Hang Up</string>
<string name="call_notification_incoming_text">Incoming call</string>
<string name="call_notification_ongoing_text">Ongoing call</string>
<string name="call_notification_screening_text">Screening an incoming call</string>
<string name="close_drawer">Close navigation menu</string>
<string name="close_sheet">Close sheet</string>
<string name="collapsed">Collapsed</string>
<string name="date_input_headline">Entered date</string>
<string name="date_input_headline_description">Entered date: %1$s</string>
<string name="date_input_invalid_for_pattern">Date does not match expected pattern: %1$s</string>
<string name="date_input_invalid_not_allowed">Date not allowed: %1$s</string>
<string name="date_input_invalid_year_range">Date out of expected year range %1$s - %2$s</string>
<string name="date_input_label">Date</string>
<string name="date_input_no_input_description">None</string>
<string name="date_input_title">Select date</string>
<string name="date_picker_headline">Selected date</string>
<string name="date_picker_headline_description">Current selection: %1$s</string>
<string name="date_picker_navigate_to_year_description">Navigate to year %1$s</string>
<string name="date_picker_no_selection_description">None</string>
<string name="date_picker_scroll_to_earlier_years">Scroll to show earlier years</string>
<string name="date_picker_scroll_to_later_years">Scroll to show later years</string>
<string name="date_picker_switch_to_calendar_mode">Switch to calendar input mode</string>
<string name="date_picker_switch_to_day_selection">Swipe to select a year, or tap to switch back to selecting a da
<string name="date_picker_switch_to_input_mode">Switch to text input mode</string>
Issues:
1 warnings
Search
ENG
IN
07:49 AM
04-04-2025

