

>./DurianAndroid



Group 17 Android Application Security Inspection Helper

Information

>./Objectives

- + To build a tool that can help security testers performing a basic security assessment on any Android application
- + To help mobile security testers skip common tasks when testing Android applications

>./Users



Security testers/Ethical hackers

Development

>./Softwares



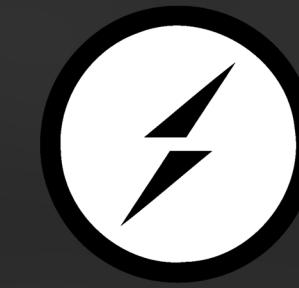
Vue.js



Koa

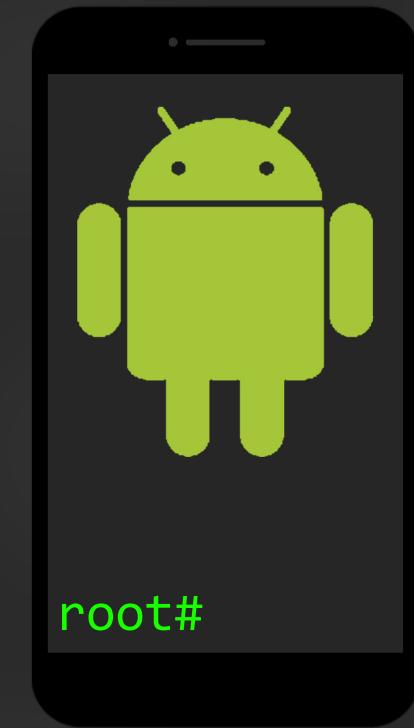


frida



Socket.io

>./Requirements



+ Frida Rooted Android device with frida-server installed

Features

>./Features

- + List all permissions that the application requested
- + Modify how the application works
- + Inspect data in the application
- + Inspect the application log
- + Run custom scripts on the application

Result

+ List all permissions

Info

package name: com.google.android.youtube

version: 13.15.61

SDK version: min: 21 target: 28

Permissions

- android.permission.INTERNET
- android.permission.ACCESS_NETWORK_STATE
- android.permission.ACCESS_WIFI_STATE
- android.permission.WRITE_EXTERNAL_STORAGE
- android.permission.RECEIVE_BOOT_COMPLETED
- android.permission.MANAGE_DOCUMENTS

+ Inspect application data

INFO CLASS FILE CODERUNNER LOCATION

Loaded: ALL HOOK_METHOD MODIFY_METHOD CLASS

01:31:33 com.pamu.d hook_method arg0 string: "pwn comment"

(Android Emulator 5554) # CLEAR

+ Modify how application works

a Modify method

Parameters

Modify parameters?

checkbox checked boolean new value: true

Return value

checkbox unchecked Return type: String input value: true

+ Inspect the application log

YouTube

com.google.android.youtube (pid: 12163)

INFO CLASS FILE CODERUNNER LOGCAT

Application Logs

Show datetime

Logcat

Unexpected CPU variant for X86 using defaults: x86_64

The ClassLoaderContext is a special shared library.

: Fetching the Gservices key 'dalvik.clear_cache_release_13_02' before the end of the bulk initialization

: Fetching the Gservices key 'diable_binder_callback_flush' before the end of the bulk initialization

: flushBindConnectionCallbacks is unverified on SDK 28

Advisor

Asst. Prof. Dr.

Marong Phadoongsidhi

Developer

Mr.

Puwit Yahom 59070501059