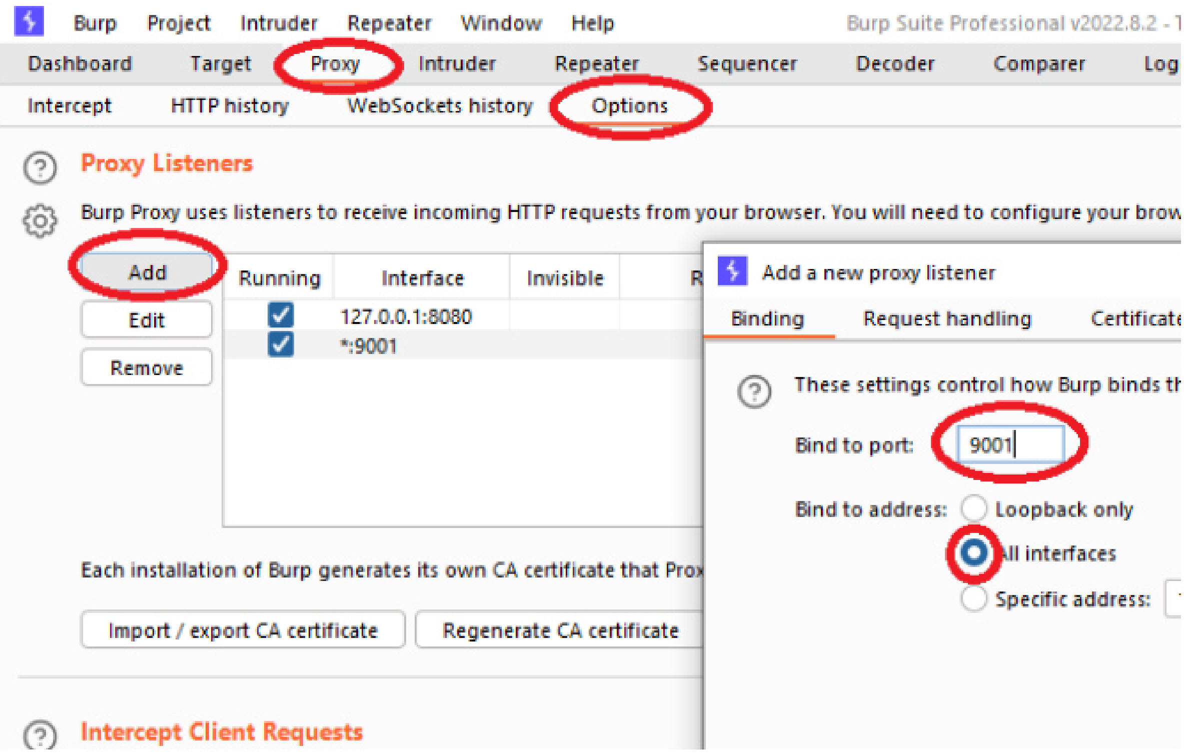
Open Burp Suite Start

Configure proxy:

configure proxy server on all interface


Burp Project Intruder Repeater Window Help
Burp Suite Professional v2022.8.2 - 1
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Log
Intercept HTTP history WebSockets history Options
Add
Edit
Remove
Import / export CA certificate
Regenerate CA certificate
Add a new proxy listener
Binding Request handling Certificate

