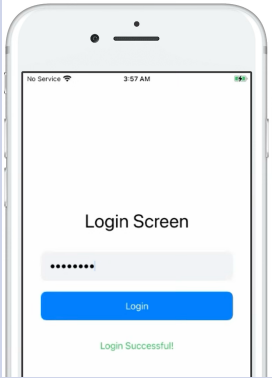
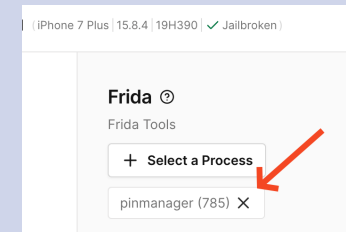


Capture the Flag (CTF)

- 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

Challenge (1/2)

App Name	Mission	Hint
Pinmanager	<div data-bbox="507 325 777 698"></div> <p>The app Pinmanager has a login screen. The password is a random number that is generated every 30 seconds. This PIN will not be available in the logs or anywhere shown in the app UI.</p> <p>You would need to find a way to dump the PIN by using Frida and get the “Login Successful” message as shown in the screenshot above.</p>	<p>Install the app 01-pinmanager and start it.</p> <p>Attach to the pinmanager app with Frida in Corellium through “Select a process”.</p> <p>Upload the script “01-show-all-methods-of-pinmanager.js” and execute it.</p> <p>Wait for a few seconds to get all the output in Frida. Find the method name that you think might generate the PIN.</p> <p>Once you have the output, detach from the app, as otherwise you will get again the listing of all methods when executing another Frida script.</p> <p>Attach again to the app.</p> <p>Upload the 01-ctf_pinmanager.js script, edit it, and replace the placeholder “<name-of-method>” in line 4 with the method name you found.</p> <p>Execute the 01-ctf_pinmanager.js script in Frida.</p> <p>If you haven’t the pin yet, you might have the wrong method or a typo.</p>



Challenges (2/2)

App Name	Mission	Hint
HiddenSecret	<p>The app HiddenSecret is decrypting a string, but it will not be available in the logs or anywhere shown in the app UI.</p> <p>You would need to find a way to dump the decrypted string by using Frida.</p>	<p>Install the app “HiddenSecret.ipa”, start it and attach Frida to it. Once the app has started the encrypted string was decrypted. You can trigger the function again by clicking the blue button. Find the decrypted string and dump it.</p> <p>Follow the "Frida flow", by identifying the method name that you want to hook. You already have a script “02-show-all-methods-of-hiddensecret.js” that will print all the methods of a specific class.</p> <p>Once you have the output, detach from the app, as otherwise you will get again the listing of all methods when executing another Frida script.</p> <p>Attach again to the app.</p> <p>Upload the 02-ctf-HiddenSecret.js, edit it, and replace the placeholder “<FUNCTION-NAME>” in line 1 with the method name you found.</p> <p>Execute the 02-ctf-HiddenSecret.js script, press the button and check if you see the output.</p>

CTF

Let's start 😊

