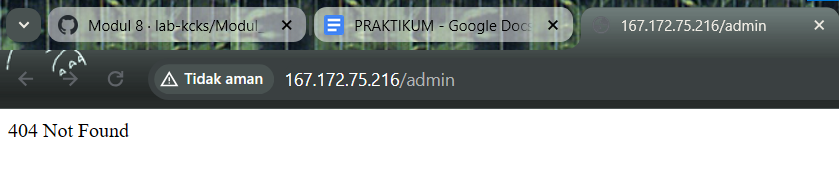
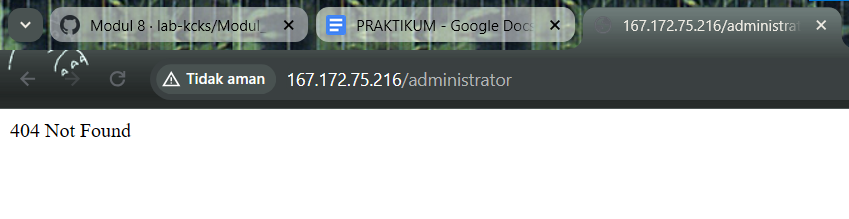
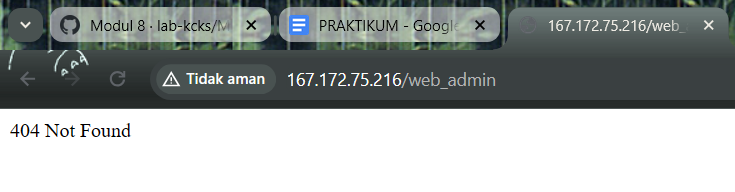
