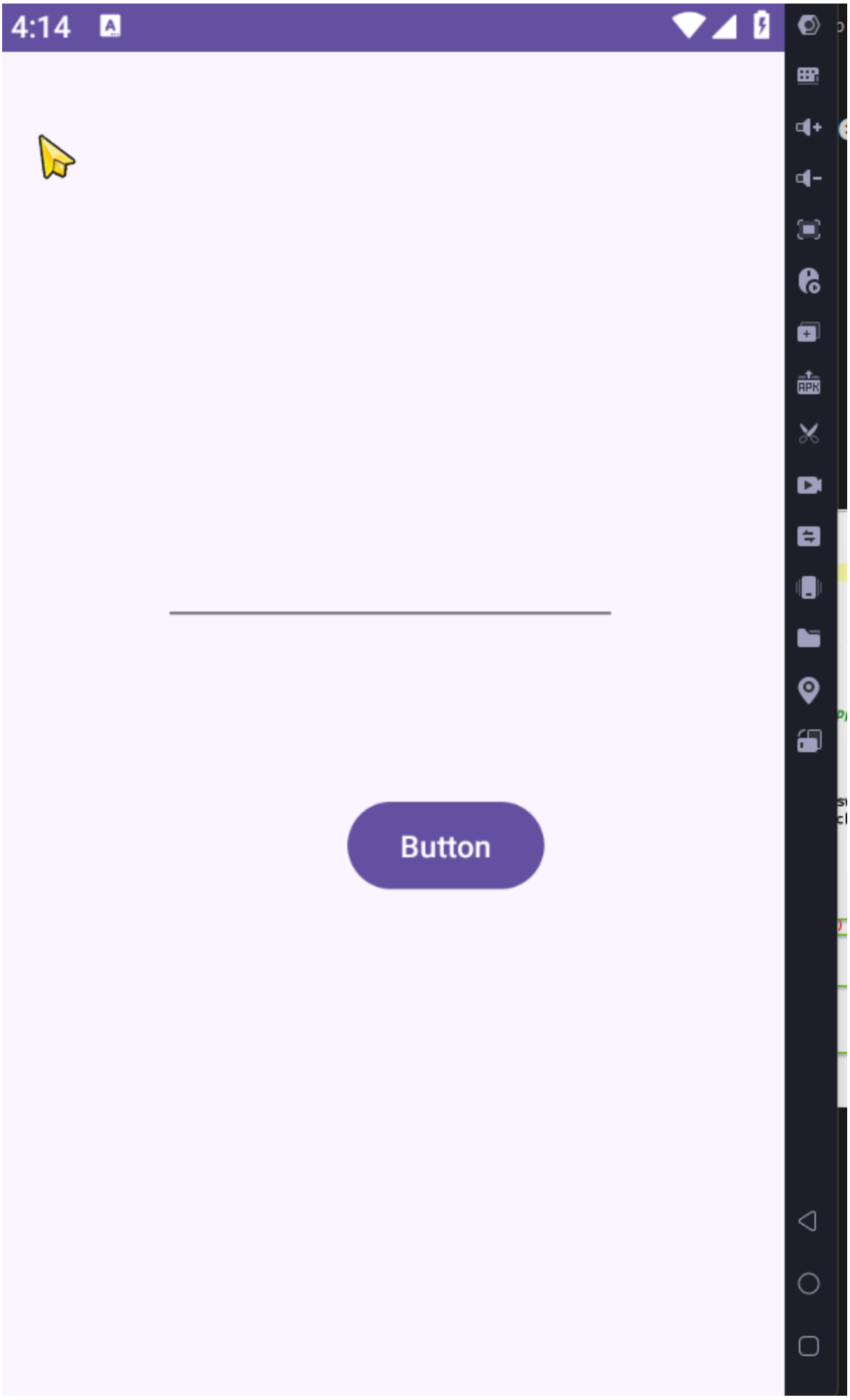
Arab War Games Double Trouble challenge write up

