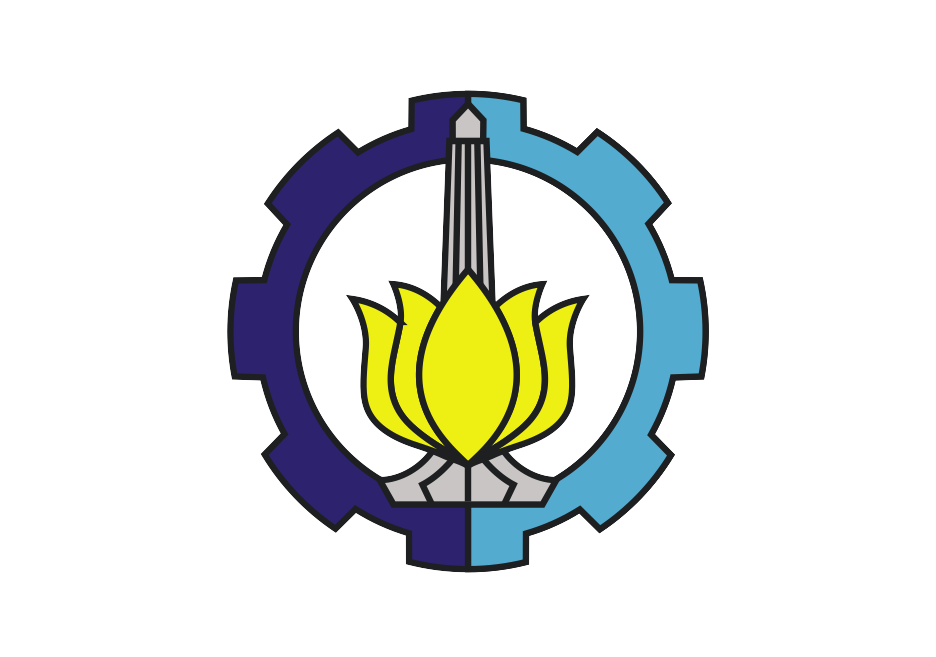
Laporan Pengerjaan Lab Praktikum

Ethical hacking



Nama : Gilang Raya Kurniawan

NRP : 5027221045

Daftar Isi

[Disclaimer](#_30j0zll) ……………………………………………………………………………………………………………...

[Contact Information](#_1fob9te) ……………………………………………………………………………………………………

[Mengidentifikasi Tingkat Kerentanan ……………………………………………………………………](#_3znysh7)…………….

Context […………………………………………………………………………………………………………](#_tyjcwt)………

Scope…………………………………………………………………………………………………………………...

Tujuan dan Batasan…………………………………………………………………………………………………….

Larangan ………………………………………………………………………………………………………………..

Metodologi ……………………………………………………………………………………………………………..

[Rangkuman Kerentanan & Rapor ……………………………………………………………………………………...](#_3dy6vkm)

# 

# **Disclaimer**

Pengerjaan Praktikum 2 kali ini dilaksanakan dalam periode selama tiga hari, dimulai dari tanggal 28 Mei 2024 hingga 1 Juni 2024. Pengerjaan praktikum bertujuan untuk menemukan kerentanan IP web yang di berikan dengan menggunakan prinsip prinsip ethical hacking

# 

# **Contact Information**

| **Name** | **Title** | **Contact Information** |
| --- | --- | --- |
| Peserta | | |
| Gilang Raya Kurniawan | Mahasiswa Teknologi Informasi Angkatan 2022 | Email: gilangraya869@gmail.com |

# 

# **Mengidentifikasi Tingkat Kerentanan**

| 0 | 0 | 0 | 0 | 0 |
| --- | --- | --- | --- | --- |
| Critical | High | Moderate | Low | Informational |

| **Penemuan** | **keparahan** | **Rekomendasi** |
| --- | --- | --- |
| Internal Penetration Test | | |
| - | - | - |

# 

# **Context**

Anda adalah seorang ahli keamanan yang ditugaskan oleh perusahaan konsultan keamanan SafeGuard Solutions untuk melakukan penetration testing terhadap aplikasi mockup bank yang masih dalam tahap development, yang disebut Jay’s Bank. Tujuan dari praktikum ini adalah untuk menemukan kerentanan yang mungkin ada dalam aplikasi dan melaporkannya untuk perbaikan sebelum aplikasi diluncurkan ke publik.

