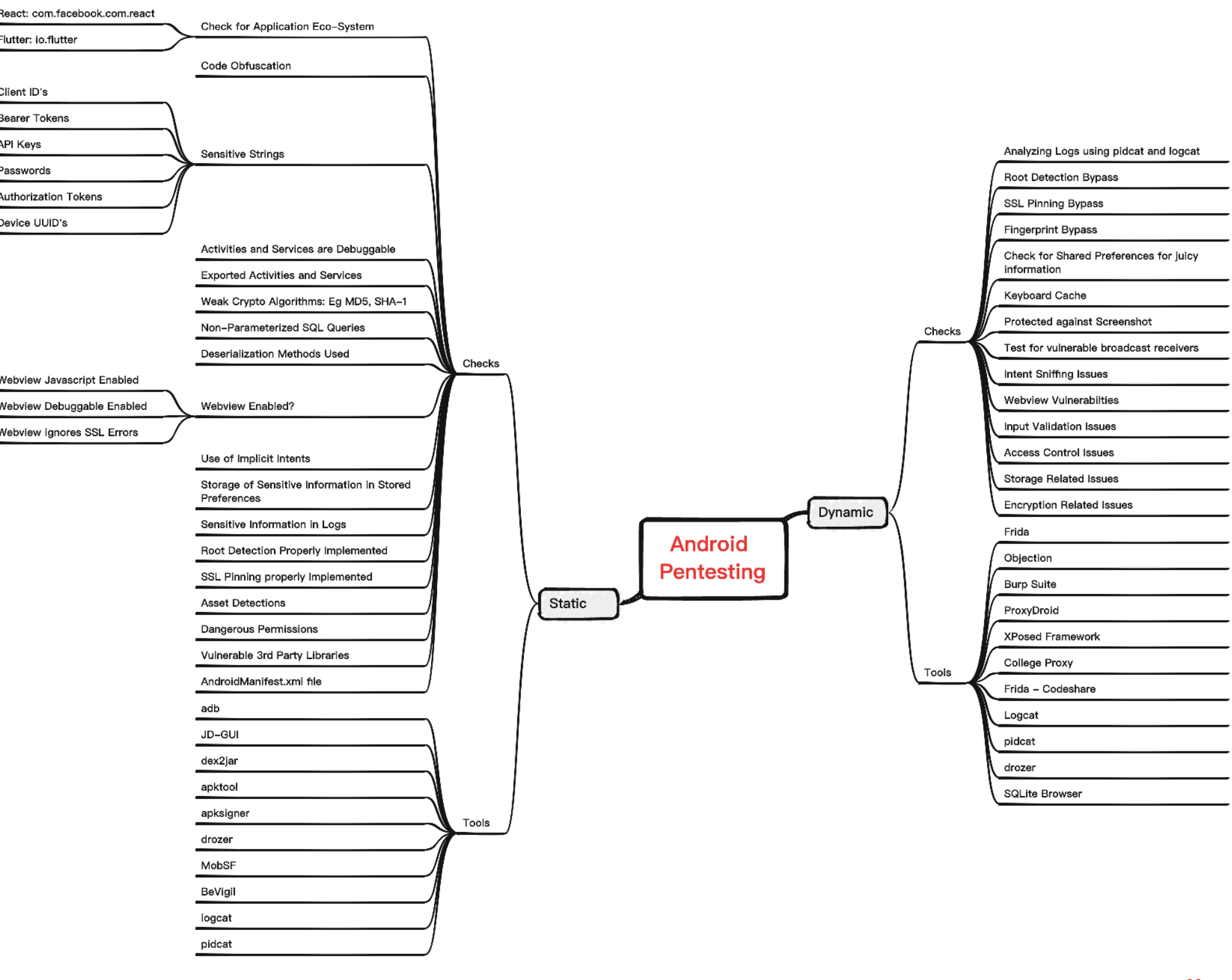
Android Pentesting
Static
Checks
Check for Application Eco-System
React: com.facebook.com.react
Flutter: io.flutter
Code Obfuscation
Sensitive Strings
Client ID's
Bearer Tokens
API Keys
Passwords
Authorization Tokens
Device UUID's
Activities and Services are Debuggable
Exported Activities and Services
Weak Crypto Algorithms: Eg MD5, SHA-1
Non-Parameterized SQL Queries
Deserialization Methods Used
Webview Enabled?
Webview Javascript Enabled
Webview Debuggable Enabled
Webview ignores SSL Errors
Use of Implicit Intents
Storage of Sensitive Information in Stored Preferences
Sensitive Information in Logs
Root Detection Properly Implemented
SSL Pinning properly Implemented
Asset Detections
Dangerous Permissions
Vulnerable 3rd Party Libraries
AndroidManifest.xml file
Tools
adb
JD-GUI
dex2jar
apktool
apksigner
drozer
MobSF
BeVigil
logcat
pidcat
Dynamic
Checks
Analyzing Logs using pidcat and logcat
Root Detection Bypass
SSL Pinning Bypass
Fingerprint Bypass
Check for Shared Preferences for juicy information
Keyboard Cache
Protected against Screenshot
Test for vulnerable broadcast receivers
Intent Sniffing Issues
Webview Vulnerabilties
Input Validation Issues
Access Control Issues
Storage Related Issues
Encryption Related Issues
Tools
Frida
Objection
Burp Suite
ProxyDroid
XPosed Framework
College Proxy
Frida - Codeshare
Logcat
pidcat
drozer
SQLite Browser