VulnDroid CTF Challenge

Shravani Bande

April 27, 2025

Contents

1 Introduction

This report provides a detailed explanation of how the VulnDroid CTF challenge was approached and successfully solved. The VulnDroid application is designed to simulate real-world Android application vulnerabilities related to local storage mismanagement. The challenge involved capturing flags hidden in different parts of the application by exploiting insecure coding practices.

2 Task Statement

The task was to:

- Install and configure VulnDroid.
- Solve the following levels by finding and submitting the hidden flags:
  1. Hardcoding Details
  2. Insecure Logging
  3. Insecure Database
  4. Sensitive Info in Android VCS
- Validate each flag by entering it in the app and reaching the Congratulations screen.
- (Additionally) Explore and solve any extra levels if possible.

3 Environment Setup

- **Device/Emulator:** Android Emulator (64-bit)
- **Tools Used:**
  - Android Debug Bridge (adb)
  - JADX decompiler
  - Android Studio (Logcat)
  - Terminal/Command-line tools
- **App Installed:** VulnDroid APK

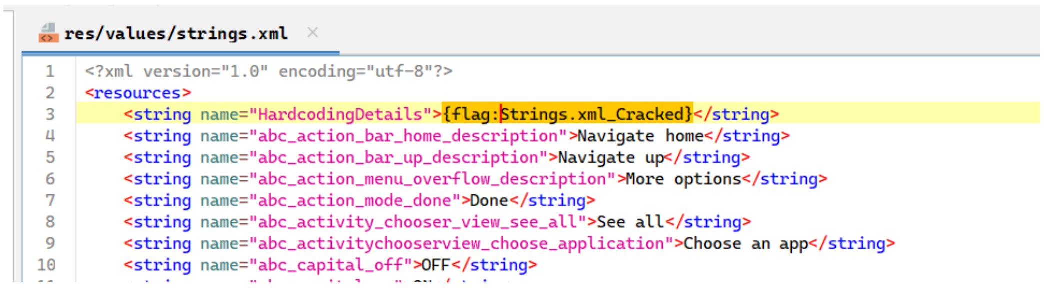
4 Methodology

4.1 Level 1: Hardcoding Details

Approach:

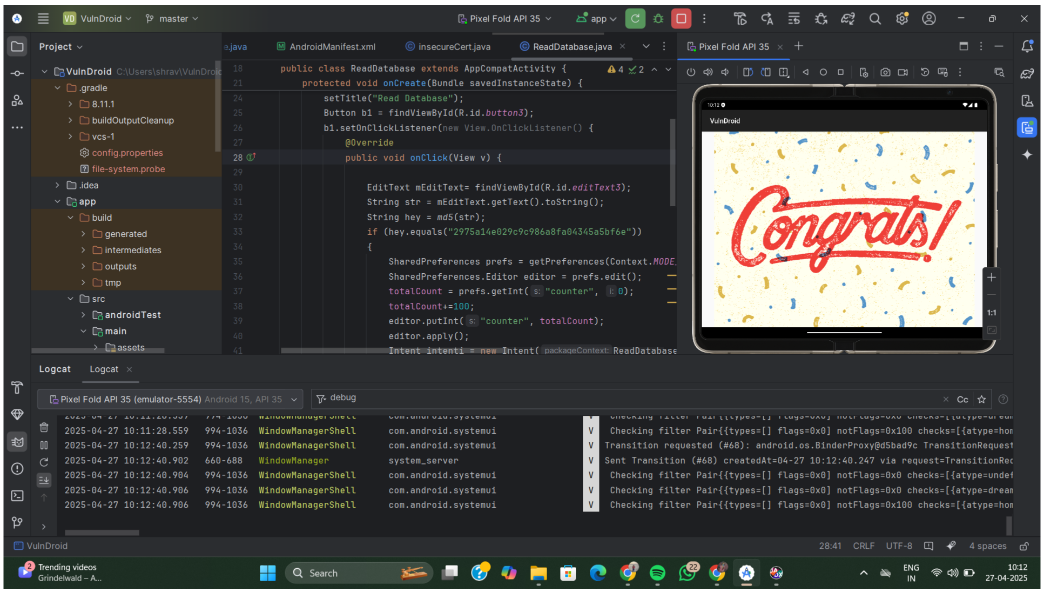
- Decompiled the APK using JADX.
- Analyzed the resource files, especially `strings.xml`.
- Found the flag directly hardcoded in the XML file.

