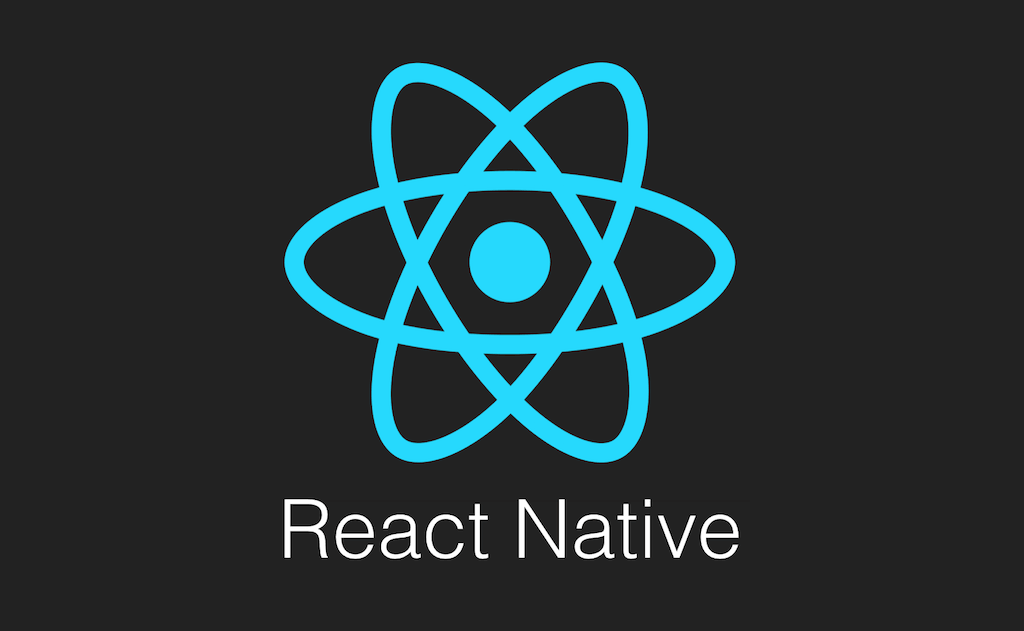
**Kira vulnerable app**

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

​[رابط البرنامج apk](https://github.com/kira2040k/Kira_vulnerable_app) ​

قبل ما نبدأ بالشرح لازم يكون عندك معرفه بأن java مو اللغه الوحيده اللي يبرمجو فيها برامج الموبايل بالعكس فيه لغات كثير مثلC#,javascript,dart,C++,python 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](https://github.com/kira2040k/apkdetector/tree/main)