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your brow

Running	Interface	Invisible	R
☑	127.0.0.1:8080		
☑	*:9001		

Each installation of Burp generates its own CA certificate that Prox

These settings control how Burp binds th

Bind to port: 9001

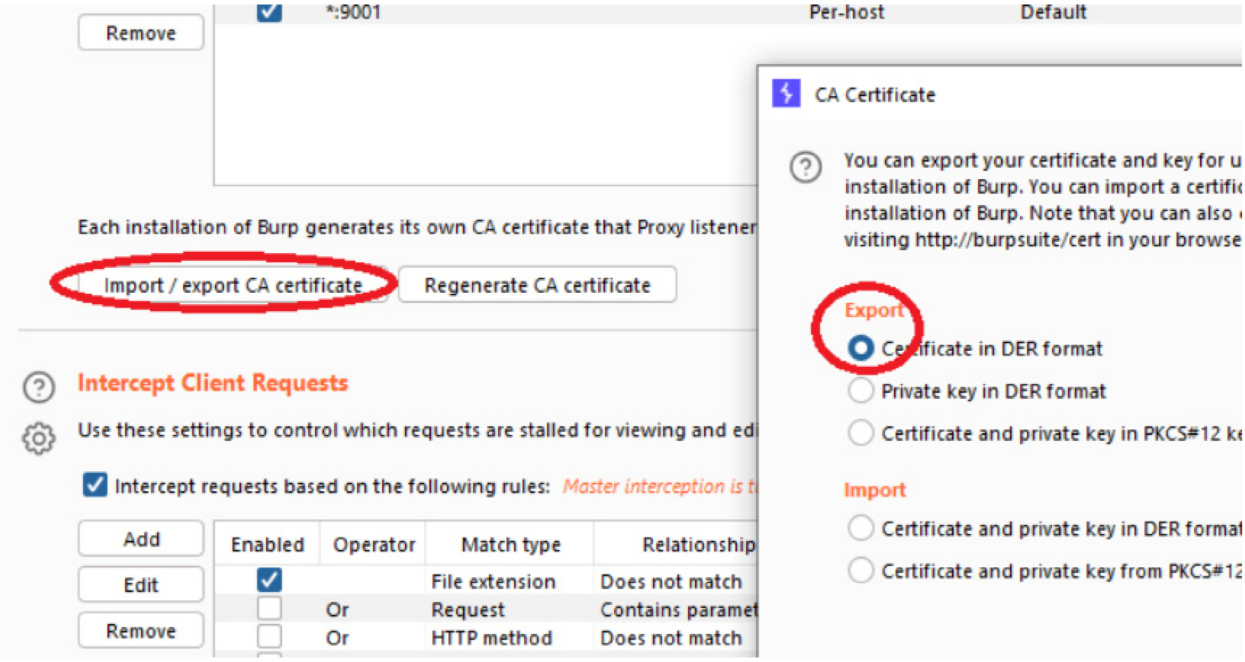
Bind to address: ○ Loopback only

● All interfaces

○ Specific address:

Intercept Client Requests

Export CA certificate Burp



☑	*:9001	Per-host	Default

Each installation of Burp generates its own CA certificate that Proxy listener

You can export your certificate and key for u installation of Burp. You can import a certific installation of Burp. Note that you can also visiting http://burpsuite/cert in your browse

Export

● Certificate in DER format

○ Private key in DER format

○ Certificate and private key in PKCS#12 ke

Import

○ Certificate and private key in DER format

○ Certificate and private key from PKCS#12

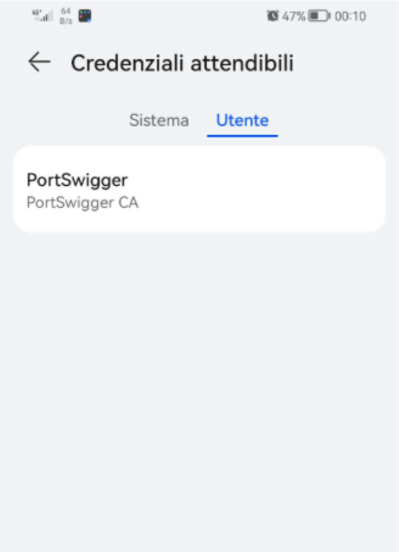
Intercept Client Requests

Use these settings to control which requests are stalled for viewing and edi

☑ Intercept requests based on the following rules: *Master interception is t*

Enabled	Operator	Match type	Relationship
☑		File extension	Does not match
□	Or	Request	Contains paramet
□	Or	HTTP method	Does not match

Download certificate and open file pem on Android Phone to install



47% 00:10

Credenziali attendibili

PortSwigger
PortSwigger CA

Install Aqara_Home_mod_network.apk on Android Phone

delete official app Aqara Home

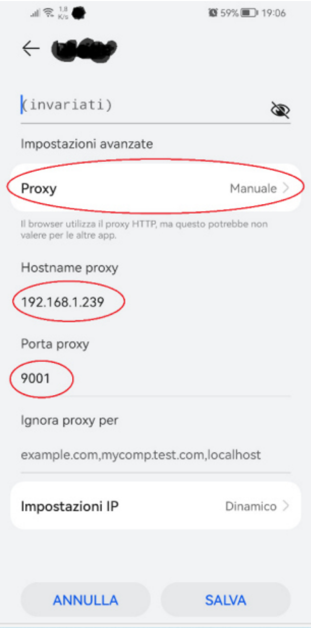
mod info: \res\xml\network_security_config.xml

```
<trust-anchors>
        <certificates src="user" />
</trust-anchors>
```

Connect network Phone Wifi and PC over same network

Set proxy on Wifi Andorid Phone

Hold tap ssid wifi -> edit network -> set proxy manual -> IP Burp PC -> Port



59% 19:06

[redacted]

(invariati)

Impostazioni avanzate

Proxy: Manuale

Il browser utilizza il proxy HTTP, ma questo potrebbe non valere per le altre app.

