MASTG

Mobile Application Security Testing Guide

Sven Schleier
Bernhard Mueller

Carlos Holguera
Jeroen Willemsen

OWASP

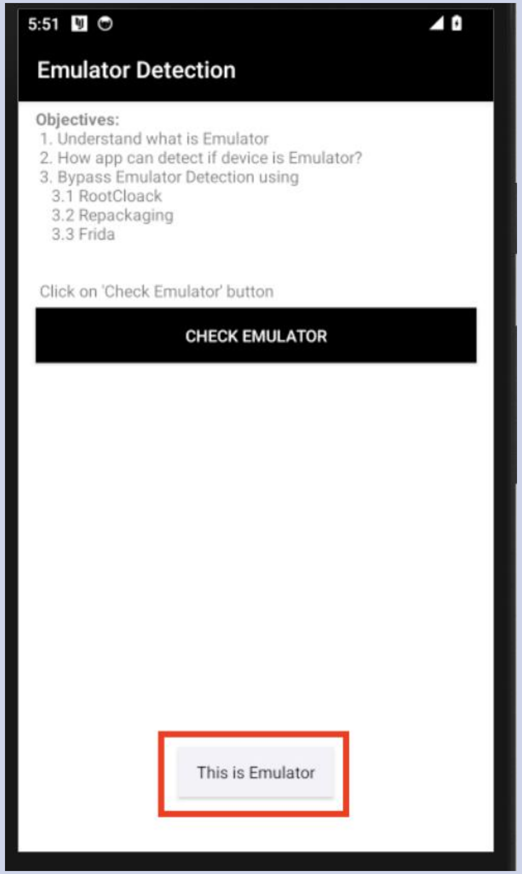
Capture the Flag (CTF)

- You work on your own!
- You have up to 30 Minutes
- The first one who contacts me via mail and shares the solutions and the Frida script get's a price, **a hardcopy of the MASTG**!
- Sent your solution to sven.schleier@owasp.org

Challenges (1/2)

App Name	Mission	Hint
Anti-Frida App	Try to bypass the server check with Frida (make it green!)	You need to add now another bypass for the “Check Frida Server” Button! 1. Find the method name of the Frida server check 2. As a starting point you can copy the existing bypass for the memory function in the Frida script that is bypassing checkMemory and modify it. 3. You will get an error if you only change the function name you are hooking. Find out what the root cause of the problem is and fix the script! **Watch out for errors in the Frida console that will help you to debug the script!** Tip: Once you make changes to the Frida script and save the file, it will be automatically reloaded in the Frida console. This allows you to quickly test the script in the running app by just pressing the button again.

Challenges (2/2)

App Name	Mission	Hint
AndroGoat	Try to bypass the emulator check  5:51 Emulator Detection Objectives: 1. Understand what is Emulator 2. How app can detect if device is Emulator? 3. Bypass Emulator Detection using 3.1 RootCloack 3.2 Repackaging 3.3 Frida Click on 'Check Emulator' button CHECK EMULATOR This is Emulator	1. Find the method name of the emulator method in the decompiled code. 2. As a starting point you can copy the existing bypass for the memory function in the Frida script that is bypassing checkMemory and modify it. Tip: Once you make changes to the Frida script and save the file, it will be automatically reloaded in the Frida console. This allows you to quickly test the script in the running app by just pressing the button again.

CTF

Let’s start ☺