**Scope**

1. IP Address Aplikasi: 167.172.75.216
2. Semua fungsi aplikasi.
3. Mekanisme akun pengguna dan autentikasi.
4. Antarmuka web dan API.
5. Interaksi database dan proses penanganan data.

# **Tujuan dan Batasan**

1. Anda diizinkan untuk mencari dan mengidentifikasi kerentanan dalam aplikasi Jay’s Bank.
2. Fokus pada kerentanan aplikasi seperti SQL injection, XSS, dan authentication/authorization issues.
3. Apabila memungkinkan, kerentanan yang ditemukan dapat di-exploit untuk mengakses akun pengguna lain, tetapi hanya sebatas aplikasi (tidak ke server).

# **Larangan**

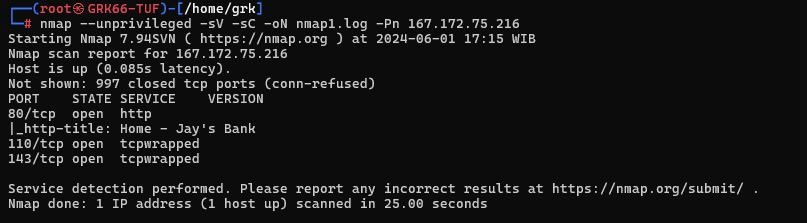
1. Tidak diperbolehkan untuk melakukan serangan yang dapat merusak data atau infrastruktur aplikasi.
2. Tidak diperbolehkan untuk mengeksploitasi kerentanan yang dapat memberikan akses ke server (contoh: RCE, privilege escalation).
3. Hindari serangan DoS/DDoS yang dapat mengganggu ketersediaan layanan aplikasi.

# **Metodologi**

1. Gunakan metode non-destruktif dalam testing.
2. Selalu lakukan verifikasi dan validasi atas temuan kerentanan sebelum melaporkannya.
3. Simpan catatan rinci tentang semua langkah yang diambil selama testing.

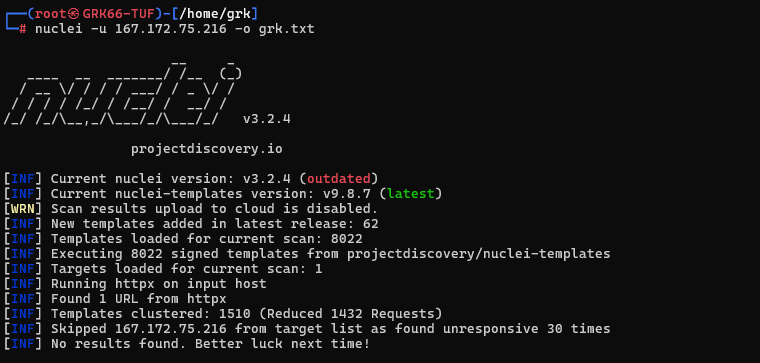
# **Rangkuman Kerentanan & Rapor**

1. Cara pertama

Coba cek IP address dengan melakukan memasukan command nmap ke terminal kali, nmap --unprivileged -sV -sC -oN nmap1.log -Pn 167.172.75.216

Ternyata tidak ditemukan kerentanan apapun

Cek dengan Nuclei nuclei -u 167.172.75.216 -o grk.txt



Sama ternyata tidak menemukan kerentanan

2. Cara kedua

Masuk ke website IP tersebut [http://167.172.75.216](http://167.172.75.216/register), lalu lakukan register terlebih dahulu, “bisa menggunakan kode seperti di bawah untuk melakukan register”

import requests

import json

url = "http://167.172.75.216/register"

data = {

'username': 'GilangRayaKurniawan',

'password': 'qwqw1212!@!@QWQW'

