

بسم الله الرحمن الرحيم والصلاة والسلام على نبينا محمد

السلام عليكم ورحمة الله وبركاته، مساكم الله بالخير جميعا.

اود ان أشارك معكم اليوم احد اسهل الطرق اللي جربتها لتجاوز حماية [ssl pinning](#) في التطبيقات  
المبنية باطار عمل [flutter](#)

قبل البدء في الفحص: من الأفضل التحقق من التطبيق على الأنظمة المختلفة مثلا اذا بتفحص  
تطبيق على نظام android جرب انك تفحصه على نظام ios ممكن ما يكون عليه حماية في  
ios والعكس كذلك , فبالتالي تختصر على نفسك الوقت

الشرح :

ما يخفى عليكم أن تطبيقات flutter من أكثر التطبيقات اللي يصعب فحصها ( ليس مستحيل)  
وذلك لان الاكواد الخاصة بالتطبيق تكون على هيئة binary code ويتم تنفيذها من قبل  
Dart virtual machine , فبذكر تجربتي لفحص تطبيقين مبنية باستعمال flutter يجب العلم  
ان هذه ليست الطرق الوحيدة لكن هذي اشوفها اسهل شيء جربته.

الجهاز اللي استعملته كان محاكي [nox](#) بإصدار 64 bit , android 9

التطبيق الأول (بطلق عليه اسم [b5t](#))

يحتوي على هذه الحمائيات

[ssl pinning](#)

vpn detection

non proxy aware application

root detection

[RASP](#)

1.1

طبعا الهدف من هذه الحمائيات فقط هو زيادة صعوبة عمل [reverse engineering](#) للتطبيق ,  
على الرغم من أن أفضل حل لتخطي هذه الحمائيات هو استخدام [Frida](#) ، إلا أنه يتطلب معرفة  
في reverse engineering كمبتدئ لم اختر هذا الحل بسبب نقص الخبرة في reverse  
engineering

## الحل الأسهل

1.2

تخطي حماية root detection هو عدم استعمال root , وبالنسبة لـ RASP، من الأفضل عدم تعديل التطبيق، وتركه كما هو.

1.3

أما بالنسبة لـ SSL Pinning وتجاهل بروكسي النظام، يمكن استخدام أدوات مثل [HTTP Toolkit](#) أو [HTTP Canary](#). أما بالنسبة لـ اكتشاف VPN، فيحتاج لتخطي إضافي للتمكن من تشغيل HTTP Toolkit.

1.4

متطلبات التنفيذ

يجب عليك تحميل البرامج التالية على هاتفك

1- تحميل تطبيق b5t

2- تحميل [http toolkit](#)

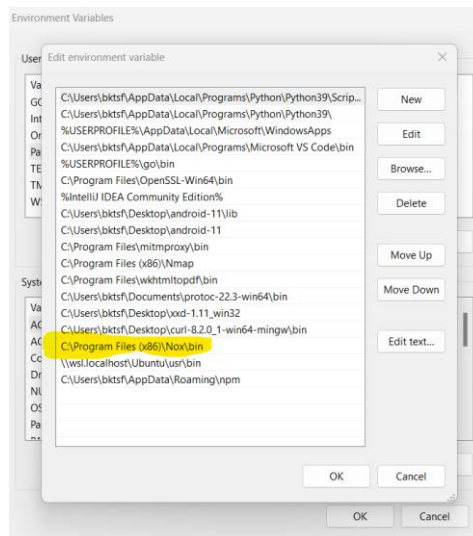
3- تحميل [root certificate manager](#)

