

Forum:[Hack Forums](#)

Thread: [Help | Finding API Endpoints from Android App?](#)

SIM-964740 - August 16, 2019, 5:44 pm

Hi there!

I made a similar thread before in another section but didn't generate much conversation.

I am trying to find a way to gather API endpoints for a particular app. I don't need to see packet information only each API call (api/v1/this/that).

Suggested was doing my own MITM but I haven't got the tools on me to do that right now, is there a simpler solution anyone can think of, remembering that it's very difficult to sniff on Android now.

Horus God - August 16, 2019, 6:05 pm

What ?! its too easy btw.

run any http debugger like Charles its have http proxy server and write http proxy in wifi settings of your phone.

~Rexon - August 16, 2019, 6:46 pm

Fiddler works great for sniffing http requests. If the app has ssl pinning you can just use frida. Some apps even trust certificates if they're in the system (you can do this by moving the install certificate into the system certs folder)

If you need help just pm me mate

Prawnster - August 16, 2019, 6:49 pm

(Aug 16, 2019 06:46 PM)~Rexon Wrote: [\[CITE\]](#) Fiddler works great for sniffing http requests. If the app has ssl pinning you can just use frida. Some apps even trust certificates if they're in the system (you can do this by moving the install certificate into the system certs folder)

If you need help just pm me mate

^ This pretty much, frida can be used for unpinning / swapping certs and then just add your own fiddler cert and sniff through that (fiddler is a http proxy) so yeah, very simple to do once you get your head around it

SIM-964740 - August 16, 2019, 8:00 pm

(Aug 16, 2019 06:05 PM)Horus God Wrote: [\[CITE\]](#) What ?! its too easy btw.

run any http debugger like Charles its have http proxy server and write http proxy in wifi settings of your phone.

I wish it were, SSL certs are being a pain.

Prawnster - August 18, 2019, 2:58 pm

(Aug 16, 2019 08:00 PM)Deadpan Wrote: [\[CITE\]](#) I wish it were, SSL certs are being a pain.

You can unpin/swap the cert with your own fiddler cert using frida and it should be able to sniff just fine