}

response = requests.post(url, headers={'Content-Type': 'application/json'}, data=json.dumps(data))

if response.status\_code == 200:

response\_data = response.json()

if response\_data.get('success'):

print("Registration successful!")

else:

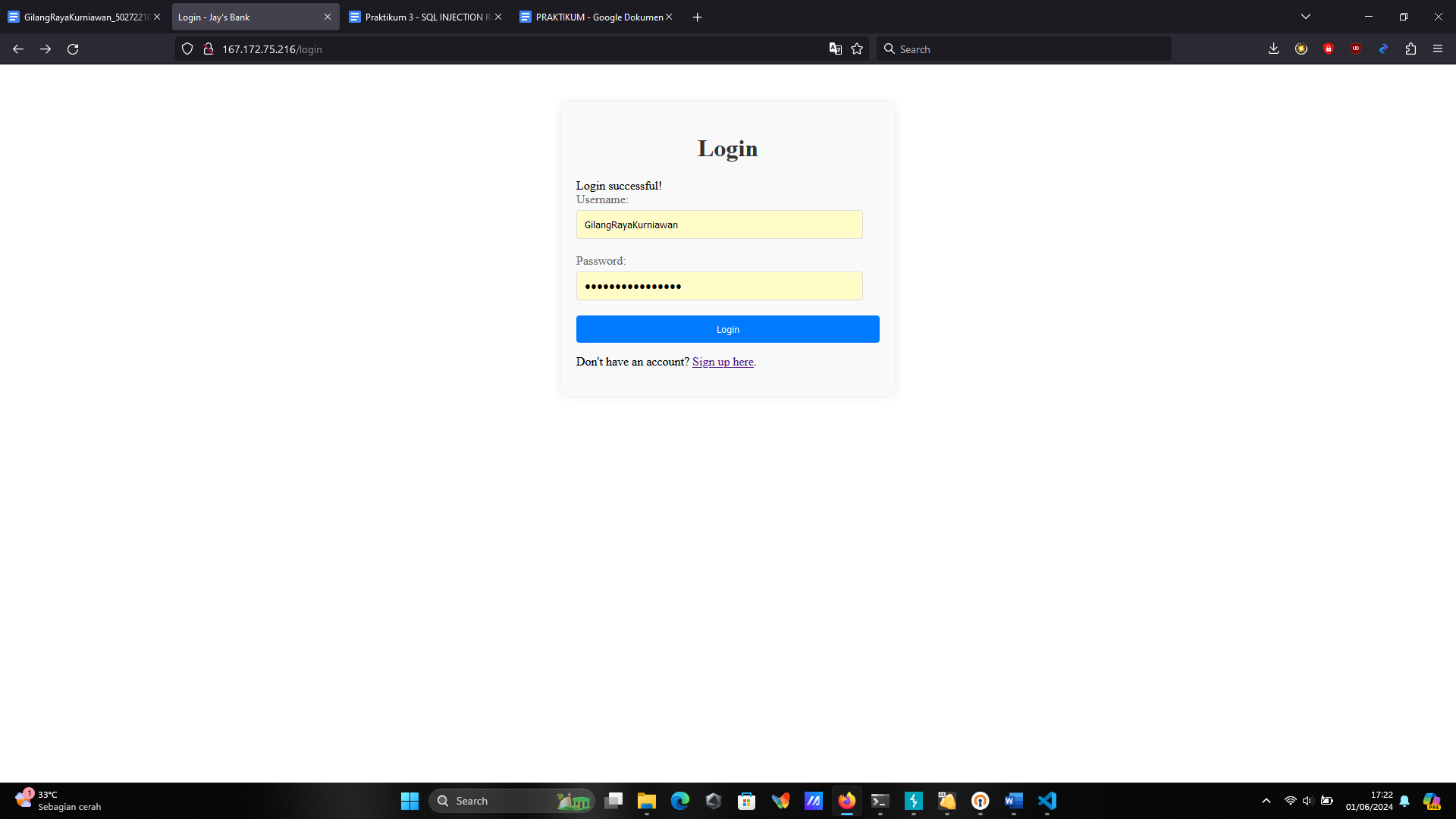
print(f"Registration failed: {response\_data.get('message')}")

else:

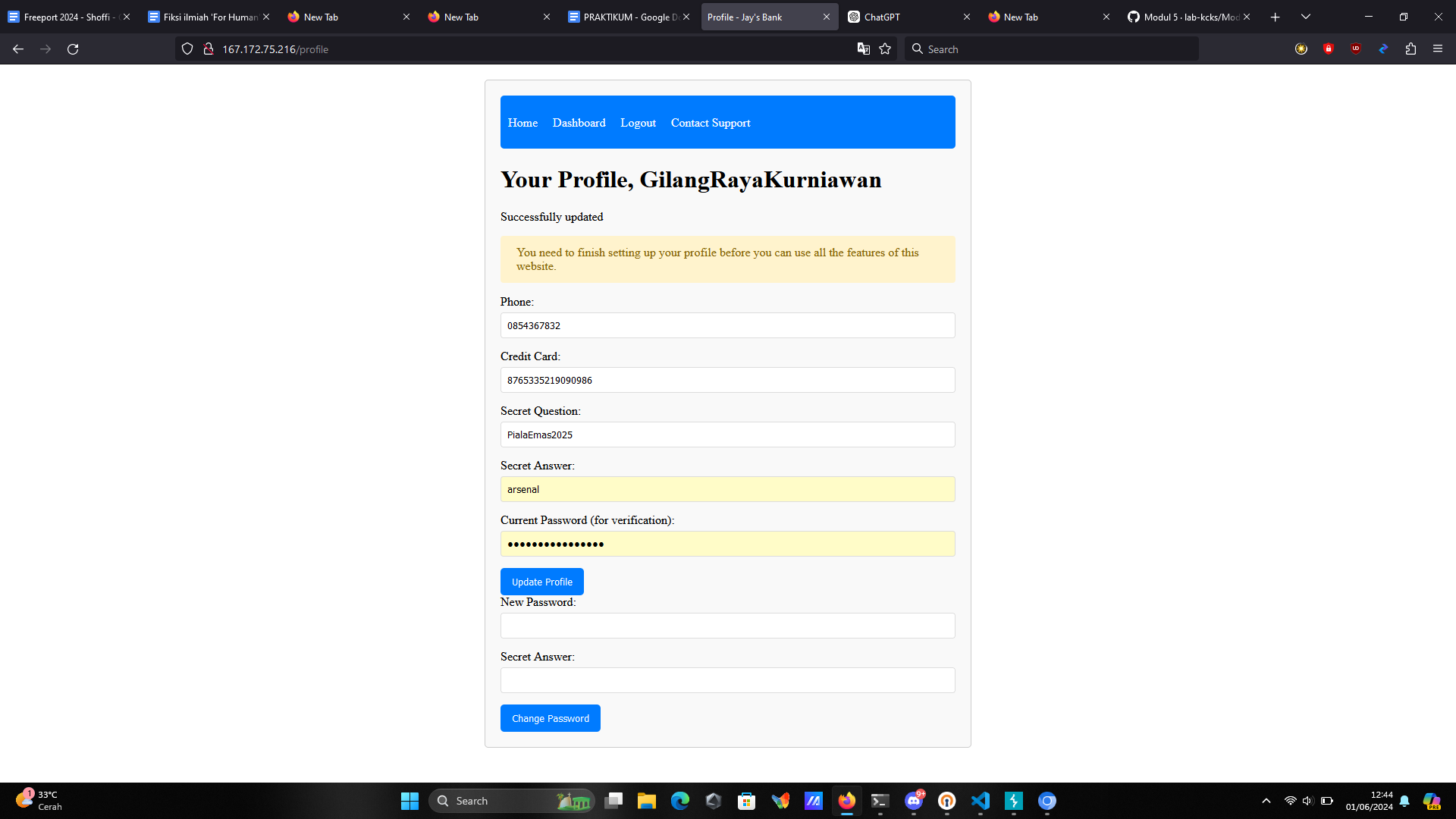
print(f"Registration failed with status code: {response.status\_code}")

print("Response:", response.text)