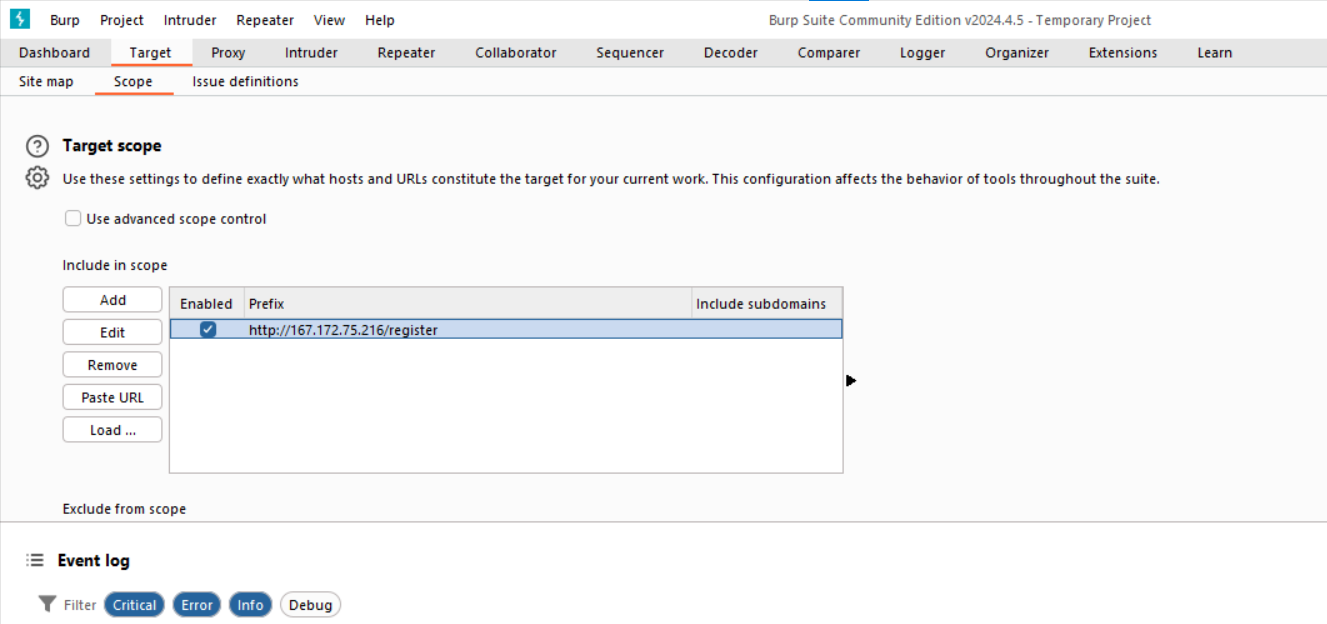
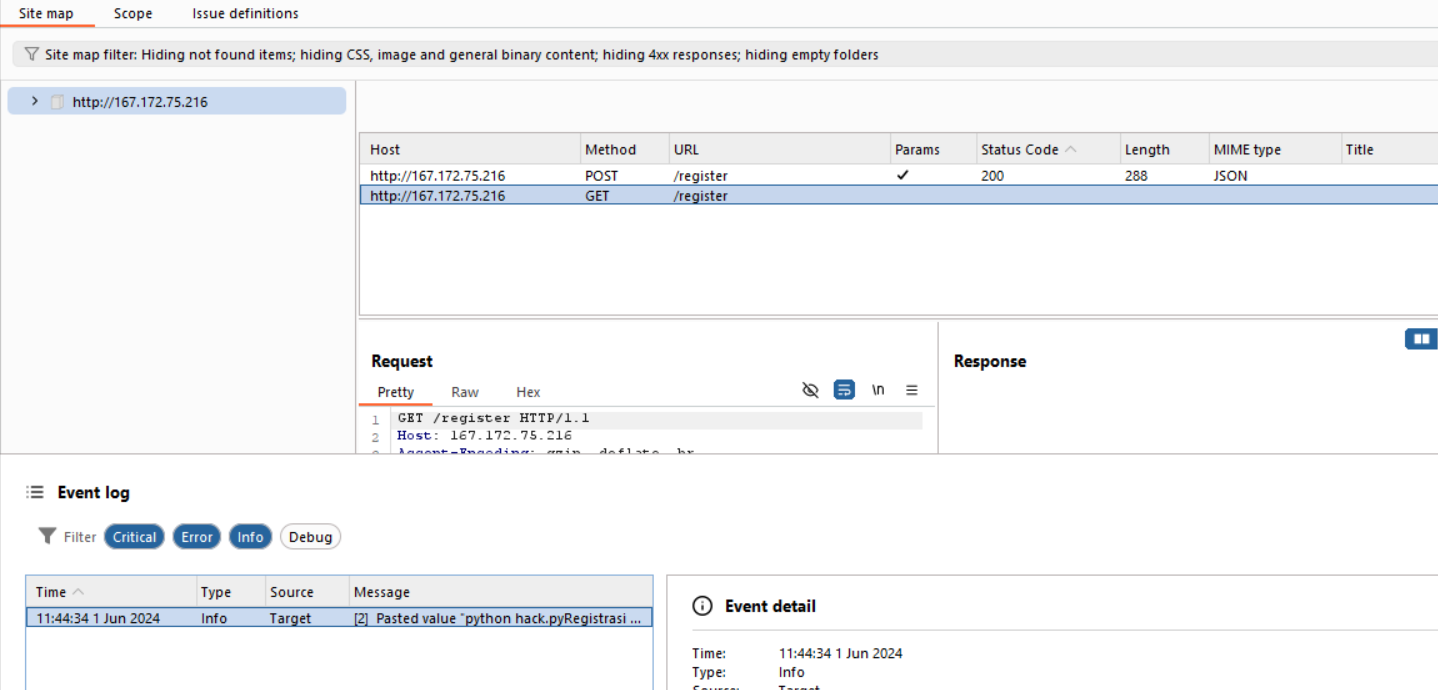
1. Mencoba apakah ada url yang bisa menembus role admin

