FIELD NOTE / ANDROID

Panduan Mengintegrasikan Burp Suite dengan Android Emulator

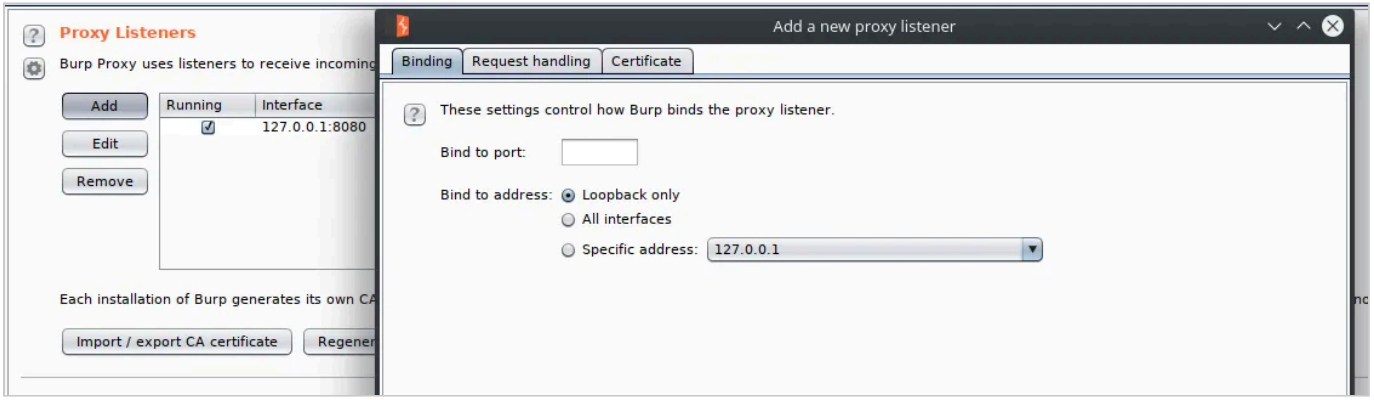
Petruknisme · 14 Mar, 2018 · 2 min to read

Sebelum kita memulai penetration testing terhadap sebuah mobile apps, ada beberapa hal yang perlu dipersiapkan. Terutama sebuah proxy intercepter yang nantinya berguna dalam intercept packet data yang diterima dan dikirimkan oleh device ke server. Pada tulisan kali ini saya hanya menggunakan Burp Suite sebagai proxy intercepter yang akan diintegrasikan dengan Android Emulator seperti Genymotion, NOX ataupun yang lain. Tulisan ini saya khususkan untuk orang-orang yang memang baru memulai dalam hal mobile pentest.

Beberapa requirement yang perlu dipersiapkan:

