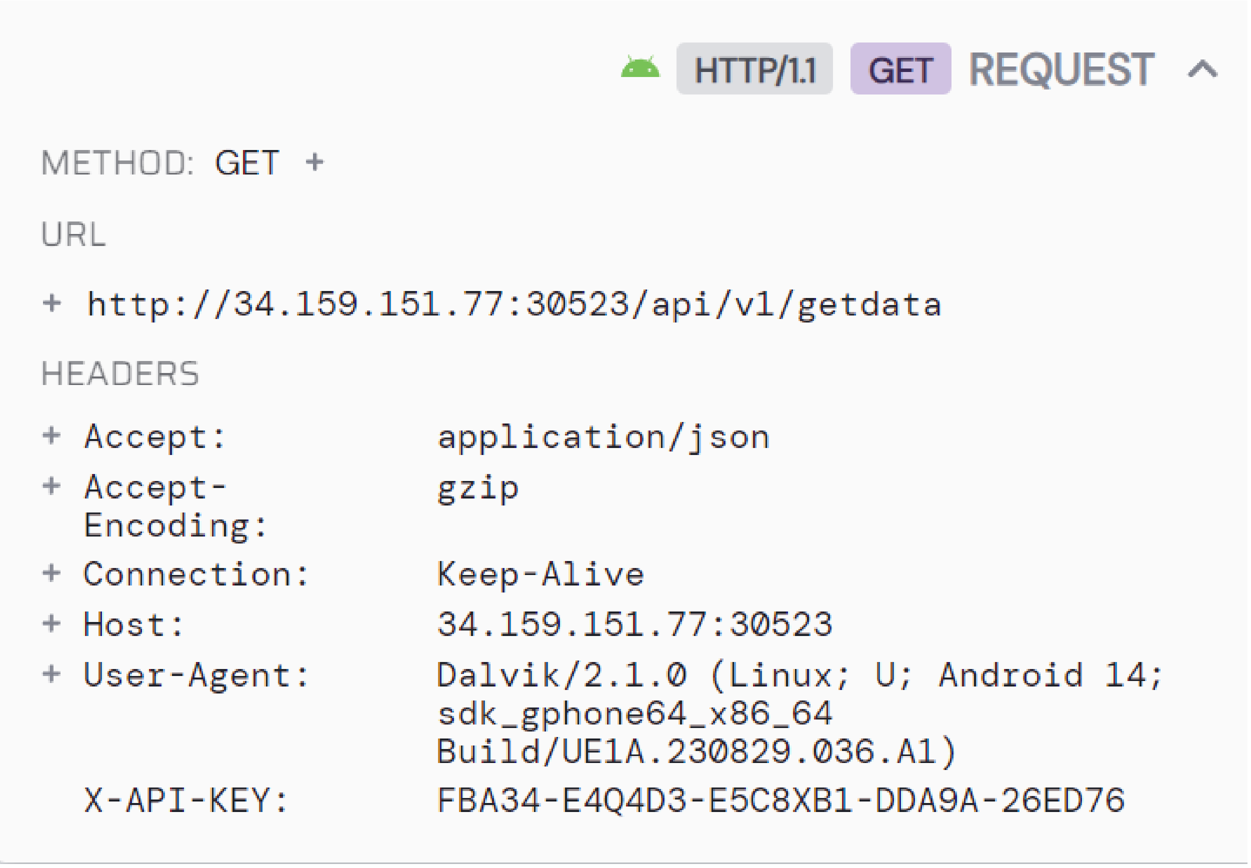
So, we've got a mobile app which takes a domain and port as input and performs a request. LogCat shows us the request is an error, so let's take a closer look. But how?