Start by running the application


4:14
Button

Started by analyzing the manifest file

```
<activity
    android:name="com.hacking.test.MainActivity"
    android:exported="true">
    <intent-filter>
        <action android:name="android.intent.action.MAIN"/>
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
</activity>
<activity
    android:name="com.hacking.test.SecondActivity"
    android:exported="false"/>
<activity
    android:theme="@style/WhiteBackgroundTheme"
    android:name="androidx.test.core.app.InstrumentationActivityInvoker$BootstrapActivity"
    android:exported="true">
    <intent-filter android:priority="-100">
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
</activity>
<activity
    android:theme="@style/WhiteBackgroundTheme"
    android:name="androidx.test.core.app.InstrumentationActivityInvoker$EmptyActivity"
    android:exported="true">
    <intent-filter android:priority="-100">
        <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
</activity>
<activity
    android:theme="@style/WhiteBackgroundDialogTheme"
    android:name="androidx.test.core.app.InstrumentationActivityInvoker$EmptyFloatingActivity"
    android:exported="true">
```

the only unexported activity was the second activity so i though the idea is to invoke the activity from the application's context i checked the other instrumentation activities to see if there is a way like intent redirection or pending intent i can use but found nothing and said ok maybe these activities are the decoy part of the challenge so lets focus on the main activity and the second activity and when i saw that the second activity is checking the value from_password which only set in the main activity i knew i was supposed to use the main activity's intent to start the second activity