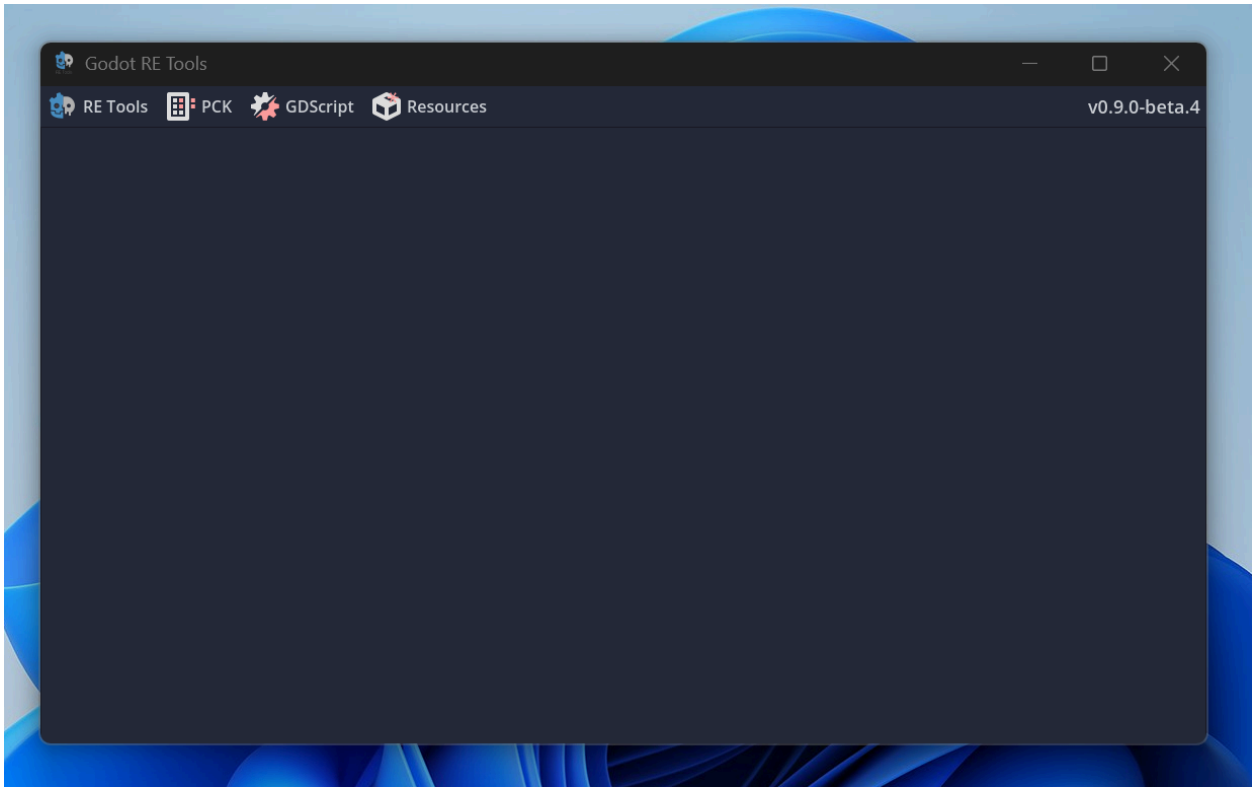

File View Navigation Tools Plugins Help
*guitar - jadx-gui
classes.dex
classes2.dex
DebugProbesKt.bin
kotlin-tooling-metadata
resources.arsc
res
values
attrs.xml
colors.xml
dimens.xml
drawables.xml
integers.xml
strings.xml
styles.xml
values-af
values-am
values-anydpi
values-ar
values-as
values-az
values-b+sr+Latn
values-be
values-bg
values-bn
values-bs
values-ca
values-cs
values-da
res/values/strings.xml
<string name="not_selected">Not selected</string>
<string name="off">Off</string>
<string name="on">On</string>
<string name="range_end">Range end</string>
<string name="range_start">Range start</string>
<string name="search_bar_search">Search</string>
<string name="secret_string">VGhlIGZsYWcgaXM6IGZsYWd7NDZhZmQ0ZjhkMmNhNTk1YzA5ZTRhYTI5N2I4NGFjYzF9Lg==</string>
<string name="selected">Selected</string>
<string name="snackbar_dismiss">Dismiss</string>
<string name="status_bar_notification_info_overflow">999+</string>
<string name="string_1">E</string>
<string name="string_2">A</string>
<string name="string_3">D</string>
<string name="string_4">G</string>
<string name="string_5">B</string>
<string name="string_6">E</string>
<string name="suggestions_available">Suggestions below</string>
<string name="switch_role">Switch</string>
<string name="tab">Tab</string>
<string name="template_percent">%1$d percent.</string>
<string name="time_picker_am">AM</string>
<string name="time_picker_hour">Hour</string>
<string name="time_picker_hour_24h_suffix">%1$d hours</string>
<string name="time_picker_hour_selection">Select hour</string>
<string name="time_picker_hour_suffix">%1$d o\'clock</string>
<string name="time_picker_hour_text_field">for hour</string>
<string name="time_picker_minute">Minute</string>
<string name="time_picker_minute_selection">Select minutes</string>
<string name="time_picker_minute_suffix">%1$d minutes</string>
<string name="time_picker_minute_text_field">for minutes</string>
<string name="time_picker_period_toggle_description">Select AM or PM</string>
<string name="time_picker_pm">PM</string>
<string name="tooltip_long_press_label">Show tooltip</string>
<string name="tooltip_pane_description">Tooltip</string>
</resources>
Issues:
1 warnings
Search
ENG IN
07:49 AM 04-04-2025