Mencoba /admin 

, /administrator



, dan /web\_admin

1. Memanfaatkan burpsuite agar dapat register dengan menginputkan target nya  sudah ada centang pada parms menandakan berhasil, register dilakukan pada code berikut

**import** requests

**import** json

*# Konfigurasi proxy Burp Suite*

proxies **=** {

    'http'**:** 'http://127.0.0.1:8080'**,**

    'https'**:** 'http://127.0.0.1:8080'

}

*# Data registrasi*

register\_data **=** {

    'username'**:** 'siklunting'**,**

    'password'**:** 'Gu3st@ccess'**,**

    'email'**:** 'contoh@email.com'

}

*# Kirim permintaan registrasi*

register\_url **=** 'http://167.172.75.216/register'

headers **=** {'Content-Type'**:** 'application/json'}

response **=** requests**.**post(register\_url**,** **data=**json**.**dumps(register\_data)**,** **headers=**headers**,** **proxies=**proxies)

*# Periksa respons*

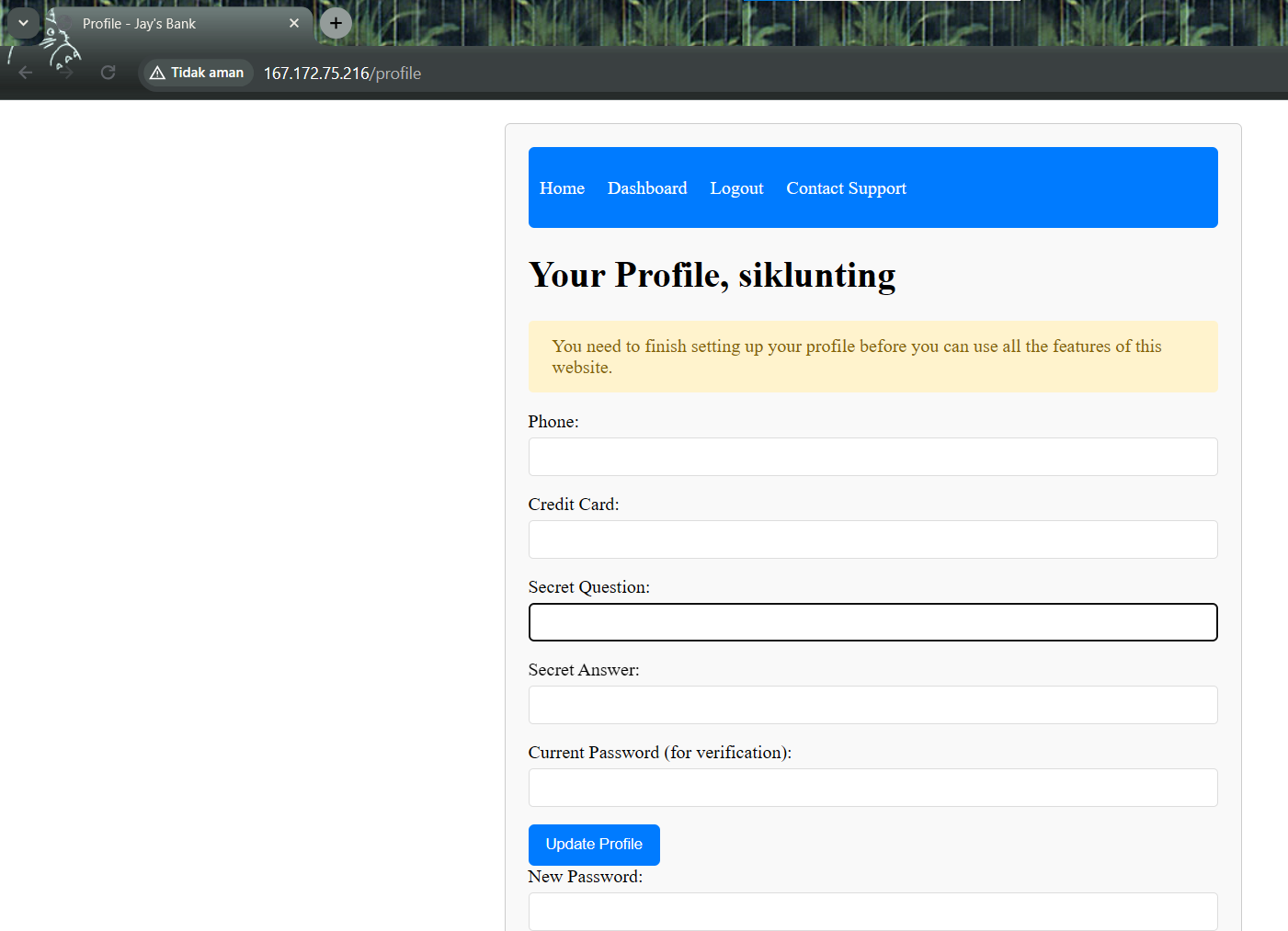
**if** response**.**status\_code **==** 200**:**