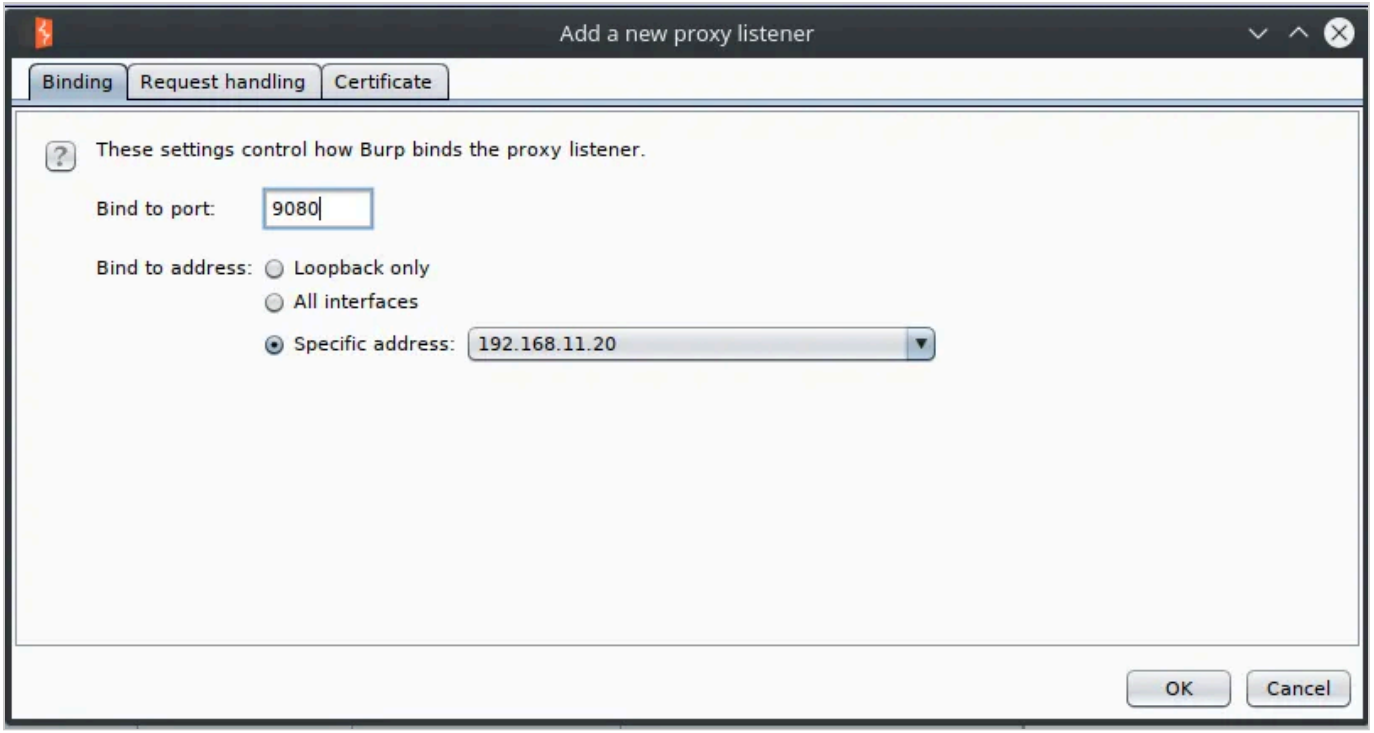
- Burp suite(saya pakai burp community edition)
- Android Emulator(saya pakai Genymotion)

Saya anggap bahwa kita sudah mempunyai dan memasang apa yang perlu dipersiapkan dengan baik. Langkah pertama, jalankan burp suite terlebih dahulu, lalu pilih tab *Proxy → Options* . Klik Add di *Proxy Listeners*:



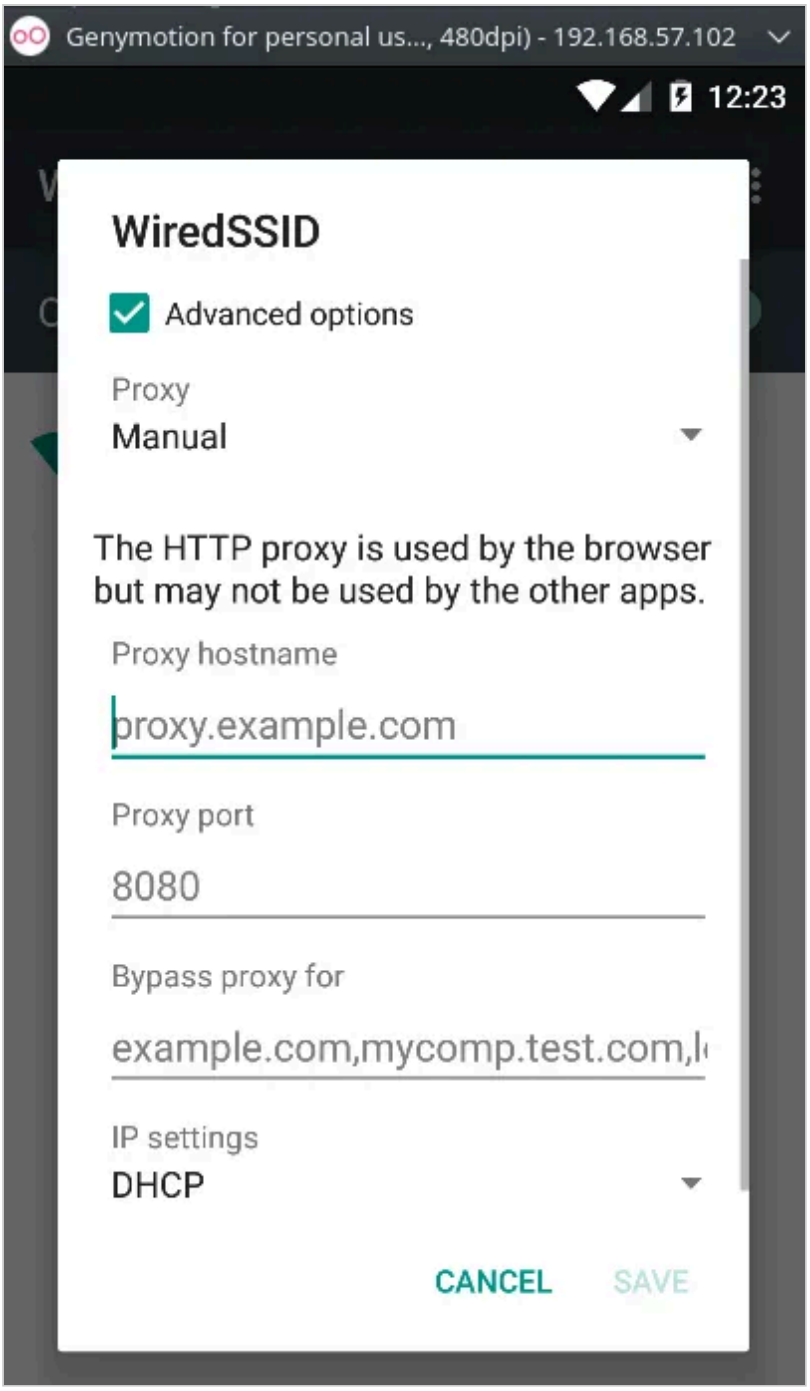
Setelah itu kita isi *bind to port* dengan port yang kita inginkan(misal: 9080), lalu pilih *spesific address* dan pilih ip address yang sesuai dengan ip yang kita miliki atau satu jaringan dengan android emulator nantinya.

Licensed under CC BY-SA 4.0



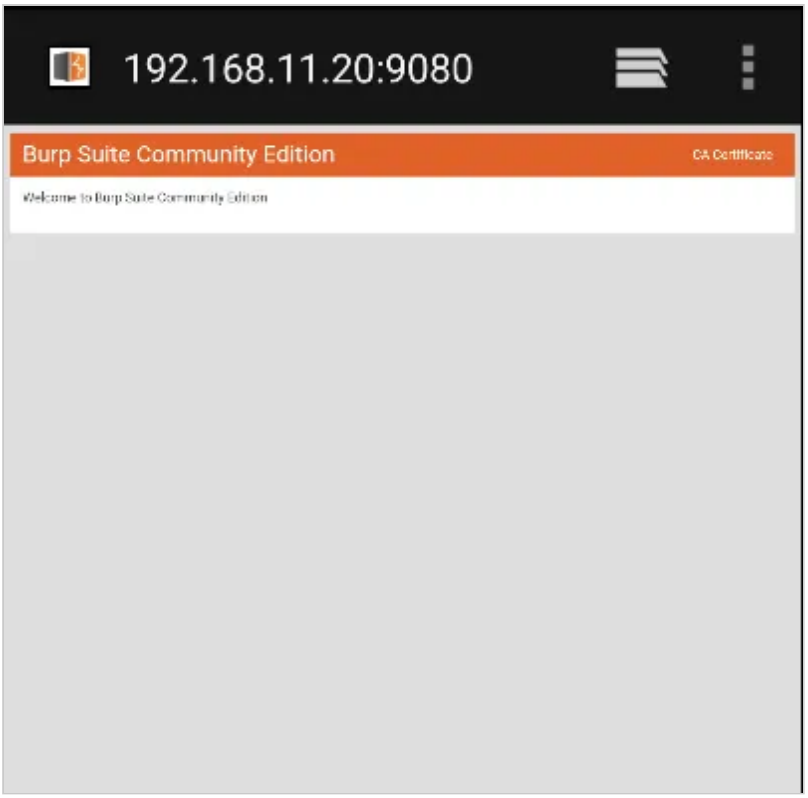
Selanjutnya jalankan Android Emulator dan masuk kedalam wifi setting, akan muncul wifi dengan nama “WiredSSID”. Tap dan hold sampai muncul *Modify network* seperti gambar:

Licensed under CC BY-SA 4.0



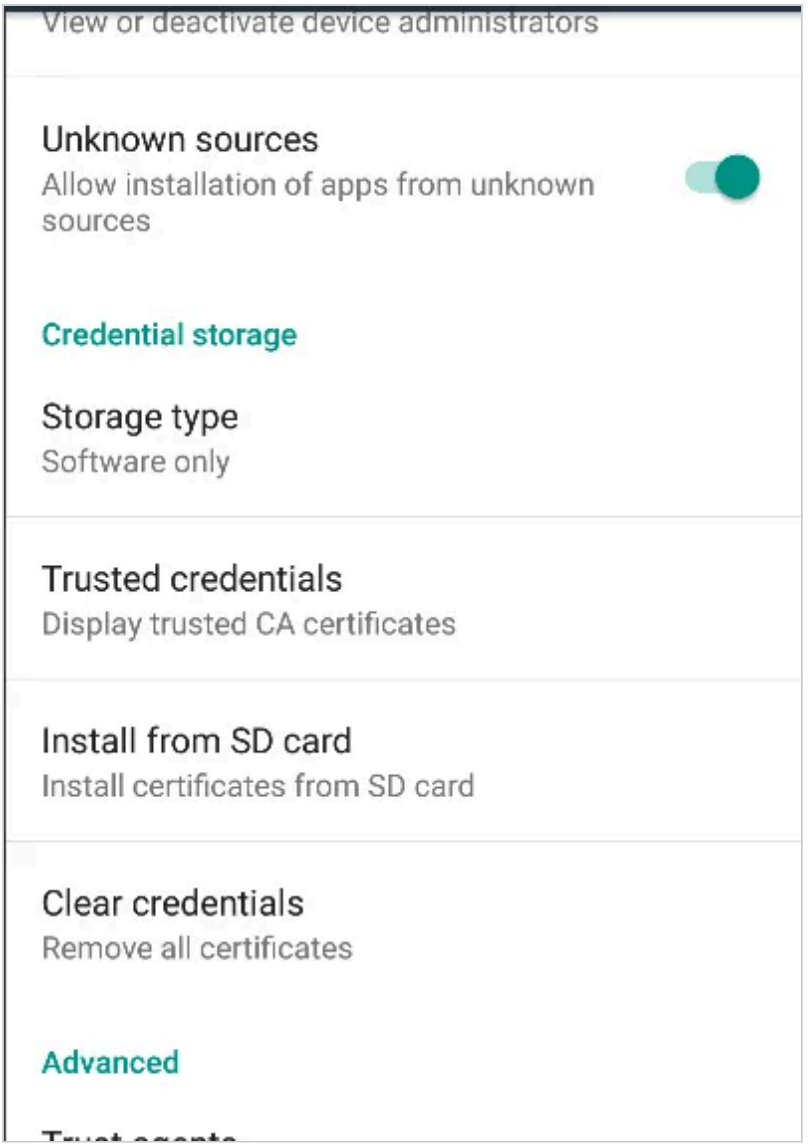
Set proxy hostname dan port sesuai dengan yang sudah kita setting sebelumnya di burp suite untuk ip dan port proxy. Kalau sudah selesai, klik on off wifi untuk merubah pengaturan wifi. Setelahnya, buka web browser dan akses alamat http://ip-proxy:portbind (http://ip-proxy:portbind) misal http://192.168.11.12:9080 (http://192.168.11.12:9080) seperti berikut:

Licensed under CC BY-SA 4.0



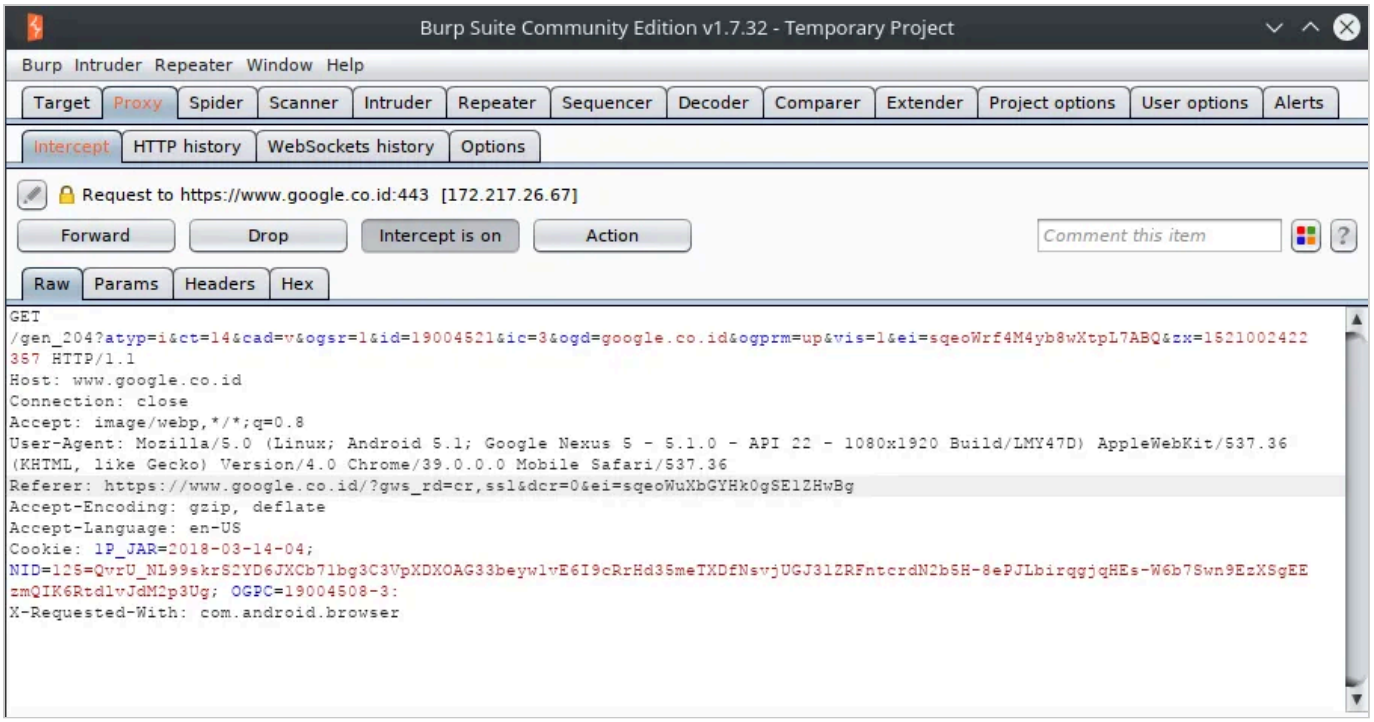
Klik CA Certificate pada bagian pojok kanan atas. Kalau sudah terunduh, buka file manager dan rename file tersebut menjadi **cacert.cer**. Setelah itu masuk ke menu setting → security dan pilih Install from SD Card:

Licensed under CC BY-SA 4.0



Klik file yang sudah kita rename dan akan muncul popup dialog penambahan certificate. Setelah berhasil, kita coba kunjungi web yang mengandung https dan kita cek pada burpsuite apakah ada response, bila sudah terintegrasi akan ada response seperti berikut pada tab intercept:

Licensed under CC BY-SA 4.0



Nah, mungkin sekian tulisan saya kali ini. Akhir kata, semoga bermanfaat.

Android # Penetration Testing # Security # Tutorial

Licensed under CC BY-SA 4.0