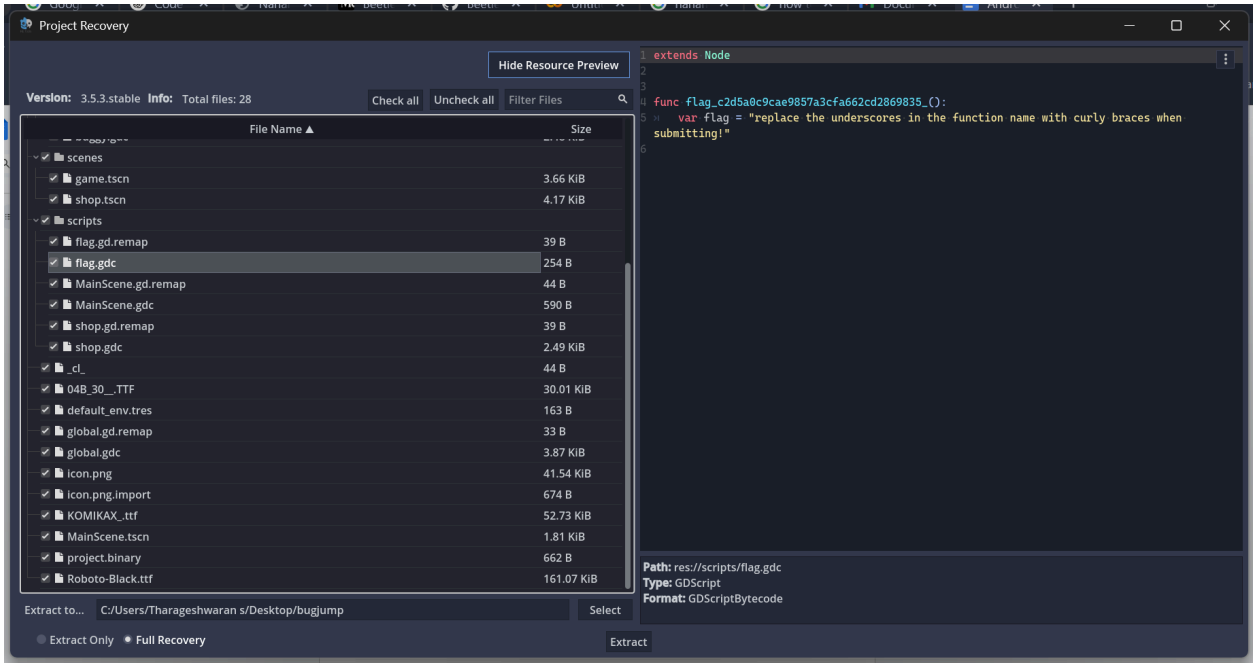

Inbox (2) - 21pc37@psgtech.ac
Android security lab report - Gc
From Base64 - CyberChef
gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=VkdobElHWnNZV2NnYVhNNklHWnNZV2Q3TkRaaFptU...
All Bookmarks
Download CyberChef
Last build: 8 hours ago - Version 10 is here! Read about the new features here
Options
About / Support
Operations
Search...
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Fork
Recipe
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Strict mode
STEP
BAKE!
Auto Bake
Input
VGhlIGZsYWcgaXM6IGZsYWd7NDZhZmQ0ZjhkMmNhNTk1YzA5ZTRhYTI5N2I4NGFjYzF9Lg==
Raw Bytes
LF
Output
The flag is: flag{46afd4f8d2ca595c09e4aa297b84acc1}.
Raw Bytes
LF
Search
ENG IN
07:49 AM 04-04-2025

Challenge 3:

This part of the app is written using Godot games. Only using those Gogot RE (Reverse engineering) tools we are able to find out the flag. Else we can’t able to find them






Project Recovery
Hide Resource Preview
Version: 3.5.3.stable Info: Total files: 28
Check all
Uncheck all
Filter Files
File Name ▲
Size
scenes
game.tscn 3.66 KiB
shop.tscn 4.17 KiB
scripts
flag.gd.remap 39 B
flag.gdc 254 B
MainScene.gd.remap 44 B
MainScene.gdc 590 B
shop.gd.remap 39 B
shop.gdc 2.49 KiB
_cl_ 44 B
04B_30__.TTF 30.01 KiB
default_env.tres 163 B
global.gd.remap 33 B
global.gdc 3.87 KiB
icon.png 41.54 KiB
icon.png.import 674 B
KOMIKAX_.ttf 52.73 KiB
MainScene.tscn 1.81 KiB
project.binary 662 B
Roboto-Black.ttf 161.07 KiB
Extract to...
C:/Users/Tharageshwaran s/Desktop/bugjump
Select
Extract Only
Full Recovery
Extract
extends Node
func flag_c2d5a0c9cae9857a3cfa662cd2869835_():
var flag = "replace the underscores in the function name with curly braces when submitting!"
Path: res://scripts/flag.gdc
Type: GDScript
Format: GDScriptBytecode

Challenge 4:

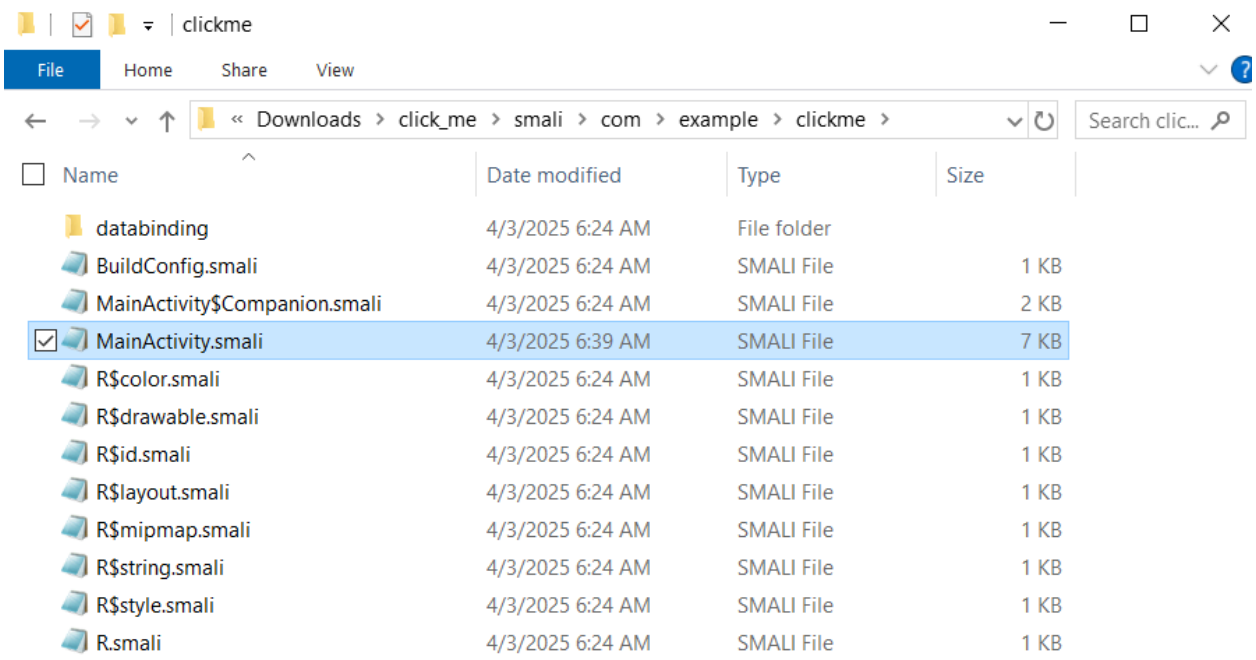
Install the apk with ADB

- adb install -r click_me.apk

Decompile it with apktool

- apktool d click_me.apk

```
public final void getFlagButtonClick(View view) {
    Intrinsics.checkNotNullParameter(view, "view");
    if (this.CLICKS == 99999999) {
        Toast.makeText(getApplicationContext(), getFlag(), 0).show();
    } else {
        Toast.makeText(getApplicationContext(), "You do not have enough cookies to get the flag", 0).show();
    }
}
```



