

# Insecure Logging

# Introduction

- Some Android apps store their logs insecurely, potentially exposing sensitive information.
- Insecure logging is a common security issue that needs to be addressed.
- Insecure logging can lead to significant security vulnerabilities. Sensitive information, such as passwords, personal data, or API keys, should never be included in logs. This kind of data should be handled with caution and should not appear in plain text in logs.

# Practical Demonstration

## Part 1: Identifying Insecure Logs in Diva APK

- Begin by connecting to your Android device using ADB:

```
adb connect [device_ip]
```

- Next, we need to find the process ID (PID) of the Diva APK using the following command:

```
adb shell ps | grep diva
```

- Now, we'll use ADB to access the logcat for the specific process:

```
adb logcat | grep [PID]
```

- You will see all the logs generated by the Diva APK, including insecure logging.
- Interact with the app, perform actions, and notice that logs are generated in real-time.
- Enter credit card detail in application
- When we scroll down, we see that our credit card number has been logged. BAD LOGCAT! Now we know how it is being logged, via the LogCat Output in Android Studio underneath a log labeled diva-log.

```
E diva-log: Error while processing transaction with credit card: 123456789
```

## Part 2: Finding Vulnerable Code

- To find the vulnerable code within the Diva APK, we'll use jadx-gui or a similar decompilation tool.
- Open jadx-gui and load the Diva APK to decompile it.
- Within the decompiled source code, look for a class named "LogActivity."
- Examine the code within "LogActivity" to identify insecure logging practices.

```
public void checkout(View view) {  
    EditText cctxt = (EditText) findViewById(R.id.ccText);  
    try {  
        processCC(cctxt.getText().toString());  
    } catch (RuntimeException e) {  
        Log.e("diva-log", "Error while processing transaction with credit card: " + cctxt.getText().toString());  
        Toast.makeText(this, "An error occurred. Please try again later", 0).show();  
    }  
}  
  
private void processCC(String ccstr) {  
    RuntimeException e = new RuntimeException();  
    throw e;  
}
```

When we look at the code, we can identify the section where it does the actual logging, thus confirming that it is logging our credit card number.