FRIDA🎅

BINARY INSTRUMENTATION VIA FUNCTION HOOKING

WHAT WE'LL COVER

WHAT WE'LL COVER

1. Hooking use cases

WHAT WE'LL COVER

1. Hooking use cases
2. Tool of choice

WHAT WE'LL COVER

1. Hooking use cases
2. Tool of choice
3. Demo

HOOKING USE CASES🎅🏻

HOOKING USE CASES?🎅🏼

- insert logging (like print debugging)

HOOKING USE CASES?🎅🏽

HOOKING USE CASES?🎅🏽

- change code logic

HOOKING USE CASES?🎅

- change code logic
    - via parameters

HOOKING USE CASES?🎅🏽

- change code logic
  - via parameters
  - function calls

HOOKING USE CASES?🎅🏽

- change code logic
  - via parameters
  - function calls
  - etc.

HOOKING USE CASES?🎅🏾

- sniff network traffic (e.g. by hooking functions which write on the wire)

HOOKING USE CASES?🎅🏿

- bypass protections (in creative ways)

TOOL OF CHOICE - FRIDA🤶🏾

TOOL OF CHOICE - FRIDA🤶🏿

- instrumentation toolkit for native apps

TOOL OF CHOICE - FRIDA🤶🏾

- instrumentation toolkit for native apps
- scriptable with JavaScript !!

TOOL OF CHOICE - FRIDA🤶🏾

- instrumentation toolkit for native apps
- scriptable with JavaScript !!
- supports multiple platforms

TOOL OF CHOICE - FRIDA🤶🏾

- instrumentation toolkit for native apps
- scriptable with JavaScript !!
- supports multiple platforms
  - i.e. Windows, Linux, Mac, Android, IOS

TOOL OF CHOICE - FRIDA🤶🏿

- instrumentation toolkit for native apps
- scriptable with JavaScript !!
- supports multiple platforms
  - i.e. Windows, Linux, Mac, Android, IOS
- paired with a set of powerful tools

TOOL OF CHOICE - FRIDA🤶🏾

- instrumentation toolkit for native apps
- scriptable with JavaScript !!
- supports multiple platforms
    - i.e. Windows, Linux, Mac, Android, IOS
- paired with a set of powerful tools
- free and open source

DEMO - LINUX🤶🏾

DEMO - LINUX🤶🏽

DEMO - LINUX🤶🏽

1. Insert debugging calls

DEMO - LINUX🤶🏽

1. Insert debugging calls
2. Hot-Reload

DEMO - LINUX🤶🏽

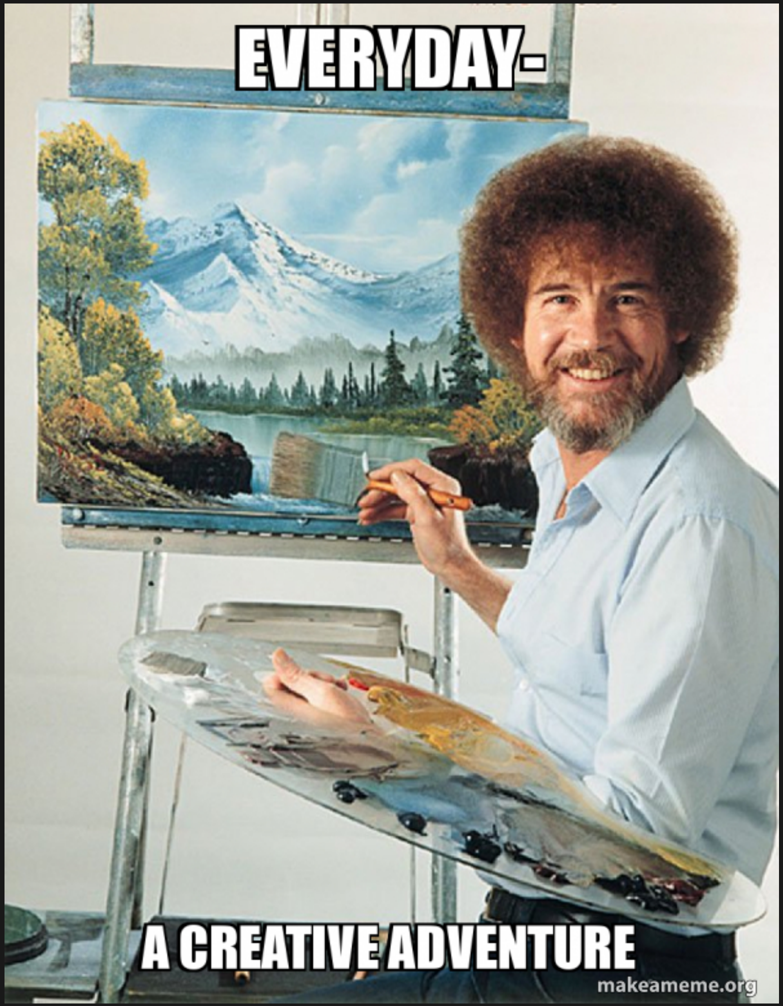
1. Insert debugging calls
2. Hot-Reload
3. Change function's parameters

DEMO - LINUX🤶🏽

1. Insert debugging calls
2. Hot-Reload
3. Change function's parameters
4. Change function behaviour

DEMO - LINUX🤶🏽

1. Insert debugging calls
2. Hot-Reload
3. Change function's parameters
4. Change function behaviour
5. Call a declared function


EVERYDAY-
A CREATIVE ADVENTURE
makeameme.org

DEMO - ANDROID🤶🏼

DEMO - ANDROID🎅🏻

DEMO - ANDROID🎅🏻

1. Change the return value of a function

DEMO - ANDROID🎅

1. Change the return value of a function
2. Change UI component

DEMO - ANDROID🎅🏻

1. Change the return value of a function
2. Change UI component
3. Root detection bypass

DEMO - ANDROID🎅

1. Change the return value of a function
2. Change UI component
3. Root detection bypass
4. Password Check Bypass

Questions? 🤶

Thank you! 🎄

RESOURCES:

1. https://frida.re/
2. https://codeshare.frida.re/
3. https://mas.owasp.org/MASTG/apps/android/MASTG-APP-0003/