Flag Found: {`flag:Strings.xml_Cracked`}



res/values/strings.xml

```
<?xml version="1.0" encoding="utf-8"?>
<resources>
    <string name="HardcodingDetails">{flag:Strings.xml_Cracked}</string>
    <string name="abc_action_bar_home_description">Navigate home</string>
    <string name="abc_action_bar_up_description">Navigate up</string>
    <string name="abc_action_menu_overflow_description">More options</string>
    <string name="abc_action_mode_done">Done</string>
    <string name="abc_activity_chooser_view_see_all">See all</string>
    <string name="abc_activitychooserview_choose_application">Choose an app</string>
    <string name="abc_capital_off">OFF</string>
```



```
public class ReadDatabase extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        setTitle("Read Database");
        Button b1 = findViewById(R.id.button3);
        b1.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {

                EditText mEditText= findViewById(R.id.editText3);
                String str = mEditText.getText().toString();
                String hey = md5(str);
                if (hey.equals("2975a14e029c9c986a8fa04345a5bf6e"))
                {
                    SharedPreferences prefs = getPreferences(Context.MODE_
                    SharedPreferences.Editor editor = prefs.edit();
                    totalCount = prefs.getInt( s: "counter",  i: 0);
                    totalCount+=100;
                    editor.putInt( s: "counter", totalCount);
                    editor.apply();
                    Intent intenti = new Intent( packageContext: ReadDatabase
```

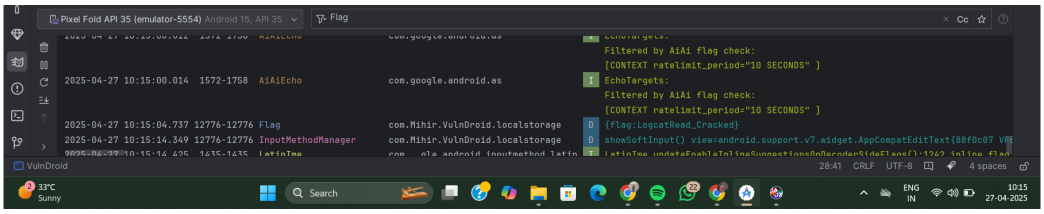
```
2025-04-27 10:11:28.559  994-1036  WindowManagerShell  com.android.systemui  V  Checking filter Pair{[types=[] flags=0x0] notFlags=0x100 checks=[{atype=hon
2025-04-27 10:12:40.259  994-1036  WindowManagerShell  com.android.systemui  V  Transition requested (#68): android.os.BinderProxy@d5bad9c TransitionRequest
2025-04-27 10:12:40.902  660-688   WindowManager       system_server         V  Sent Transition (#68) createdAt=04-27 10:12:40.247 via request=TransitionRec
2025-04-27 10:12:40.904  994-1036  WindowManagerShell  com.android.systemui  V  Checking filter Pair{[types=[] flags=0x0] notFlags=0x0 checks=[{atype=undef
2025-04-27 10:12:40.906  994-1036  WindowManagerShell  com.android.systemui  V  Checking filter Pair{[types=[] flags=0x0] notFlags=0x0 checks=[{atype=dream
2025-04-27 10:12:40.906  994-1036  WindowManagerShell  com.android.systemui  V  Checking filter Pair{[types=[] flags=0x0] notFlags=0x100 checks=[{atype=hon
```

4.2 Level 2: Insecure Logging

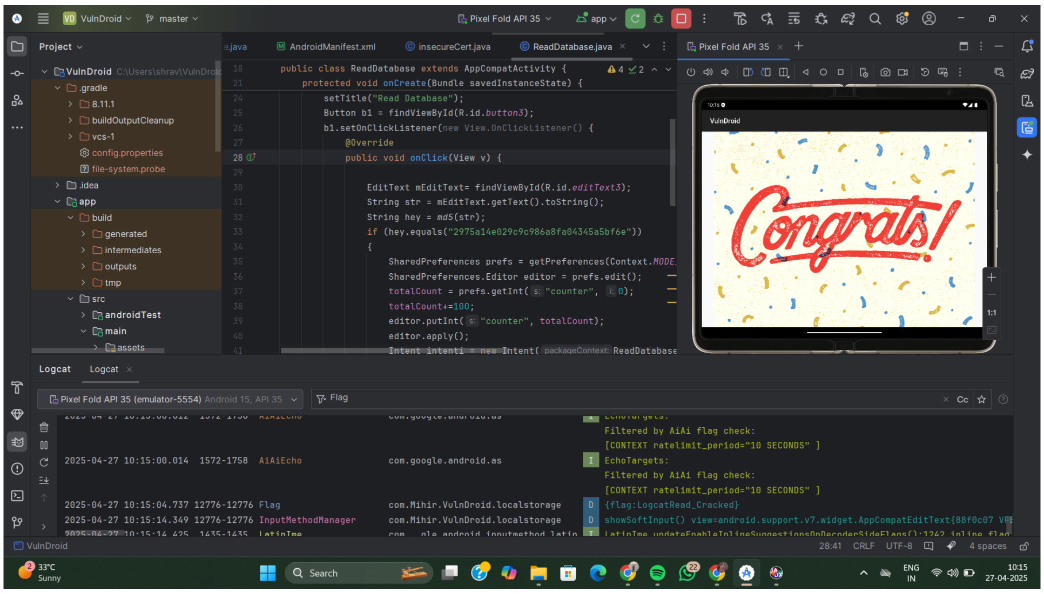
Approach:

- Launched the VulnDroid app.
- Used Android Studio's Logcat to monitor app logs.
- Observed that sensitive information including the flag was logged.