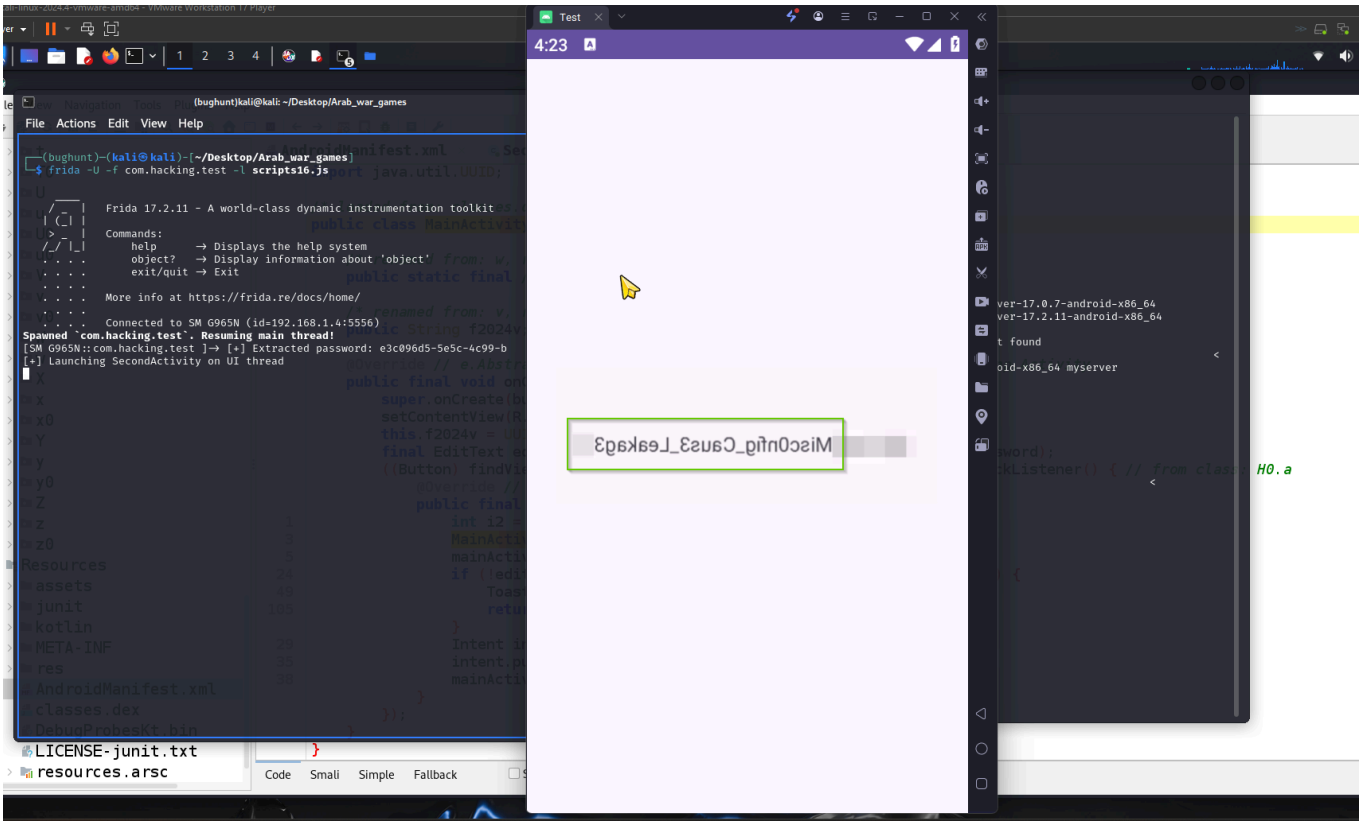
Start to analyze the source code

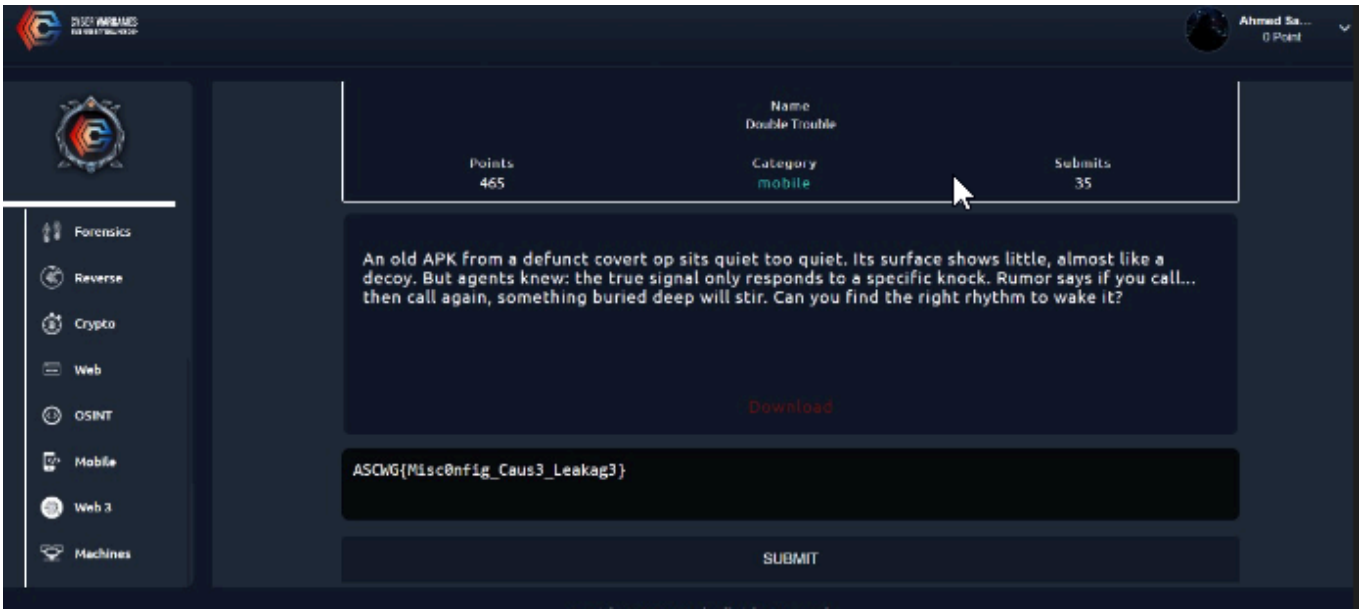
```java
import java.util.UUID;

/* loaded from: classes.dex */
public class MainActivity extends AbstractActivityC0119i {

    /* renamed from: w, reason: collision with root package name */
    public static final /* synthetic */ int f2023w = 0;

    /* renamed from: v, reason: collision with root package name */
    public String f2024v;

    @Override // e.AbstractActivityC0119i, androidx.activity.k, y.f, android.app.Activity
    public final void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        setContentView(R.layout.activity_main);
        this.f2024v = UUID.randomUUID().toString().substring(0, 20);
        final EditText editText = (EditText) findViewById(R.id.editTextTextPassword);
        ((Button) findViewById(R.id.button)).setOnClickListener(new View.OnClickListener() { // from class: H0.
            @Override // android.view.View.OnClickListener
            public final void onClick(View view) {
                int i2 = MainActivity.f2023w;
                MainActivity mainActivity = MainActivity.this;
                mainActivity.getClass();
                if (!editText.getText().toString().equals(mainActivity.f2024v)) {
                    Toast.makeText(mainActivity, "Wrong password", 0).show();
                    return;
                }
                Intent intent = new Intent(mainActivity, (Class<?>) null);
                intent.putExtra("from_password", true);
                mainActivity.startActivity(intent);
            }
        });
    }
}
```