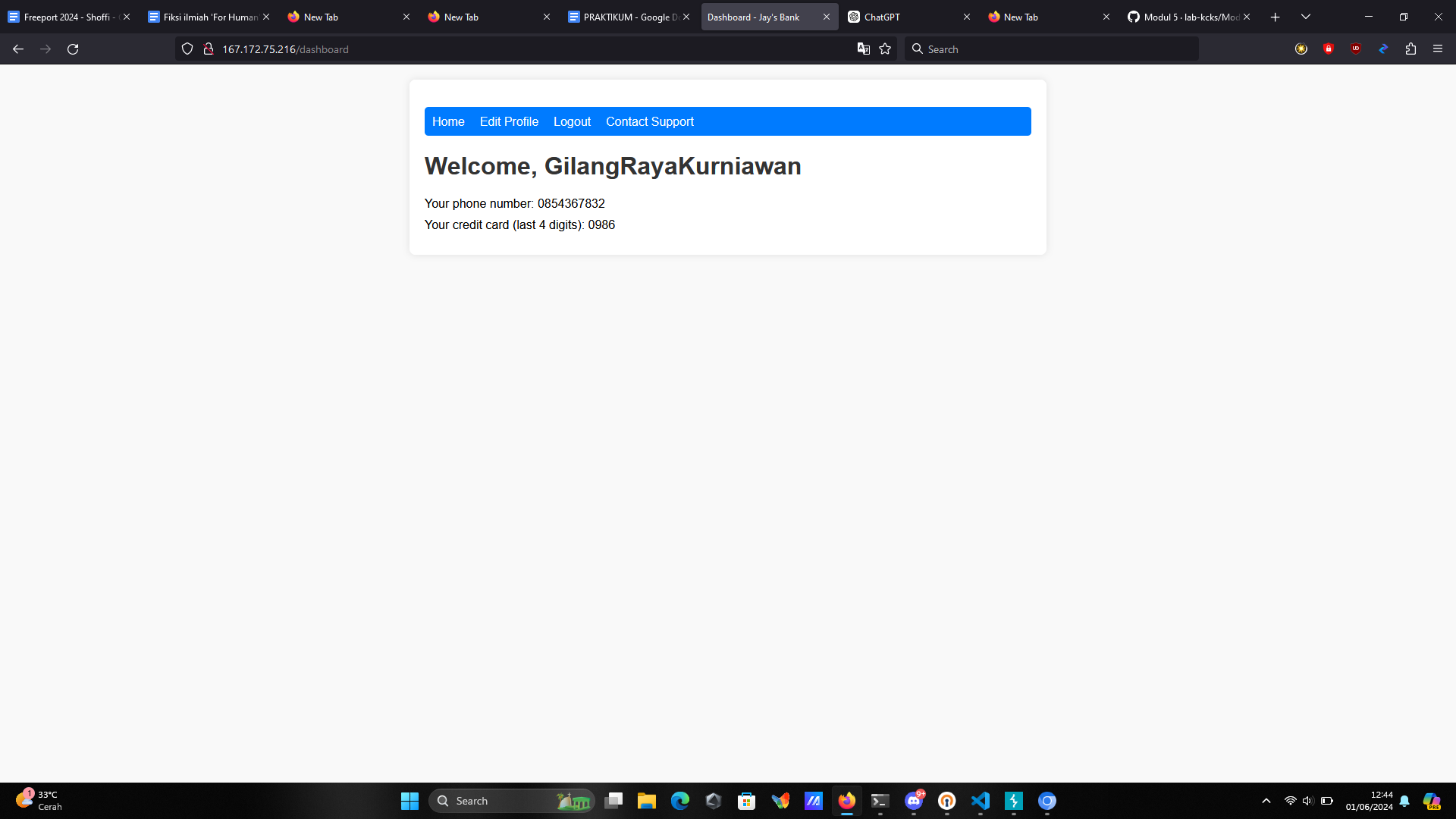
Setelah melakukan register lalu login/masuk pada halaman login web