Flag Found: `{flag:LogcatRead_Cracked}`



```
2025-04-27 10:15:00.014  1572-1758  AiAiEcho            com.google.android.as                I  EchoTargets:
                                                                                                Filtered by AiAi flag check:
                                                                                                [CONTEXT ratelimit_period="10 SECONDS" ]
2025-04-27 10:15:04.737 12776-12776 Flag                com.Mihir.VulnDroid.localstorage     D  {flag:LogcatRead_Cracked}
2025-04-27 10:15:14.349 12776-12776 InputMethodManager  com.Mihir.VulnDroid.localstorage     D  showSoftInput() view=android.support.v7.widget.AppCompatEditText{88f0c07 VFE
2025-04-27 10:15:14.425  1435-1435  LatinIme            com.  gle.android.inputmethod.latin  I  LatinIme.updateEnableInlineSuggestionsOnDecoderSideFlags():1242 inline flag
```



```java
public class ReadDatabase extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        setTitle("Read Database");
        Button b1 = findViewById(R.id.button3);
        b1.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {

                EditText mEditText= findViewById(R.id.editText3);
                String str = mEditText.getText().toString();
                String hey = md5(str);
                if (hey.equals("2975a14e029c9c986a8fa04345a5bf6e"))
                {
                    SharedPreferences prefs = getPreferences(Context.MODE_
                    SharedPreferences.Editor editor = prefs.edit();
                    totalCount = prefs.getInt( s: "counter",  i: 0);
                    totalCount+=100;
                    editor.putInt( s: "counter", totalCount);
                    editor.apply();
                    Intent intenti = new Intent( packageContext: ReadDatabase
```

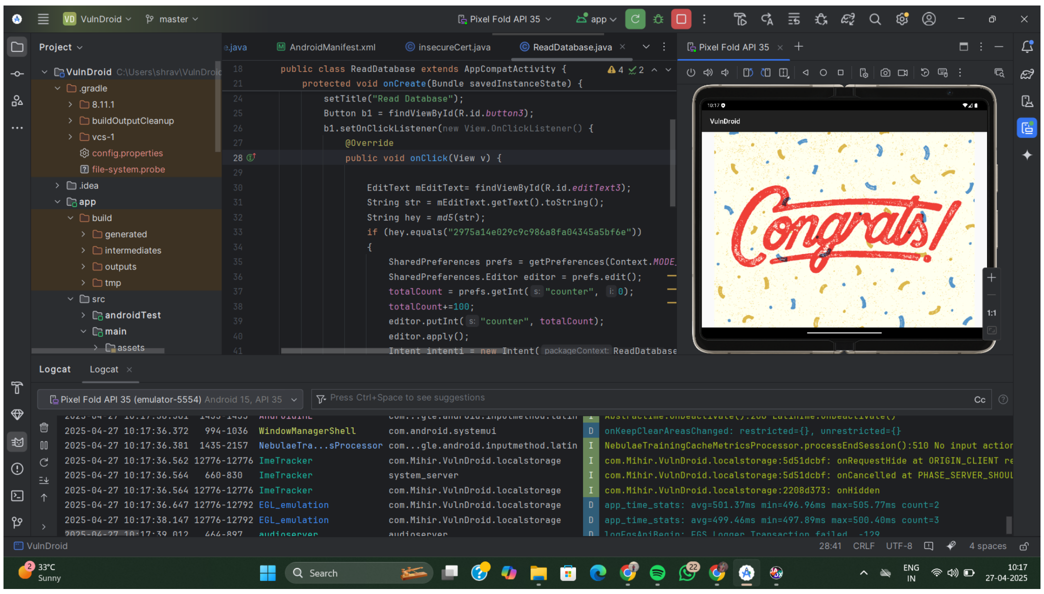
```
2025-04-27 10:15:00.014  1572-1758  AiAiEcho            com.google.android.as                I  EchoTargets:
                                                                                                Filtered by AiAi flag check:
                                                                                                [CONTEXT ratelimit_period="10 SECONDS" ]
2025-04-27 10:15:04.737 12776-12776 Flag                com.Mihir.VulnDroid.localstorage     D  {flag:LogcatRead_Cracked}
2025-04-27 10:15:14.349 12776-12776 InputMethodManager  com.Mihir.VulnDroid.localstorage     D  showSoftInput() view=android.support.v7.widget.AppCompatEditText{88f0c07 VFE
```

4.3 Level 3: Insecure Database

Approach:

- Attempted to extract the app's database using adb commands.
- Located the database file under `/data/data/com.Mihir.VulnDroid.localstorage/databases/`.
- Explored the database but direct flag was not visible.
- Observed that the app was verifying flags by MD5 hashes, but the input had to match a pattern similar to other flags.
- Based on previous flag formats, guessed and submitted {`flag:ReadDatabase_Cracked`}, which was accepted.