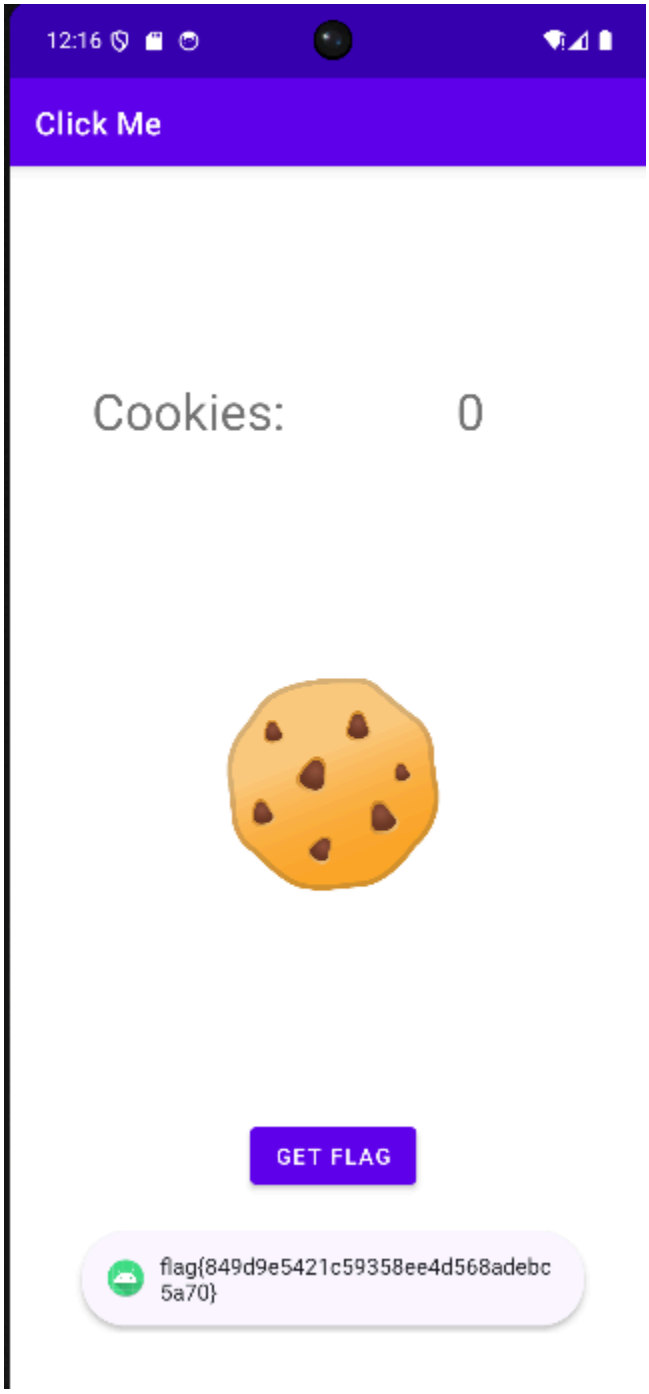
```
new-instance v0, Lcom/example/clickme/MainA

const/4 v1, 0x5f5e0ff

invoke-direct {v0, v1}, Lcom/example/clickme/M
```

instead of the above
Substitute the below

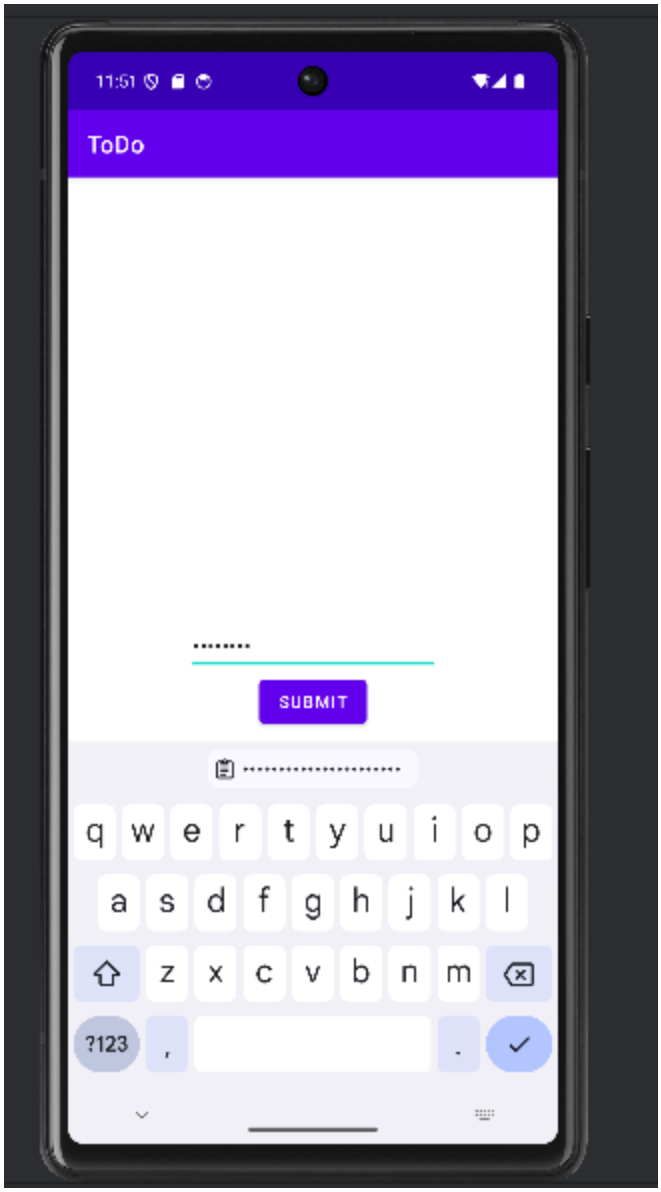
```
# direct methods
.method static constructor <clinit>()V
    .locals 2

    new-instance v0, Lcom/example/clickme/MainActivity$Compani

    const/4 v1, 0x0

    invoke-direct {v0, v1}, Lcom/example/clickme/MainActivity$Com

    sput-object v0, Lcom/example/clickme/MainActivity;->Companio

    const-string v0, "clickme"
```

```
1  if (this.CLICKS == 0) {
2      Toast.makeText(getApplicationContext(), getFlag(), 0).show();
3  }
```