Lalu masuk, saya masukkan data isi tabel tabel sesuai dengan yang anda mau, dengan maksimal jumlah angka nomor telepon 10 dan maksimal nomor kartu kredit 16



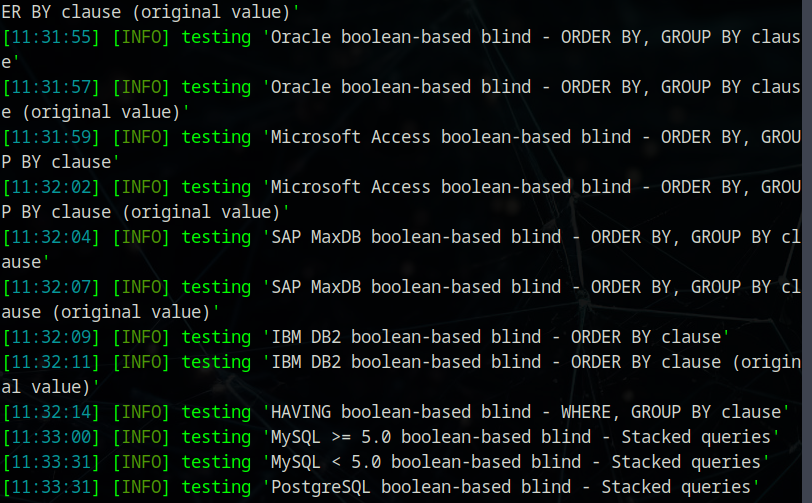
Save lalu cek di dashboard, apakah berhasil atau tidak



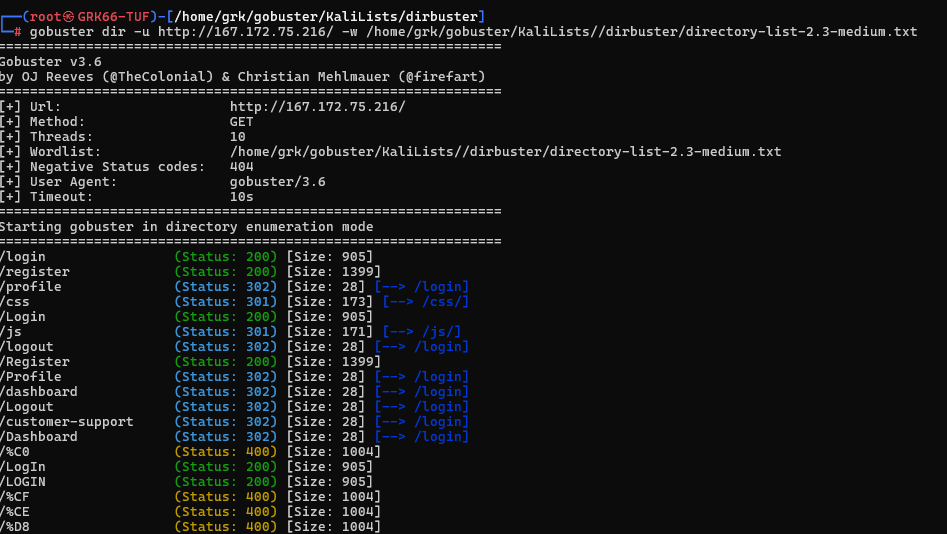
3. Cara ketiga

Gunakan SQLmap untuk merekon jenis sql apa saja yang ada pada IP tersebut gunakan command pada terminal parrot sqlmap -u "http://167.172.75.216/login" --level=5 --risk=3 --delay=1, lalu cek (mungkin memerlukan waktu yang lumayan lama karena alat tersebut untuk memetakan database, dan eksploitasi database)





4. Cara ke empat

Menggunakan gobuster dir dengan command, gobuster dir -u http://167.172.75.216/ -w /home/grk/gobuster/KaliLists//dirbuster/directory-list-2.3-medium.txt

Setelah dilakukan recon ternyata ada beberapa endpoint yang mungkin dapat diakses