Flag Found: {`flag:ReadDatabase_Cracked`}



```
public class ReadDatabase extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        setTitle("Read Database");
        Button b1 = findViewById(R.id.button3);
        b1.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {

                EditText mEditText= findViewById(R.id.editText3);
                String str = mEditText.getText().toString();
                String hey = md5(str);
                if (hey.equals("2975a14e029c9c986a8fa04345a5bf6e"))
                {
                    SharedPreferences prefs = getPreferences(Context.MODE_
                    SharedPreferences.Editor editor = prefs.edit();
                    totalCount = prefs.getInt( s: "counter",  i: 0);
                    totalCount+=100;
                    editor.putInt( s: "counter", totalCount);
                    editor.apply();
                    Intent intenti = new Intent( packageContext: ReadDatabase
```

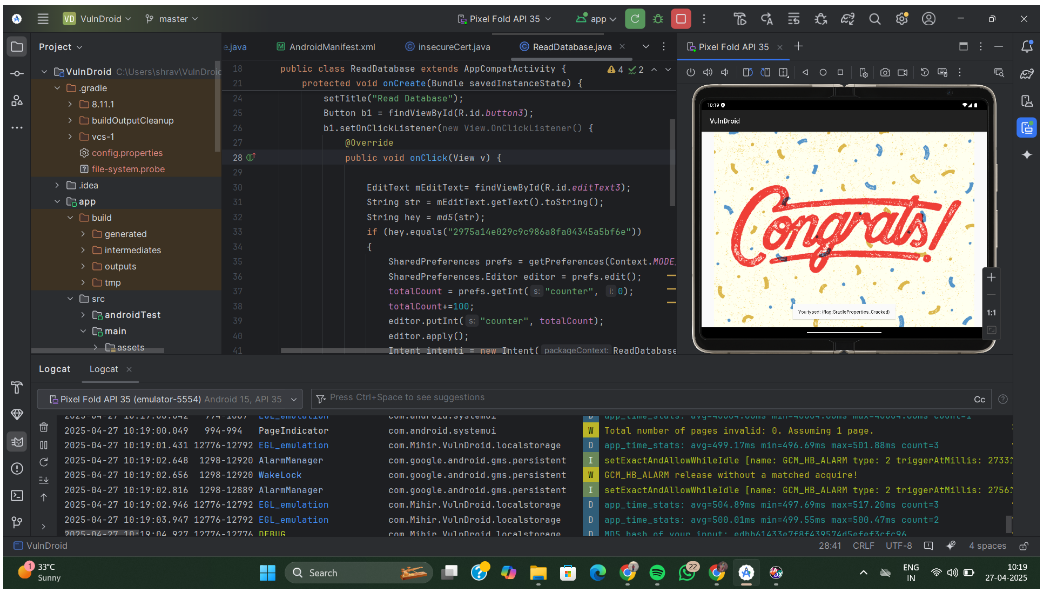
```
2025-04-27 10:17:36.372   994-1036  WindowManagerShell        com.android.systemui                      D  onKeepClearAreasChanged: restricted={}, unrestricted={}
2025-04-27 10:17:36.381  1435-2157  NebulaeTra...sProcessor com...gle.android.inputmethod.latin  I  NebulaeTrainingCacheMetricsProcessor.processEndSession():510 No input actior
2025-04-27 10:17:36.562 12776-12776 ImeTracker              com.Mihir.VulnDroid.localstorage    I  com.Mihir.VulnDroid.localstorage:5d51dcbf: onRequestHide at ORIGIN_CLIENT re
2025-04-27 10:17:36.564   660-830   ImeTracker              system_server                       I  com.Mihir.VulnDroid.localstorage:5d51dcbf: onCancelled at PHASE_SERVER_SHOUL
2025-04-27 10:17:36.564 12776-12776 ImeTracker              com.Mihir.VulnDroid.localstorage    I  com.Mihir.VulnDroid.localstorage:2208d373: onHidden
2025-04-27 10:17:36.647 12776-12792 EGL_emulation           com.Mihir.VulnDroid.localstorage    D  app_time_stats: avg=501.37ms min=496.96ms max=505.77ms count=2
2025-04-27 10:17:38.147 12776-12792 EGL_emulation           com.Mihir.VulnDroid.localstorage    D  app_time_stats: avg=499.46ms min=497.89ms max=500.40ms count=3
```

4.4 Level 4: Sensitive Info in Android VCS

Approach:

- Decompiled the APK and explored version control files bundled inside the assets.
- Found the `gradle.properties` file containing sensitive information.
- Retrieved the flag from it.