واما الكمبيوتر الخاص بك يجب عليك تحميل

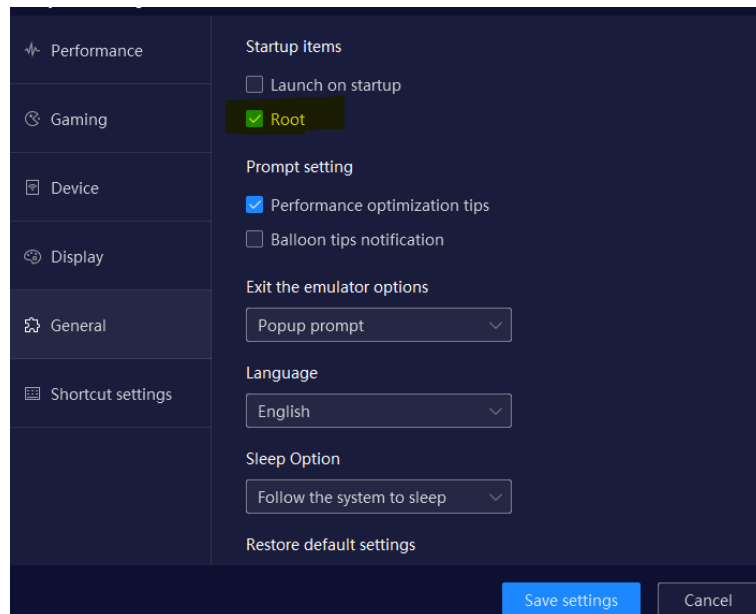
1- أي أداة proxy

2- http toolkit for windows

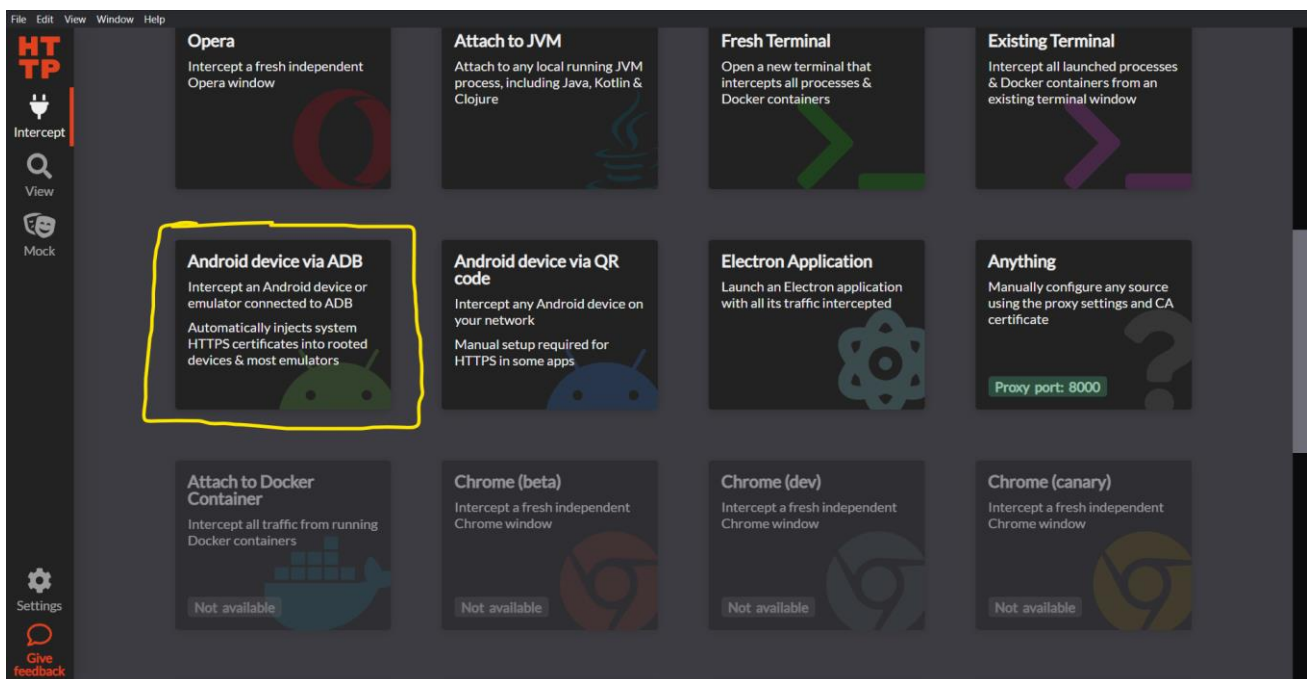
ملاحظة مهمة يجب التأكد من ان adb الخاص بي nox موجود في path الخاص بجهازك



