Challenge:
Don't Overreact

Challenge Description:

Always make sure to check via the terminal the integrity on the pdf file using sha-256.

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 .

```
birdo@DESKTOP-0ENQDDA:/mnt/d/HackTBox/Don t Overreact$ apktool d app-release.apk
I: Using Apktool 2.5.0-dirty on app-release.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/birdo/.local/share/apktool/framework/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
birdo@DESKTOP-0ENQDDA:/mnt/d/HackTBox/Don t Overreact$
```

- 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}

```
        scales: [1],
        hash: "364ec975243cfa24b8c9b8cc5247747c",
        name: "logo-htb",
        type: "png"
    })
}, 399, [393]);
__d(function (g, r, i, a, m, e, d) {
    Object.defineProperty(e, "__esModule", {
        value: !0
    }), e.myConfig = void 0;
    var t = {
        importantData: "baNaNa".toLowerCase(),
        apiUrl: 'https://www.hackthebox.eu/',
        debug: 'SFRCezIzbTQxbl9jNDFtXzRuZF9kMG43XzB2MzIyMzRjN30='
    };
    e.myConfig = t
}, 400, []);
__d(function (e, o, m, s, t, a, c) {
    t.exports = {
        name: "AwesomeProject",
        displayName: "AwesomeProject"
    }
}, 401, []);
__r(73);
__r(0);
```