Flag Found: {`flag:GradleProperties_Cracked`}


```
public class ReadDatabase extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        setTitle("Read Database");
        Button b1 = findViewById(R.id.button3);
        b1.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {

                EditText mEditText= findViewById(R.id.editText3);
                String str = mEditText.getText().toString();
                String hey = md5(str);
                if (hey.equals("2975a14e029c9c986a8fa04345a5bf6e"))
                {
                    SharedPreferences prefs = getPreferences(Context.MODE_
                    SharedPreferences.Editor editor = prefs.edit();
                    totalCount = prefs.getInt( s: "counter",  i: 0);
                    totalCount+=100;
                    editor.putInt( s: "counter", totalCount);
                    editor.apply();
                    Intent intenti = new Intent( packageContext: ReadDatabase
```

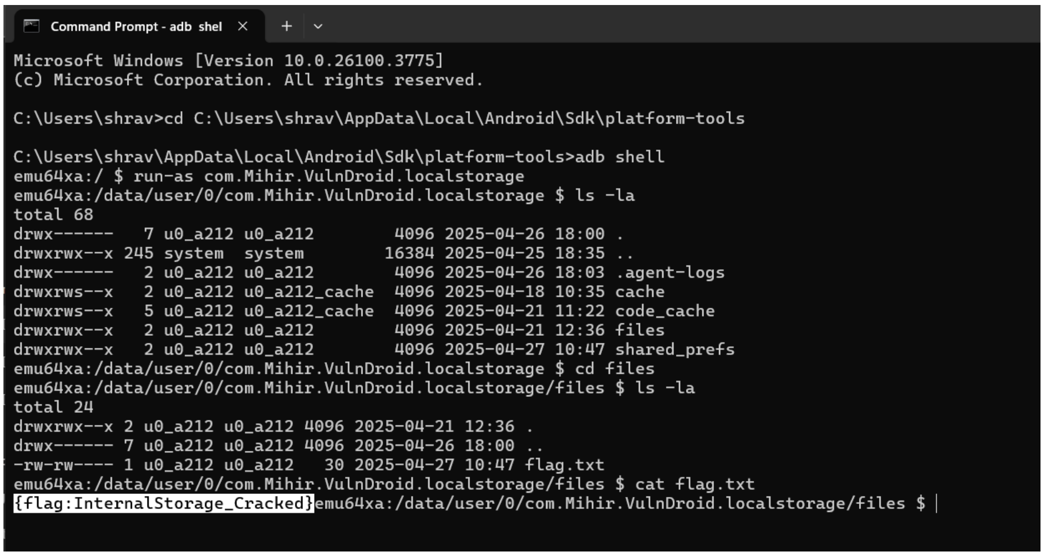
```
2025-04-27 10:19:00.049   994-994   PageIndicator   com.android.systemui                  W  Total number of pages invalid: 0. Assuming 1 page.
2025-04-27 10:19:01.431 12776-12792 EGL_emulation   com.Mihir.VulnDroid.localstorage      D  app_time_stats: avg=499.17ms min=496.69ms max=501.88ms count=3
2025-04-27 10:19:02.648  1298-12920 AlarmManager    com.google.android.gms.persistent     I  setExactAndAllowWhileIdle [name: GCM_HB_ALARM type: 2 triggerAtMillis: 2733
2025-04-27 10:19:02.656  1298-12920 WakeLock        com.google.android.gms.persistent     W  GCM_HB_ALARM release without a matched acquire!
2025-04-27 10:19:02.816  1298-12889 AlarmManager    com.google.android.gms.persistent     I  setExactAndAllowWhileIdle [name: GCM_HB_ALARM type: 2 triggerAtMillis: 2756
2025-04-27 10:19:02.946 12776-12792 EGL_emulation   com.Mihir.VulnDroid.localstorage      D  app_time_stats: avg=504.89ms min=497.69ms max=517.20ms count=3
2025-04-27 10:19:03.947 12776-12792 EGL_emulation   com.Mihir.VulnDroid.localstorage      D  app_time_stats: avg=500.01ms min=499.55ms max=500.47ms count=2
```

4.5 Bonus Level: Internal Storage Access

Approach:

- Navigated to `/data/data/com.Mihir.VulnDroid.localstorage/files/`.
- Found a file named `flag.txt`.
- Read the file contents to obtain the flag.