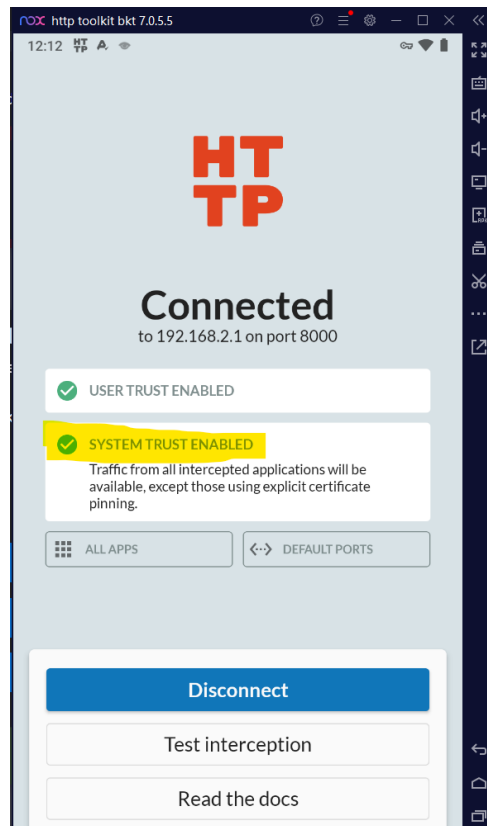
## 1- نقوم بتشغيل المحاكى بصلاحيه root



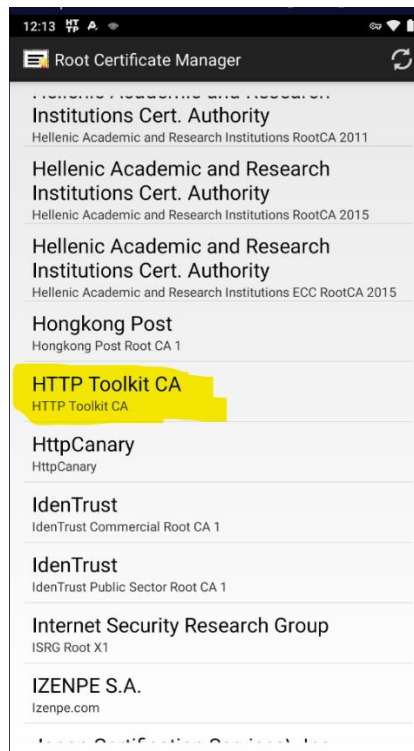
## 2- نقوم بربط http tool kit بالهاتف



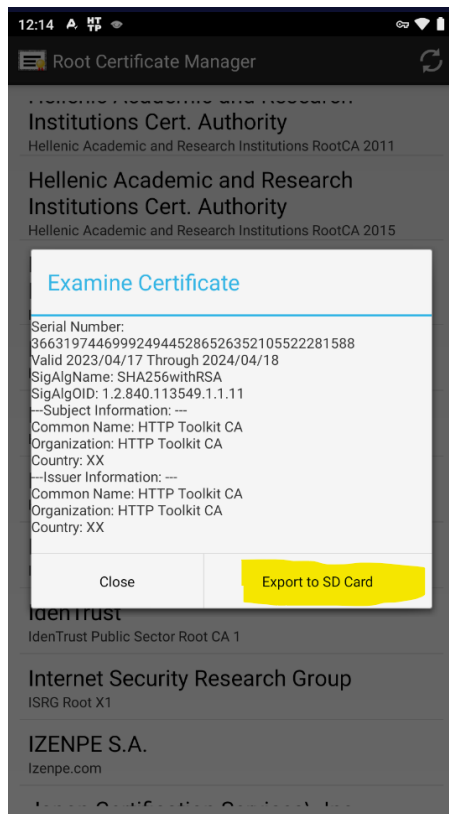
3- بعد ربط http tool kit وتشغيلها في الهاتف بصلاحيه root نقوم بالتأكد من ان الشهادة مثبتة بصلاحيه root



4- بعد ذلك نقوم بالذهاب الى root certfacte manager ونبحث عن شهادة باسم HTTP tool kit