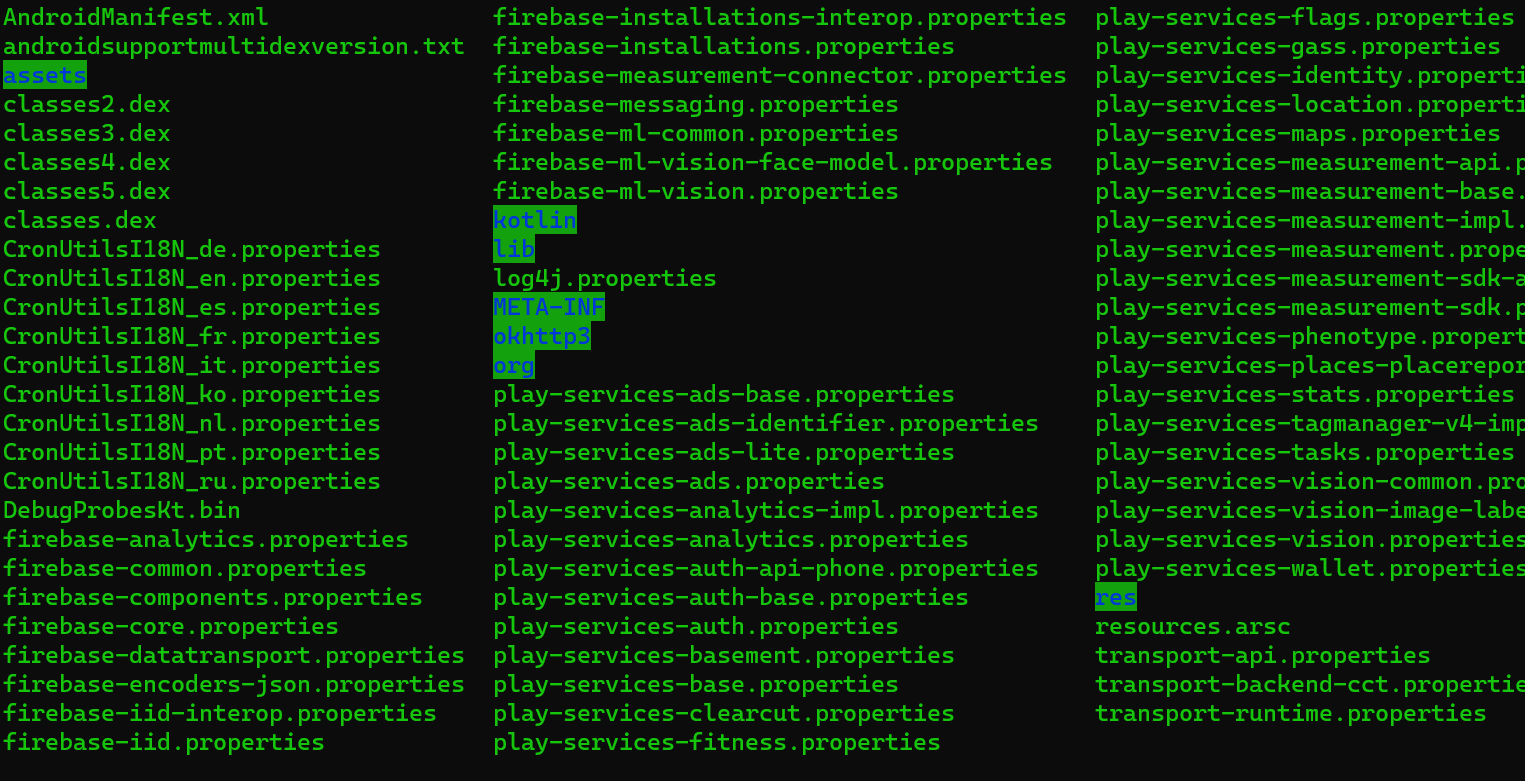
الحين نحمل البرنامج و نشغل الاداة عشان نشوف نتايجها

Text

Description automatically generated with medium confidence

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

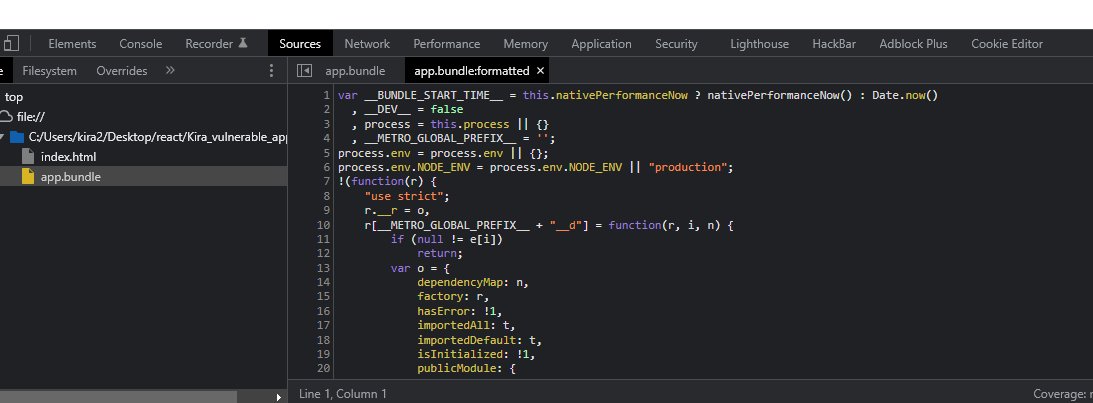


طلعت لي ملفات كثير بعد مافكيت الضغط قبل ما نروح لسورس لو تلاحظون فيه ملفات firebase يعني اكيد ان البرنامج يستخدم firebase و هي database الحين نروح assets و بنلاقي ملف app.bundle