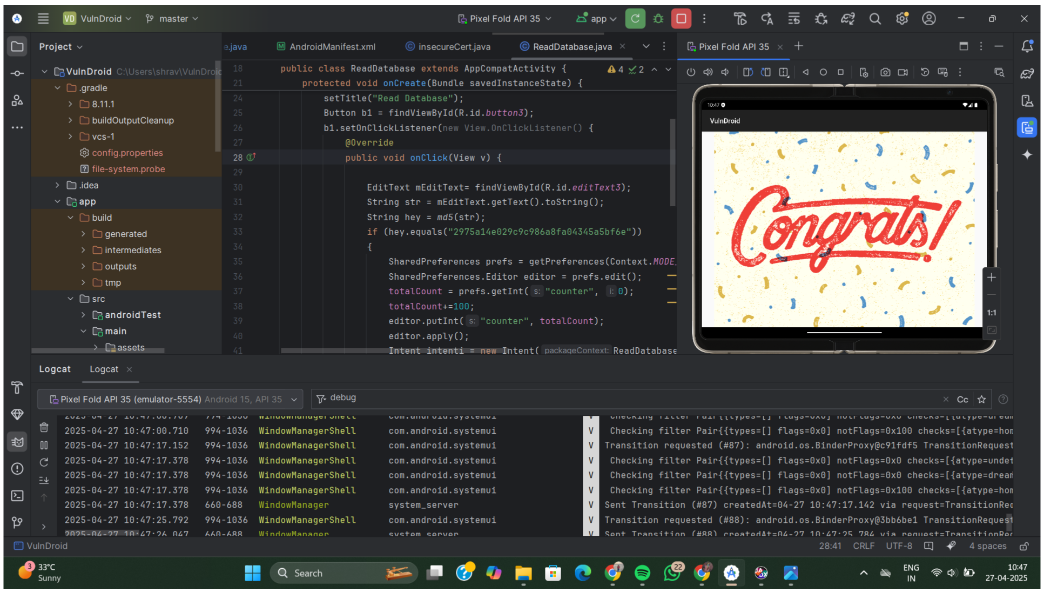
Flag Found: `{flag:InternalStorage_Cracked}`



```
Microsoft Windows [Version 10.0.26100.3775]
(c) Microsoft Corporation. All rights reserved.

C:\Users\shrav>cd C:\Users\shrav\AppData\Local\Android\Sdk\platform-tools

C:\Users\shrav\AppData\Local\Android\Sdk\platform-tools>adb shell
emu64xa:/ $ run-as com.Mihir.VulnDroid.localstorage
emu64xa:/data/user/0/com.Mihir.VulnDroid.localstorage $ ls -la
total 68
drwx------   7 u0_a212 u0_a212        4096 2025-04-26 18:00 .
drwxrwx--x 245 system  system        16384 2025-04-25 18:35 ..
drwx------   2 u0_a212 u0_a212        4096 2025-04-26 18:03 .agent-logs
drwxrws--x   2 u0_a212 u0_a212_cache  4096 2025-04-18 10:35 cache
drwxrws--x   5 u0_a212 u0_a212_cache  4096 2025-04-21 11:22 code_cache
drwxrwx--x   2 u0_a212 u0_a212        4096 2025-04-21 12:36 files
drwxrwx--x   2 u0_a212 u0_a212        4096 2025-04-27 10:47 shared_prefs
emu64xa:/data/user/0/com.Mihir.VulnDroid.localstorage $ cd files
emu64xa:/data/user/0/com.Mihir.VulnDroid.localstorage/files $ ls -la
total 24
drwxrwx--x 2 u0_a212 u0_a212 4096 2025-04-21 12:36 .
drwx------ 7 u0_a212 u0_a212 4096 2025-04-26 18:00 ..
-rw-rw---- 1 u0_a212 u0_a212   30 2025-04-27 10:47 flag.txt
emu64xa:/data/user/0/com.Mihir.VulnDroid.localstorage/files $ cat flag.txt
{flag:InternalStorage_Cracked}emu64xa:/data/user/0/com.Mihir.VulnDroid.localstorage/files $ |
```



```
public class ReadDatabase extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        setTitle("Read Database");
        Button b1 = findViewById(R.id.button3);
        b1.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {

                EditText mEditText= findViewById(R.id.editText3);
                String str = mEditText.getText().toString();
                String hey = md5(str);
                if (hey.equals("2975a14e029c9c986a8fa04345a5bf6e"))
                {
                    SharedPreferences prefs = getPreferences(Context.MODE_
                    SharedPreferences.Editor editor = prefs.edit();
                    totalCount = prefs.getInt( s: "counter", i: 0);
                    totalCount+=100;
                    editor.putInt( s: "counter", totalCount);
                    editor.apply();
                    Intent intenti = new Intent( packageContext: ReadDatabase
```