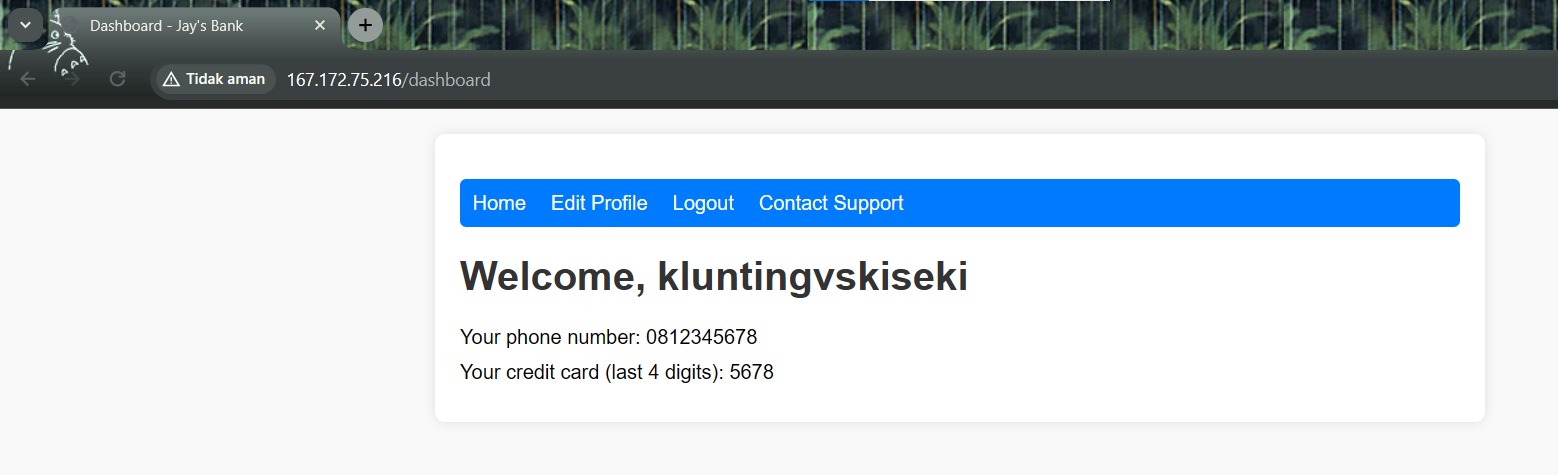
    print('Registrasi berhasil')