- apktool b click_me
- keytool -genkey -v -keystore name.keystore -keyalg RSA -keysize 2048 -validity 10000 -alias alias
- C:\Users\smrit\AppData\Local\Android\Sdk\build-tools\34.0.0\zipalign.exe -v -p 4 click_me/dist/click_me.apk clicc_me-aligned.apk
- C:\Users\smrit\AppData\Local\Android\Sdk\build-tools\34.0.0 \apksigner.bat sign --ks name.keystore --ks-key-alias alias --ks-pass "pass:Smrin@0123" --key-pass "pass:Smrin@0123" --out click_me-signed.apk click_me-aligned.apk


12:16
Click Me
Cookies: 0
GET FLAG
flag{849d9e5421c59358ee4d568adebc5a70}

Challenge 5:



Inspect using JDAX

```java
public class LoginActivity extends AppCompatActivity {
    @Override
    protected void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        setContentView(C0523R.layout.activity_login);
        Button button = (Button) findViewById(C0523R.id.button);
        final TextView textView = (TextView) findViewById(C0523R.id.password);
        final Intent intent = new Intent(this, (Class<?>) MainActivity.class);
        button.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View view) {
                if (textView.getText().toString().equals("testtest")) {
                    LoginActivity.this.startActivity(intent);
                } else {
                    Toast.makeText(LoginActivity.this.getApplicationContext(), "Wrong password", 0).show();
                }
            }
        });
    }
}
```

By examining the AndroidManifest.xml file, I noticed that the MainActivity is marked as exported, meaning it can be accessed directly without going through the login activity.

To exploit this, I closed the app and used ADB to start the MainActivity directly with the following command:

adb shell am start -n com.congon4tor.todo/.MainActivity

This command successfully launched the MainActivity, bypassing the login screen altogether.

Next, I needed to determine where the notes—and potentially the flag—were stored. Upon analyzing the MainActivity code, I observed that during its creation (onCreate method), it interacts with a database helper. This suggests that the notes, and likely the flag, are stored in a database managed by the app. Further investigation into the database helper would reveal the exact location and contents of the notes, including the flag.