Hostname proxy: 192.168.1.239

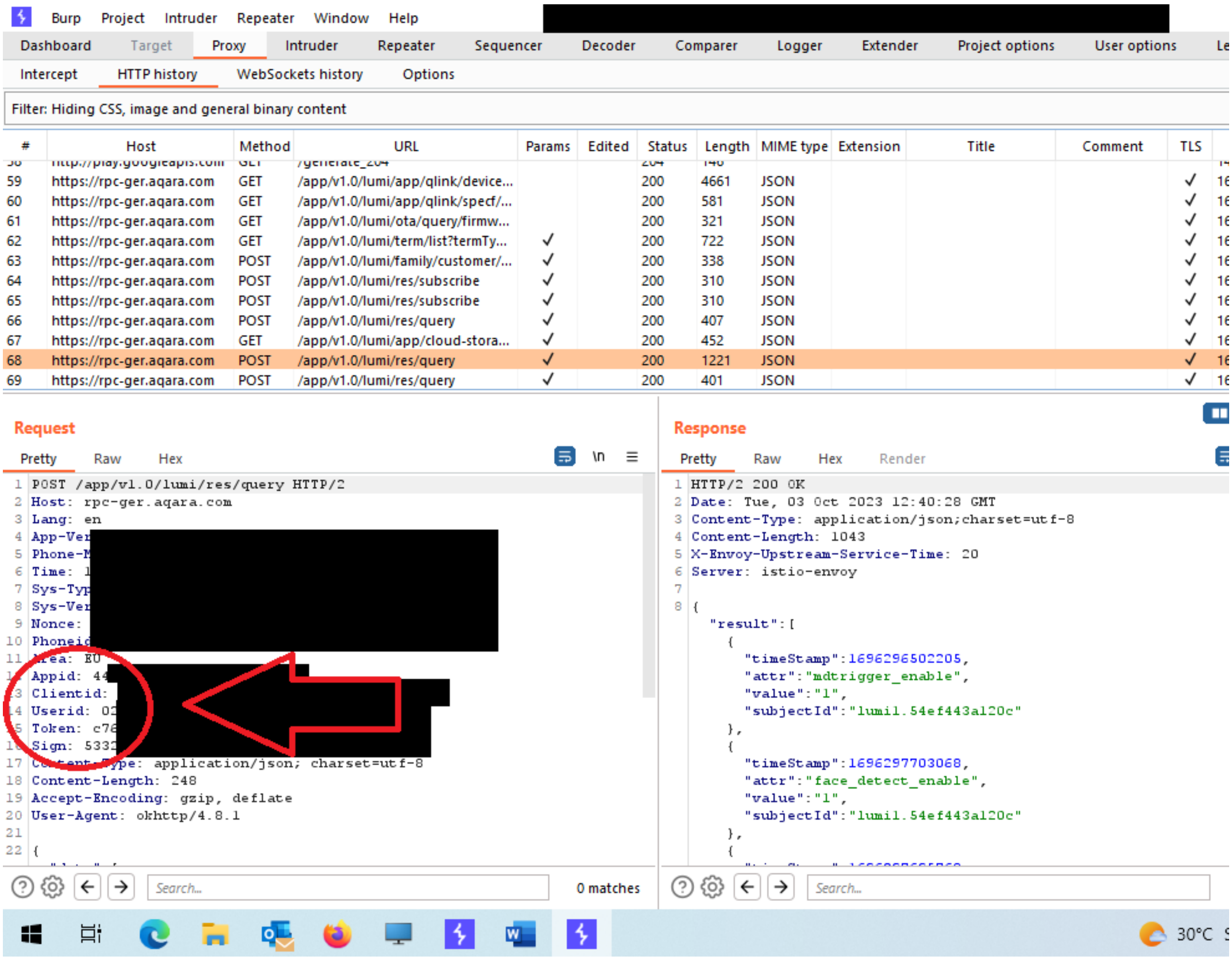
Porta proxy: 9001

Ignora proxy per: example.com,mycomp.test.com,localhost

Impostazioni IP: Dinamico

Open Aqara Home app (Aqara_Home_mod_network.apk) on Android

move camera and see post request from Burp:



Burp Project Intruder Repeater Window Help
[redacted]
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options
Intercept HTTP history WebSockets history Options
Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS
59	https://rpc-ger.aqara.com	GET	/app/v1.0/lumi/app/qlink/device...			200	4661	JSON				✓
60	https://rpc-ger.aqara.com	GET	/app/v1.0/lumi/app/qlink/specf/...			200	581	JSON				✓
61	https://rpc-ger.aqara.com	GET	/app/v1.0/lumi/ota/query/firmw...			200	321	JSON				✓
62	https://rpc-ger.aqara.com	GET	/app/v1.0/lumi/term/list?termTy...	✓		200	722	JSON				✓
63	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/family/customer/...	✓		200	338	JSON				✓
64	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/res/subscribe	✓		200	310	JSON				✓
65	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/res/subscribe	✓		200	310	JSON				✓
66	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/res/query	✓		200	407	JSON				✓
67	https://rpc-ger.aqara.com	GET	/app/v1.0/lumi/app/cloud-stora...	✓		200	452	JSON				✓
68	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/res/query	✓		200	1221	JSON				✓
69	https://rpc-ger.aqara.com	POST	/app/v1.0/lumi/res/query	✓		200	401	JSON				✓

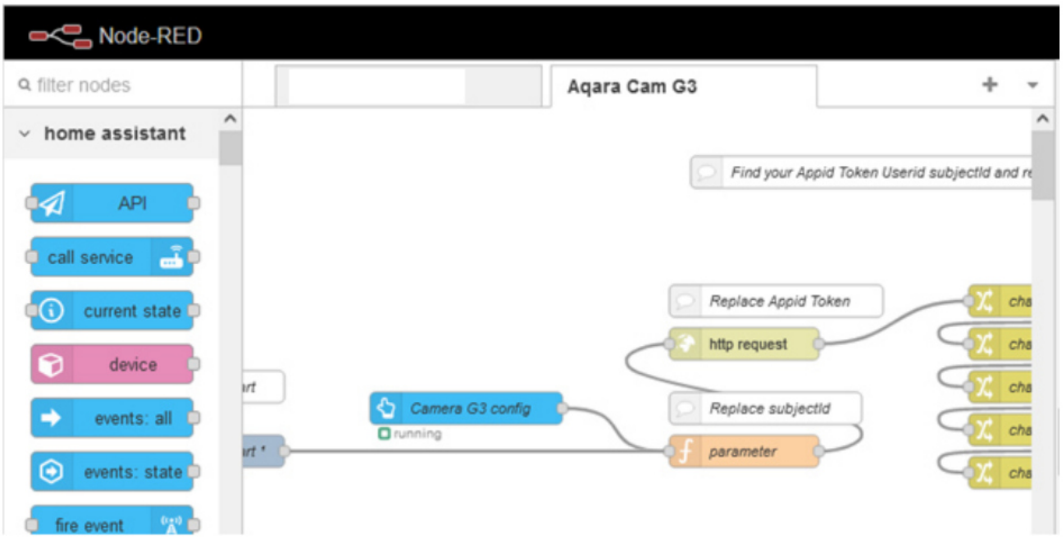
Request

```
POST /app/v1.0/lumi/res/query HTTP/2
Host: rpc-ger.aqara.com
Lang: en
App-Ver [redacted]
Phone-M
Time: 1
Sys-Typ
Sys-Ver
Nonce:
Phoneid
Area: EU
Appid: 44 [redacted]
Clientid:
Userid: 02
Token: c76
Sign: 5332
Content-Type: application/json; charset=utf-8
Content-Length: 248
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.8.1

{
```

Response

```
HTTP/2 200 OK
Date: Tue, 03 Oct 2023 12:40:28 GMT
Content-Type: application/json;charset=utf-8
Content-Length: 1043
X-Envoy-Upstream-Service-Time: 20
Server: istio-envoy

{
  "result":[
    {
      "timeStamp":1696296502205,
      "attr":"mdtrigger_enable",
      "value":"1",
      "subjectId":"lumi1.54ef443a120c"
    },
    {
      "timeStamp":1696297703068,
      "attr":"face_detect_enable",
      "value":"1",
      "subjectId":"lumi1.54ef443a120c"
    },
    {
```

Import json Flow and replace your data into nodes (Appid - Token - subjectId – Userid)



Node-RED
filter nodes
home assistant
API
call service
current state
device
events: all
events: state
fire event
Aqara Cam G3
Find your Appid Token Userid subjectId and re
Replace Appid Token
http request
Replace subjectId
parameter
Camera G3 config
running
cha
cha
cha
cha
cha