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

Graphical user interface, website

Description automatically generated

**التحدي الأول**

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

Graphical user interface, application

Description automatically generated

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

Text

Description automatically generated

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**

Text

Description automatically generated

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

Graphical user interface, application

Description automatically generated

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

Text

Description automatically generated with medium confidence

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

Graphical user interface, text, application

Description automatically generated

و بكذا قدرنا نتخطى الحمايه بكل سهوله بتعديل الكود

​

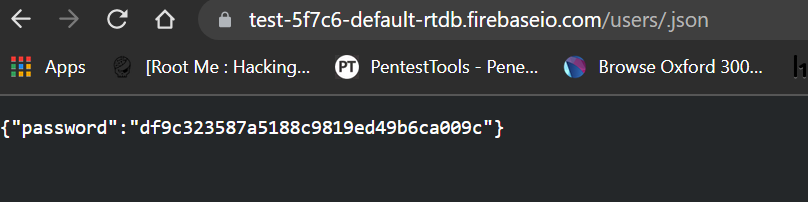
**التحدي الثالث**

نفس الخطوات....

Text

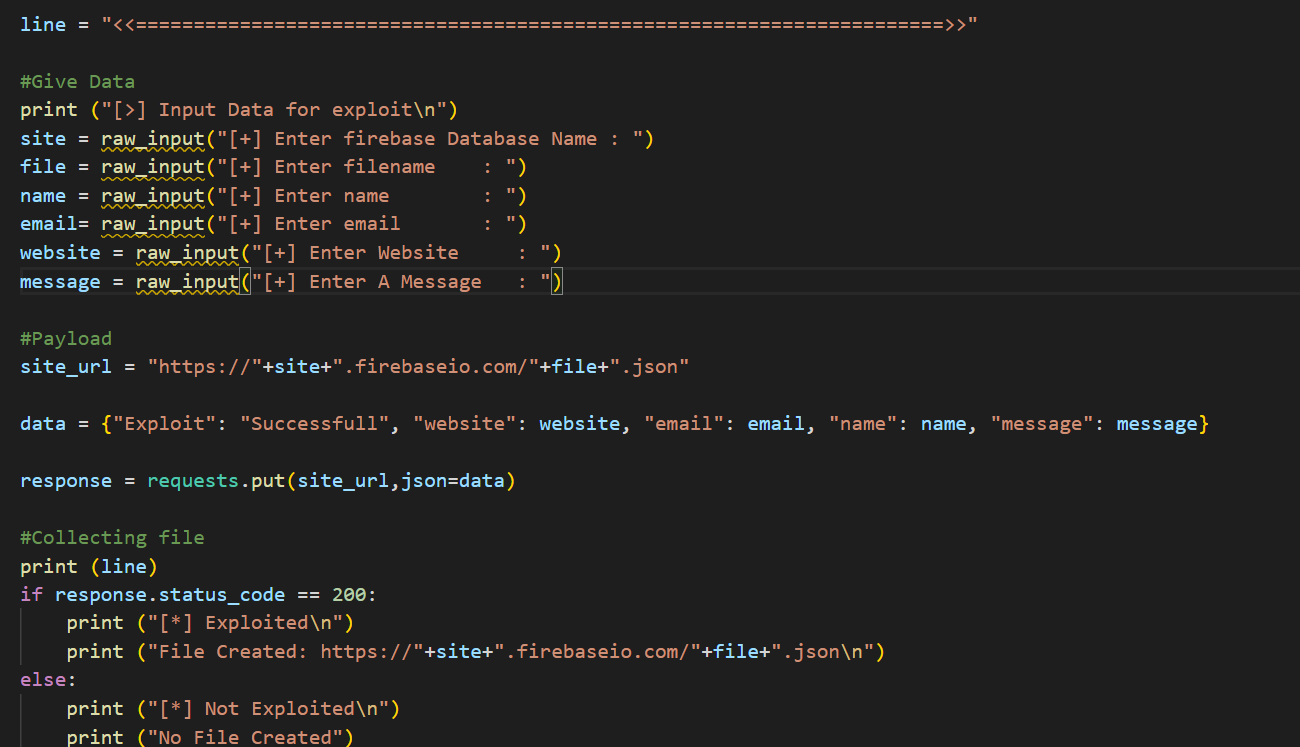
Description automatically generated

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](https://github.com/MuhammadKhizerJaved/Insecure-Firebase-Exploit)​



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

Text

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

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

Graphical user interface, application

Description automatically generated

و كذا حلينا التحدي

**التحدي الرابع**

اول ما ندخل تجينا هذي الرساله

Graphical user interface, application

Description automatically generated

ببحث بالكود عن permissions denied

Text

Description automatically generated

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

Text

Description automatically generated

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

Graphical user interface, application

Description automatically generated

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