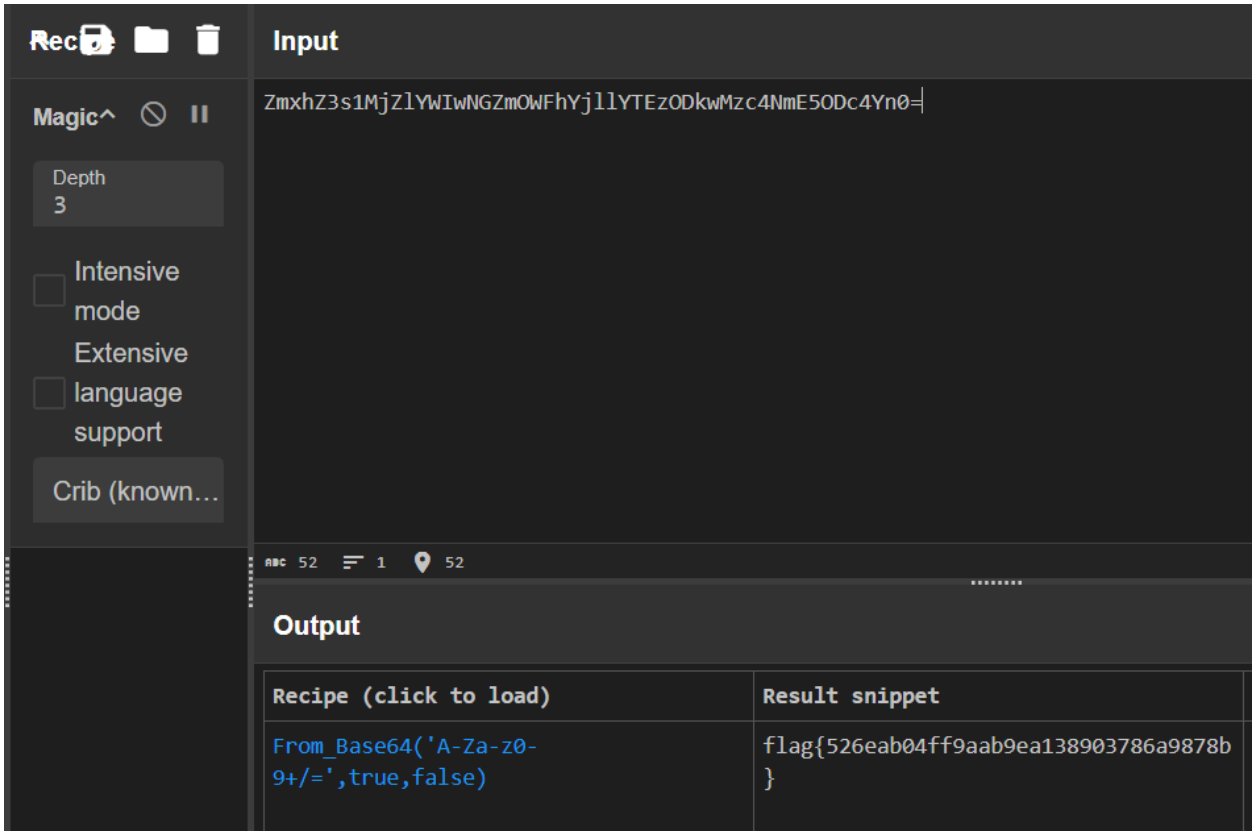
```
public void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        setContentView(C0523R.layout.activity_main);
        MyDatabase myDatabase = new MyDatabase(this);
        this.f92db = myDatabase;
        this.todos = myDatabase.getTodos();
        ArrayList arrayList = new ArrayList();
        try {
[...]
[...]
[...]
```

```
public class MyDatabase extends SQLiteAssetHelper {
    private static final String DATABASE_NAME = "todos.db";
    private static final int DATABASE_VERSION = 1;

    public MyDatabase(Context context) {
        super(context, DATABASE_NAME, null, 1);
    }

    public Cursor getTodos() {
        SQLiteDatabase readableDatabase = getReadableDatabase();
        SQLiteQueryBuilder sQLiteQueryBuilder = new SQLiteQueryBuilder();
        sQLiteQueryBuilder.setTables("todo");
        Cursor query = sQLiteQueryBuilder.query(readableDatabase, new String[]{"id AS _id", "content"}, null, null, null
        query.moveToFirst();
        return query;
    }
}
```

Upon examining the AndroidManifest.xml file, I noticed that the android:allowBackup="true" attribute is enabled. This setting allows the app's data to be backed up using ADB. Leveraging this, I created a backup of the app's data with ADB and successfully extracted the todo.db file, which likely contains the notes and the flag.

Additionally, for those with a rooted device, an alternative approach is to execute a series of commands to directly access the app's data.

```
PS C:\Users\smrit\Downloads\c4> adb shell
emu64xa:/ $ su
emu64xa:/ # cp /data/data/com.congon4tor.todo/databases/todos.db /sdcard/
emu64xa:/ # exit
PS C:\Users\smrit\Downloads\c4> adb pull /sdcard/todos.db .
PS C:\Users\smrit\Downloads\c4> sqlite3 todos.db
SQLite version 3.42.0 2023-05-16 12:36:15
Enter ".help" for usage hints.
sqlite> .headers on
sqlite> .tables
android_metadata  todo
sqlite> select * from todo;
id|content
1|ZmxhZ3s1MjZlYWIwNGZmOWFhYjllYTEzODkwMzc4NmE5ODc4Yn0=
2|VXNlIGFjdHVhbCBlbmNyeXB0aW9uIG5vdCBqdXN0IGJhc2U2NA==
sqlite> exit
```



Flag: flag{526eab04ff9aab9ea138903786a9878b}