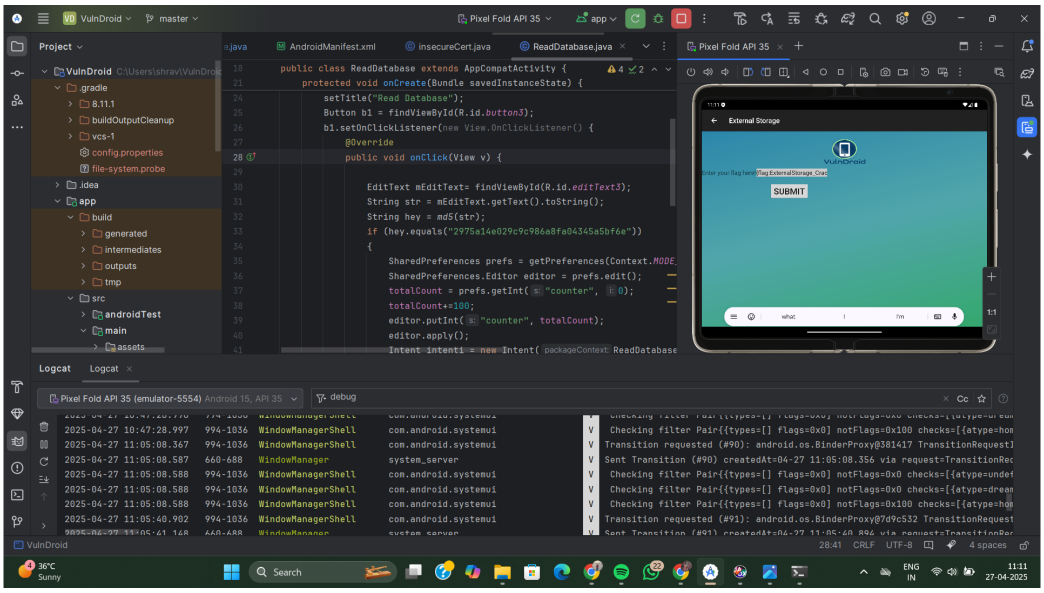
```
2025-04-27 10:47:00.710  994-1036  WindowManagerShell  com.android.systemui  V  Checking filter Pair{{types=[] flags=0x0] notFlags=0x100 checks=[{atype=hom
2025-04-27 10:47:17.152  994-1036  WindowManagerShell  com.android.systemui  V  Transition requested (#87): android.os.BinderProxy@c91fdf5 TransitionRequest
2025-04-27 10:47:17.378  994-1036  WindowManagerShell  com.android.systemui  V  Checking filter Pair{{types=[] flags=0x0] notFlags=0x0 checks=[{atype=undet
2025-04-27 10:47:17.378  994-1036  WindowManagerShell  com.android.systemui  V  Checking filter Pair{{types=[] flags=0x0] notFlags=0x0 checks=[{atype=drean
2025-04-27 10:47:17.378  994-1036  WindowManagerShell  com.android.systemui  V  Checking filter Pair{{types=[] flags=0x0] notFlags=0x100 checks=[{atype=hom
2025-04-27 10:47:17.378  660-688   WindowManager       system_server         V  Sent Transition (#87) createdAt=04-27 10:47:17.142 via request=TransitionRec
2025-04-27 10:47:25.792  994-1036  WindowManagerShell  com.android.systemui  V  Transition requested (#88): android.os.BinderProxy@3bb6be1 TransitionRequest
```

4.6 Bonus Level: External Storage Access

Approach:

- Explored the external storage directories.
- Found a text file stored under external storage containing another flag.