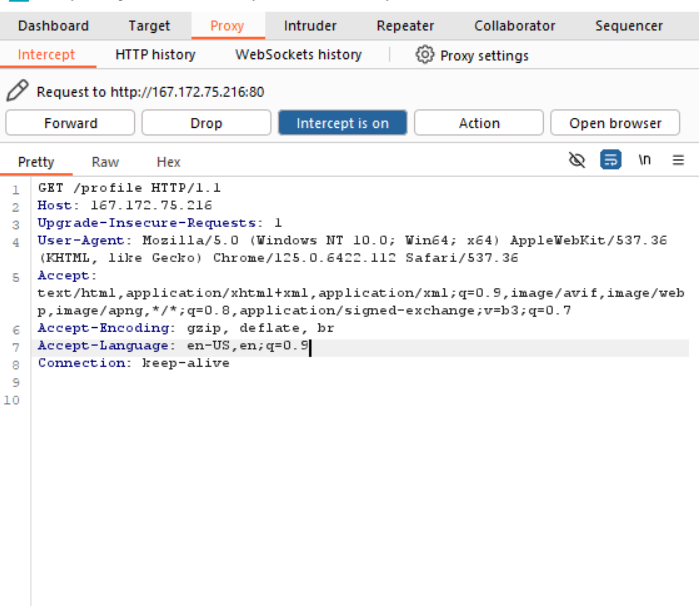
**else:**

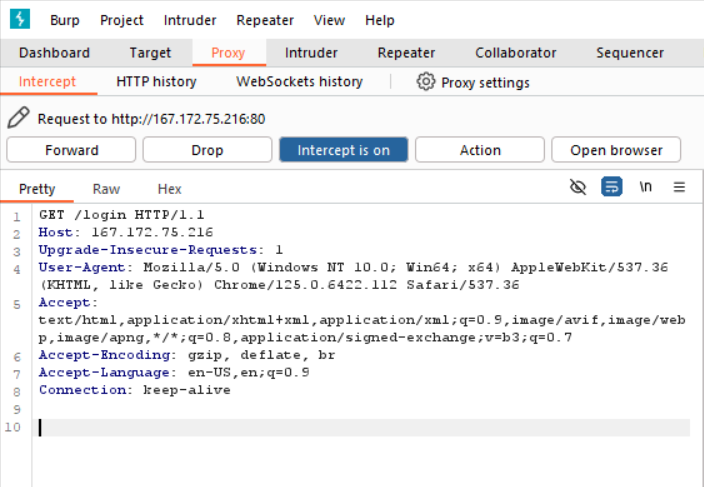
    print('Registrasi gagal')

