Challenge:

Don't Overreact

# Challenge Description:

Some web developers wrote this fancy new app! It's really cool, isn't it?

# Context:

## Decompile (Unpack) the APK file, and either find a pdf file containing the flag, or a string after decompiling.

* + - Getting the needed encryption type
    - How to send data
    - Is it fast enough

# Notes:

* Easiest way to do this would be to use ADB to run the APK file, and .
* It's also using a JS native framework React
* I Also used DE4JS to Deobufuscate and unpack js code + Format it to look beautiful, cleaner code.

# Challenge:

* First we download the files, and unzip them with the HTB password given. Hint it the same password till you do sherlocks or machines.
* We then use apktool to unpack the apk file to gain the original files .
* We then go through the folders with the unpacked apk files to look for anything like a Flag, as this one is found in the source code, not with an online Instance.
* When we go through each line of code within each file within each folder this file is the one i'm most interested in:

D:\Don't Overreact\app-release\assets\index.android.bundle

* Shortly After i was analyzing the found a base64 string containing the flag, to get it i would recommend using DE4JS,

# Flag:

* After copying and pasting the JS code from index.android.bundle

In DE4JS i can clearly see the code being base64 encoded.

When we Decode the string:

We get the flag : HTB{23m41n\_c41m\_4nd\_d0n7\_0v32234c7}

From Birdo