



# Android Application Penetration Testing

Raja Nagori

# Static Analysis

# Android manifest file

- Extension is .xml
- You'll get basic information about the application
  - SDK version
  - Permission
  - Activities
  - Content Providers
  - Intent

# Permission

- Doesn't have any extension unfortunately 😞
- It defines what data and hardware component can be need at the runtime
  - Camera
  - Internet
  - Access external storage
  - Bluetooth
  - ETC.

- It also do not have any extension too 🙄
- UI element of the application or different screen in the application.

(take example of Gpay)

- First screen will show you Gpay Logo.
- Second will ask you the Fingerprint.
- Third will display all the payment you did in past.

## Activities

NOTE: 1. Here **INTENT** is changing from one screen to other.

2. If you see exported="True"

# Finding Hardcoded Strings

- Usually find in resources/strings.xml
- Threat Vector
  - Login Bypass
  - URL's Exposed
  - API Keys Exposed
  - Firebase URL's

See you on next chapter of this series