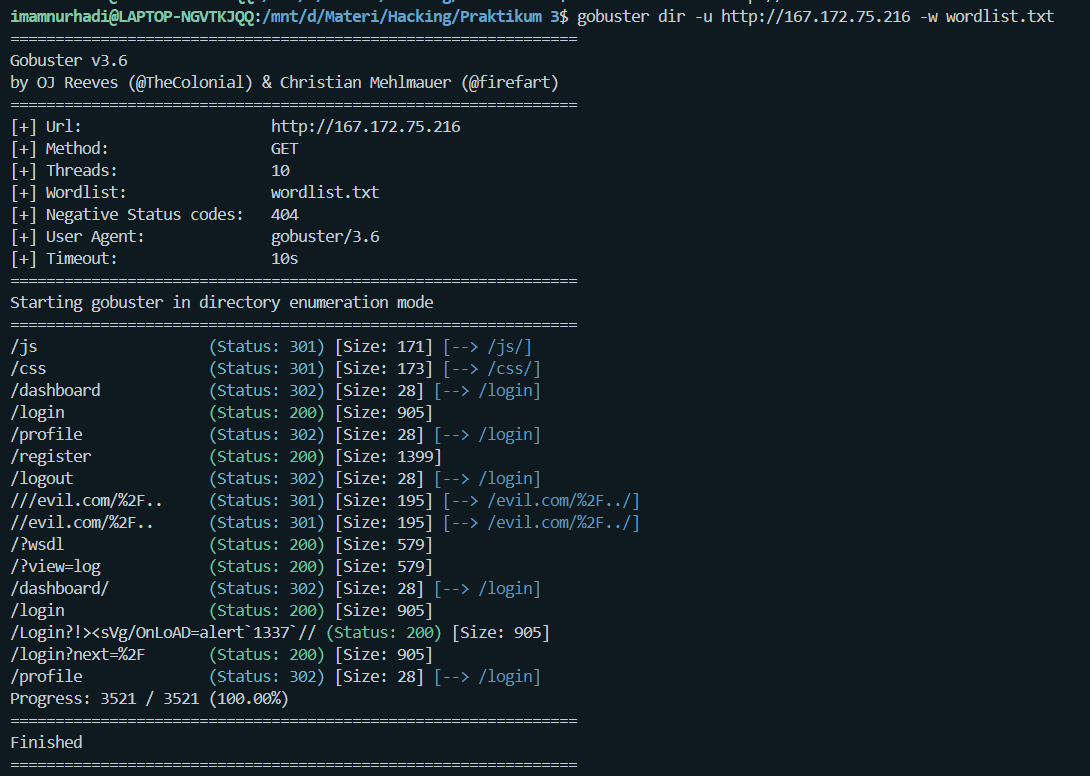
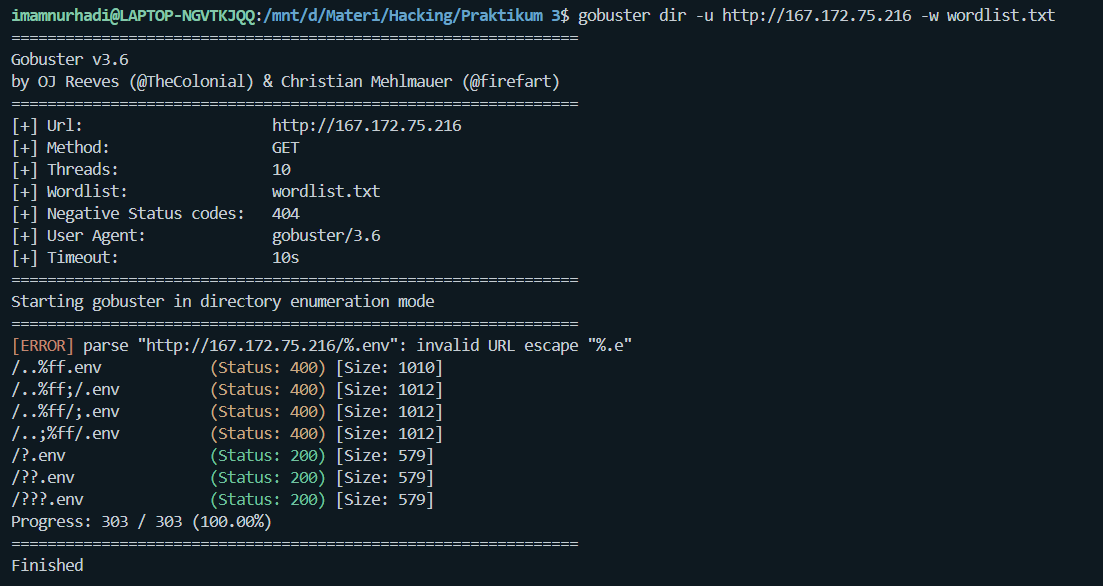
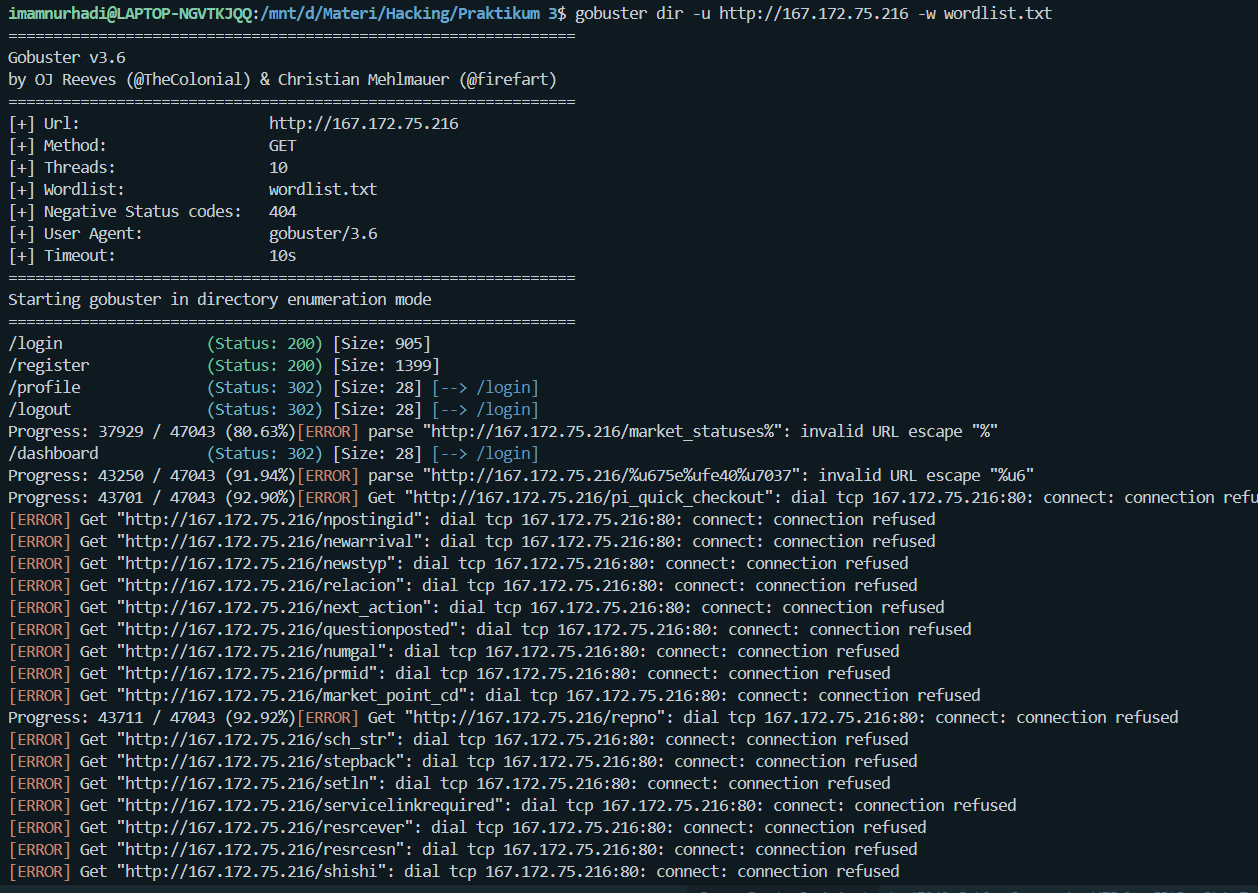
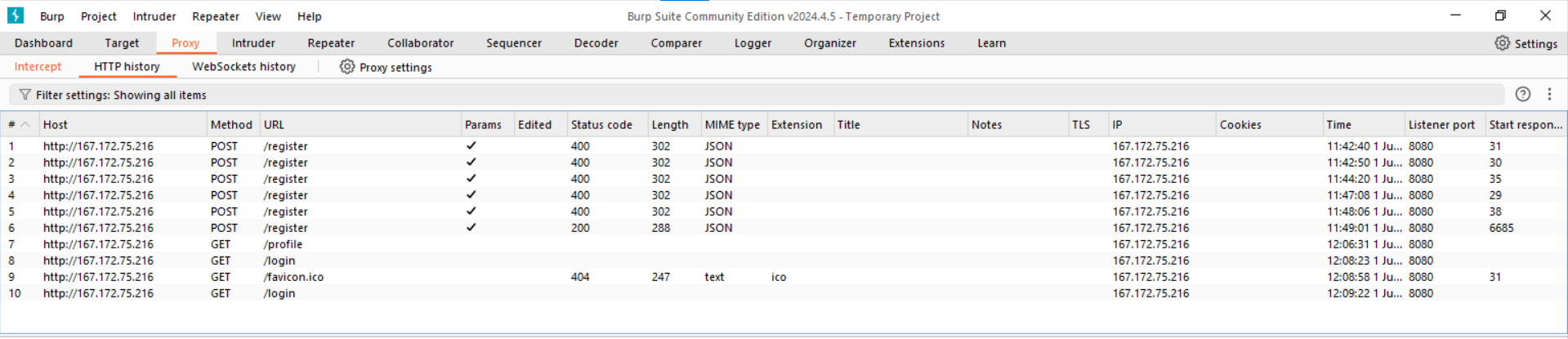
    print(response**.**text)

Namun, hal ini dapat dilakukan tanpa perlu melakukan burpsuite. Disini Kita tidak dapat membuka dashboard kecuali melakukan update profile degan memasukkan phone number dan kredit card. Jika tidak maka akan keluar 404 not found.

Setelah itu mencoba melakukan update profile 

1. Mencoba memasukkan ip ke burpsuite proxy untuk dilakukan intercept dan hasilnya sebagai berikut 



1. Menjalankan gobuster untuk mencari direktori yang ada   
2. Mencari tau history HTTP pada ip tersebut saat dijalankan 
3. Mencoba menginputkan script pada semua kolom input 