Introducing: https://httptoolkit.com/

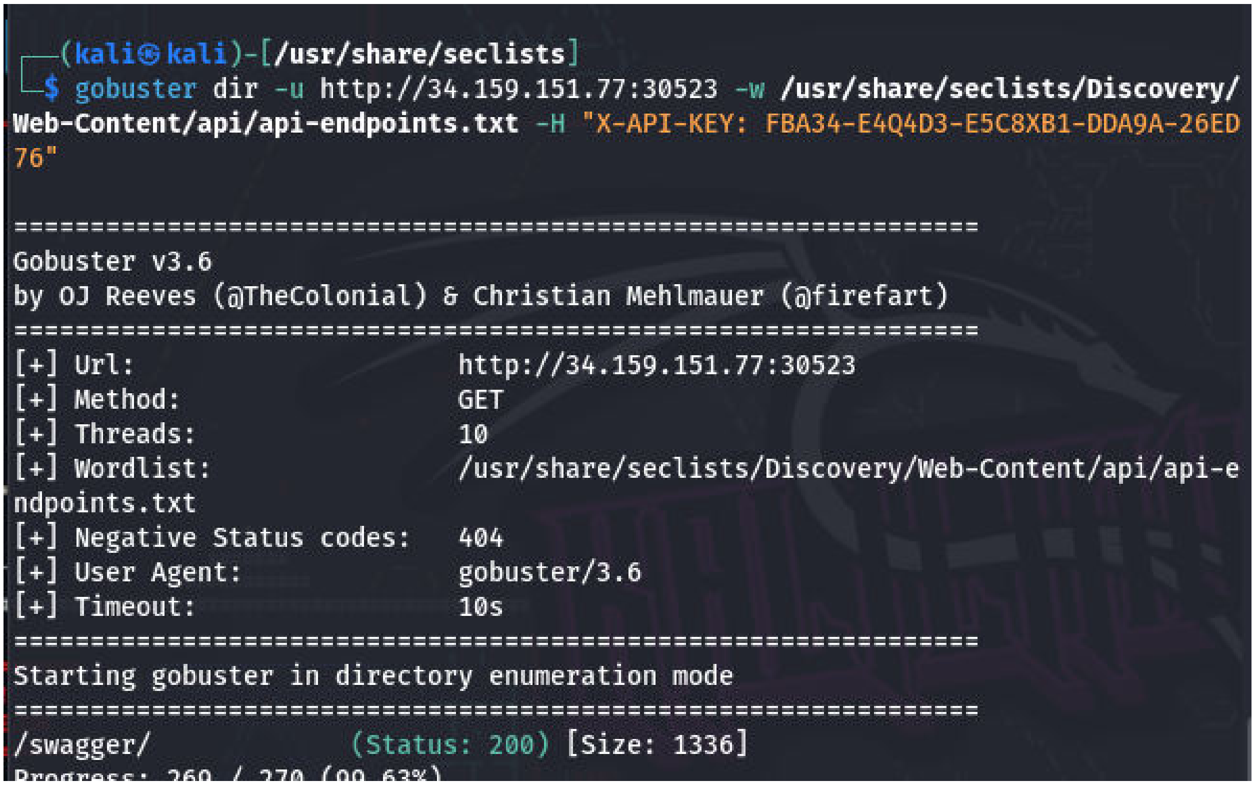
Using this and android studio I was able to capture the requests made by the app. There. I found this:



```
METHOD: GET +

URL

+ http://34.159.151.77:30523/api/v1/getdata

HEADERS

+ Accept:            application/json
+ Accept-            gzip
  Encoding:
+ Connection:        Keep-Alive
+ Host:              34.159.151.77:30523
+ User-Agent:        Dalvik/2.1.0 (Linux; U; Android 14;
                     sdk_gphone64_x86_64
                     Build/UE1A.230829.036.A1)
  X-API-KEY:         FBA34-E4Q4D3-E5C8XB1-DDA9A-26ED76
```

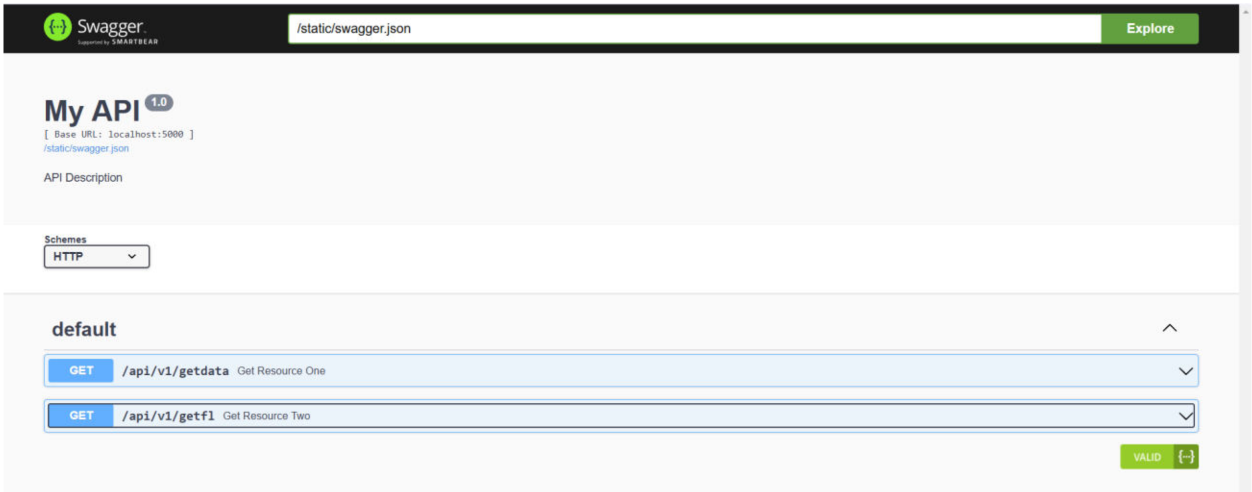
Note: After using the http toolkit, the app also started to work (the requests were going through)

So, we got an api. getdata is effectively useless, so let's see if there are any other endpoints



```
┌──(kali㉿kali)-[/usr/share/seclists]
└─$ gobuster dir -u http://34.159.151.77:30523 -w /usr/share/seclists/Discovery/
Web-Content/api/api-endpoints.txt -H "X-API-KEY: FBA34-E4Q4D3-E5C8XB1-DDA9A-26ED
76"

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://34.159.151.77:30523
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/api/api-e
ndpoints.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/swagger/             (Status: 200) [Size: 1336]
Progress: 269 / 270 (99.63%)
```

Mm, swagger. I tried to connected it in my browser, but I realized I needed the X-API-KEY header, so I used a chrome extension I had, https://chromewebstore.google.com/detail/modheader-modify-http-hea/idgpnmonknjnojddfkpgkljpfnnfcklj, to insert that header and make the request:



/static/swagger.json

My API 1.0

[Base URL: localhost:5000]

/static/swagger.json

API Description

Schemes: HTTP

default

GET /api/v1/getdata Get Resource One

GET /api/v1/getfl Get Resource Two

So the app has 2 api endpoints, a useless one and one which gives us the flag. Neat!

Made with love by: AndreiCat