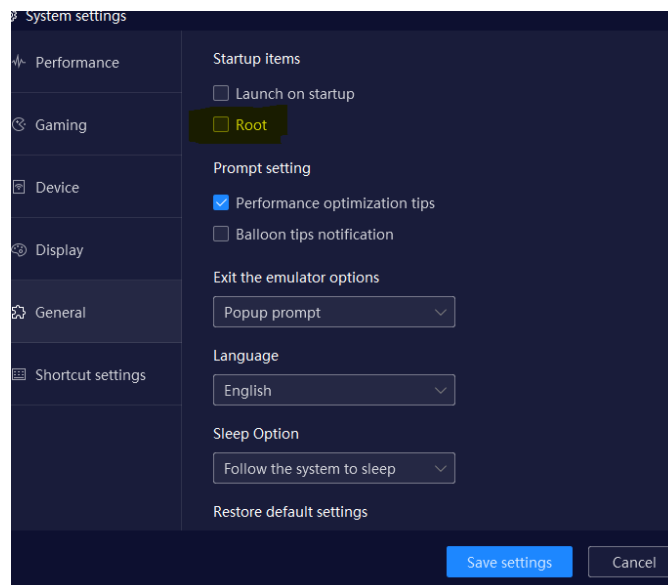


5- نقوم بالضغط على الشهادة وتصديرها الى storage

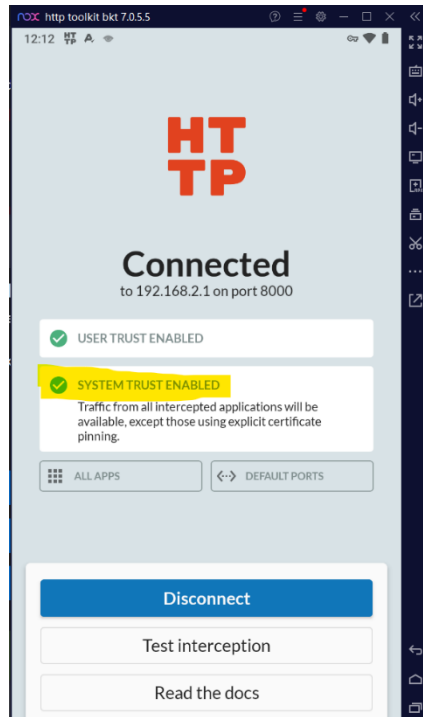


6- الان نقوم بقطع الاتصال في http tool kit ونقوم بالرجوع الى root certificate manager ونحذف الشهادة ثم نقوم بتنصيب الشهادة اللتي قمنا بتصديرها من قبل ( تقدر ترا تنسخ الشهادة عندك على طول من الويندوز لكن كلها تؤدي نفس الغرض)

7- نقوم بإيقاف root في المحاكى ونعيد تشغيل المحاكى



8- نقوم بتشغيل http tool kit للتأكد من ان الشهادة مثبتة و root غير فعال



9- بعد التأكد من ان الشهادة تعمل و الروت غير فعال في الجهاز هذا الشيء سيمكننا من تخطي ssl pinning وتجاهل التطبيق للبروكسي الخاص بالنظام

10- مثل ما ذكرت سابقا تطبيق b5t فيه vpn detection يعني لو شغلت http tool kit التطبيق مراح يفتح معي فالحل كان اني اشغل التطبيق ثم اربط http tool kit

لكن المشكلة ان التطبيق بعد كل ريكويست ينرسل يكشفني فلازم ارجع اظفي http tool kit بعدين اشغل التطبيق وهكذا ( طريقة غير فعالة لكن اسهل من اني اسوي هندسة عكسية )

وبكذا انتهينا من شرح تخطي تطبيق b5t .

**ملاحظة:** من خلال خبرتي المتواضعة هناك نوعين في detection للحمايات نوع يكون dynamic يعني طول ما التطبيق شغال يشيك كل شوي وفيه نوع يكون بس اول ماتفتح التطبيق بعدها معاد يشيك

ولان عندنا التطبيق الثاني بطلق عليه اسم dr3

يحتوي على هذه الحماية :

[ssl pinning](#)

vpn detection

non proxy aware application

root detection

## 2.1

استعملت نفس المحاكى لكن من بعد الخطوة رقم 3 فوق ما يحتاج نسويها لأننا أساسا بنستخدم الروت

**2.2** ثبت عليه روت magisk و Isposed (يعني root شغال)

و فعلت Isposed module هذه

1- novpndetect لاختفاء vpn عن التطبيقات

2- sslunpinning (الصحيح مدري اذا كنت احتاجه ولا لا لكنه كان شغال )

## Modules

2 modules enabled



NoVPNDetect

1.1

Prevent some apps detect your phone connected to VPN.



SSLUnpinning

1.0.0

Android Xposed Module to bypass SSL certificate validation (Certificate Pinning).

## 2.2

الان بما اننا الان نستعمل root اول ما نفتح تطبيق dr3 راح يعرف اننا نستعمل root فطريقة التخطي لحماية root detection هي عن طريق اننا نشغل أداة http tool kit ونروح نفتح تطبيق dr3 لكن قبل يفتح التطبيق نضغط زر home ثم نرجع ندخل التطبيق , نكرر العملية الين يفتح تطبيق dr3 بشكل طبيعي ( مادري ليه هذي الطريقة ضبطت لكن أتوقع ان التطبيق يتحقق من الروت فقط عند تشغيل التطبيق بعد ذلك ما يتحقق منها )

## ختاماً

اللهم انفعني بما علمتني، وعلمني ما ينفعني، وزدني علماً  
ختاماً, اتمنى اني غطيت الموضوع بشكل ممتاز واعذرونا على القصور ولاستفسارات  
والاسالة والمقترحات حسابات التواصل في الأسفل

تويتر – [m\\_b5t](#)

الايمل – [bktsfr@hotmail.com](mailto:bktsfr@hotmail.com)

قت هب – [mdr3](#)