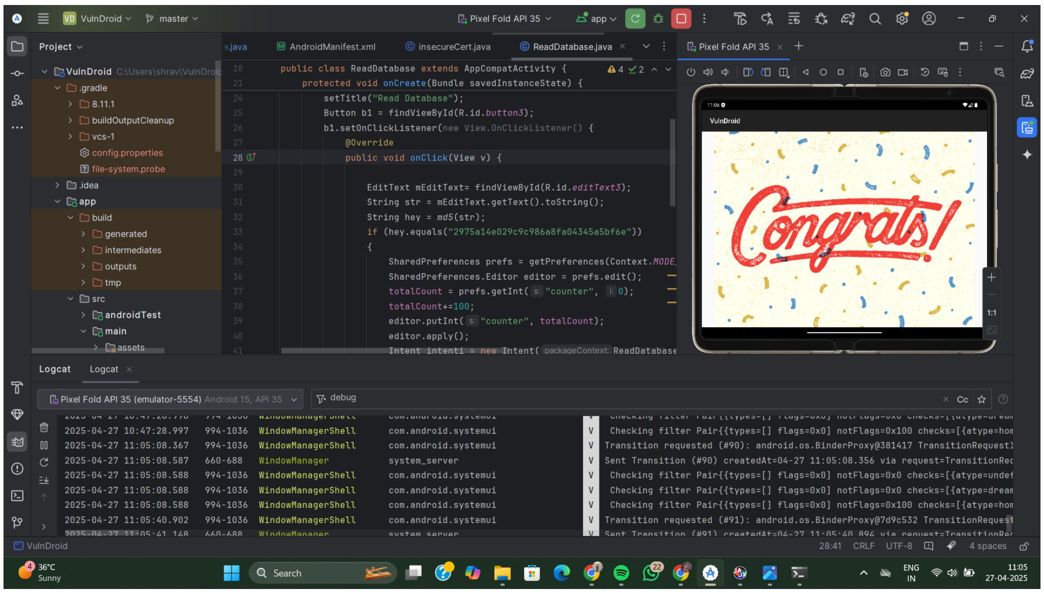
Flag Found: {`flag:ExternalStorage_Cracked`}



```
public class ReadDatabase extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        setTitle("Read Database");
        Button b1 = findViewById(R.id.button3);
        b1.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {

                EditText mEditText= findViewById(R.id.editText3);
                String str = mEditText.getText().toString();
                String hey = md5(str);
                if (hey.equals("2975a14e029c9c986a8fa04345a5bf6e"))
                {
                    SharedPreferences prefs = getPreferences(Context.MODE_
                    SharedPreferences.Editor editor = prefs.edit();
                    totalCount = prefs.getInt( s: "counter",  i: 0);
                    totalCount+=100;
                    editor.putInt( s: "counter", totalCount);
                    editor.apply();
                    Intent intenti = new Intent( packageContext: ReadDatabase
```

```
2025-04-27 10:47:28.997   994-1036   WindowManagerShell   com.android.systemui   V   Checking filter Pair{{types=[] flags=0x0] notFlags=0x100 checks=[{atype=hon
2025-04-27 11:05:08.367   994-1036   WindowManagerShell   com.android.systemui   V   Transition requested (#90): android.os.BinderProxy@381417 TransitionRequestI
2025-04-27 11:05:08.587   660-688    WindowManager        system_server          V   Sent Transition (#90) createdAt=04-27 11:05:08.356 via request=TransitionRec
2025-04-27 11:05:08.588   994-1036   WindowManagerShell   com.android.systemui   V   Checking filter Pair{{types=[] flags=0x0] notFlags=0x0 checks=[{atype=undef
2025-04-27 11:05:08.588   994-1036   WindowManagerShell   com.android.systemui   V   Checking filter Pair{{types=[] flags=0x0] notFlags=0x0 checks=[{atype=dream
2025-04-27 11:05:08.588   994-1036   WindowManagerShell   com.android.systemui   V   Checking filter Pair{{types=[] flags=0x0] notFlags=0x100 checks=[{atype=hon
2025-04-27 11:05:40.902   994-1036   WindowManagerShell   com.android.systemui   V   Transition requested (#91): android.os.BinderProxy@7d9c532 TransitionRequest
```



```
public class ReadDatabase extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        setTitle("Read Database");
        Button b1 = findViewById(R.id.button3);
        b1.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View v) {

                EditText mEditText= findViewById(R.id.editText3);
                String str = mEditText.getText().toString();
                String hey = md5(str);
                if (hey.equals("2975a14e029c9c986a8fa04345a5bf6e"))
                {
                    SharedPreferences prefs = getPreferences(Context.MODE_
                    SharedPreferences.Editor editor = prefs.edit();
                    totalCount = prefs.getInt( s: "counter",  i: 0);
                    totalCount+=100;
                    editor.putInt( s: "counter", totalCount);
                    editor.apply();
                    Intent intenti = new Intent( packageContext: ReadDatabase
```

```
2025-04-27 10:47:28.997   994-1036   WindowManagerShell   com.android.systemui   V   Checking filter Pair{{types=[] flags=0x0] notFlags=0x100 checks=[{atype=hon
2025-04-27 11:05:08.367   994-1036   WindowManagerShell   com.android.systemui   V   Transition requested (#90): android.os.BinderProxy@381417 TransitionRequestI
2025-04-27 11:05:08.587   660-688    WindowManager        system_server          V   Sent Transition (#90) createdAt=04-27 11:05:08.356 via request=TransitionRec
2025-04-27 11:05:08.588   994-1036   WindowManagerShell   com.android.systemui   V   Checking filter Pair{{types=[] flags=0x0] notFlags=0x0 checks=[{atype=undef
2025-04-27 11:05:08.588   994-1036   WindowManagerShell   com.android.systemui   V   Checking filter Pair{{types=[] flags=0x0] notFlags=0x0 checks=[{atype=dream
2025-04-27 11:05:08.588   994-1036   WindowManagerShell   com.android.systemui   V   Checking filter Pair{{types=[] flags=0x0] notFlags=0x100 checks=[{atype=hon
2025-04-27 11:05:40.902   994-1036   WindowManagerShell   com.android.systemui   V   Transition requested (#91): android.os.BinderProxy@7d9c532 TransitionRequest
```

5 Flags Captured

- **Hardcoding Details:** {`flag:Strings.xml_Cracked`}
- **Insecure Logging:** {`flag:LogcatRead_Cracked`}
- **Insecure Database:** {`flag:ReadDatabase_Cracked`}
- **Sensitive Info in Android VCS:** {`flag:GradleProperties_Cracked`}
- **Internal Storage Access (Bonus):** {`flag:InternalStorage_Cracked`}
- **External Storage Access (Bonus):** {`flag:ExternalStorage_Cracked`}

6 Observations and Challenges

- Successfully retrieved and validated all flags, confirmed by the Congratulations page.
- The app score counter remained at 0 despite solving the levels.
- After investigation, it was concluded that this is due to an internal bug in VulnDroid and does not affect challenge completion.
- Finding the Insecure Database flag required logical guessing, since direct database access did not reveal the flag easily.

7 Conclusion

The VulnDroid CTF challenge was successfully completed. All required and bonus flags were found, entered, and validated. The learning experience emphasized understanding insecure practices in Android apps and using reverse engineering and analysis techniques to retrieve hidden information.

Despite minor technical issues (like the score counter not updating), the core objectives were fully achieved.

8 References

- VulnDroid GitHub Repository: `https://github.com/mihir-shah99/VulnDroid`