main activity is generating a 20 character password and compares it to the user's input
if equal create an intent and add an extra from_password with value true if not print wrong password

So the idea is Hooking the main activity and capture the generated password and use it to login

The thing is -> even if you captured the password and passed it , the application will crash and frida logs will say there is null pointer exception
and the reason is that the developer wrote this app is creating the intent with null class
so i wrote a script to :
Hook the main activity
extract the password
write this password in the edit text automatically
overwrote the intent creation and specified the class name of the second activity





Frida script i used :

```
  Java.perform(function () {
    var MainActivity = Java.use("com.hacking.test.MainActivity");
    var SecondActivity = Java.use("com.hacking.test.SecondActivity");
    var Intent = Java.use("android.content.Intent");
    var EditText = Java.use("android.widget.EditText");
    var BufferType = Java.use("android.widget.TextView$BufferType");
    var JavaString = Java.use("java.lang.String");

    MainActivity.onCreate.overload("android.os.Bundle").implementation = function (bundle) {
        this.onCreate(bundle);

        var activity = this;

        try {
            // Extract the password from field "v"
            var cls = Java.use("java.lang.Class").forName("com.hacking.test.MainActivity");
            var field = cls.getDeclaredField("v");
            field.setAccessible(true);
            var password = field.get(activity);
            console.log("[+] Extracted password: " + password);

            // Fill the password into EditText
            var editText = Java.cast(
                activity.findViewById(activity.getResources().getIdentifier("editTextTextPassword", "id",
activity.getPackageName())),
                EditText
            );

            editText.setText.overload('java.lang.CharSequence', 'android.widget.TextView$BufferType')
                .call(editText, JavaString.$new(password), BufferType.NORMAL.value);

            // Start the SecondActivity on the main (UI) thread
            activity.runOnUiThread(Java.registerClass({
                name: 'com.hacking.test.FakeRunnable',
                implements: [Java.use('java.lang.Runnable')],
                methods: {
                    run: function () {
                        try {
                            console.log("[+] Launching SecondActivity on UI thread");

                            var intent = Intent.$new(activity, SecondActivity.class);
                            intent.putExtra("from_password", true);
                            activity.startActivity(intent);
                        } catch (e) {
                            console.error("[-] Failed in Runnable: " + e);
                        }
                    }
                }
            }).$new());

        } catch (err) {
            console.error("[-] Hooking failed: " + err);
        }
    };
});
```