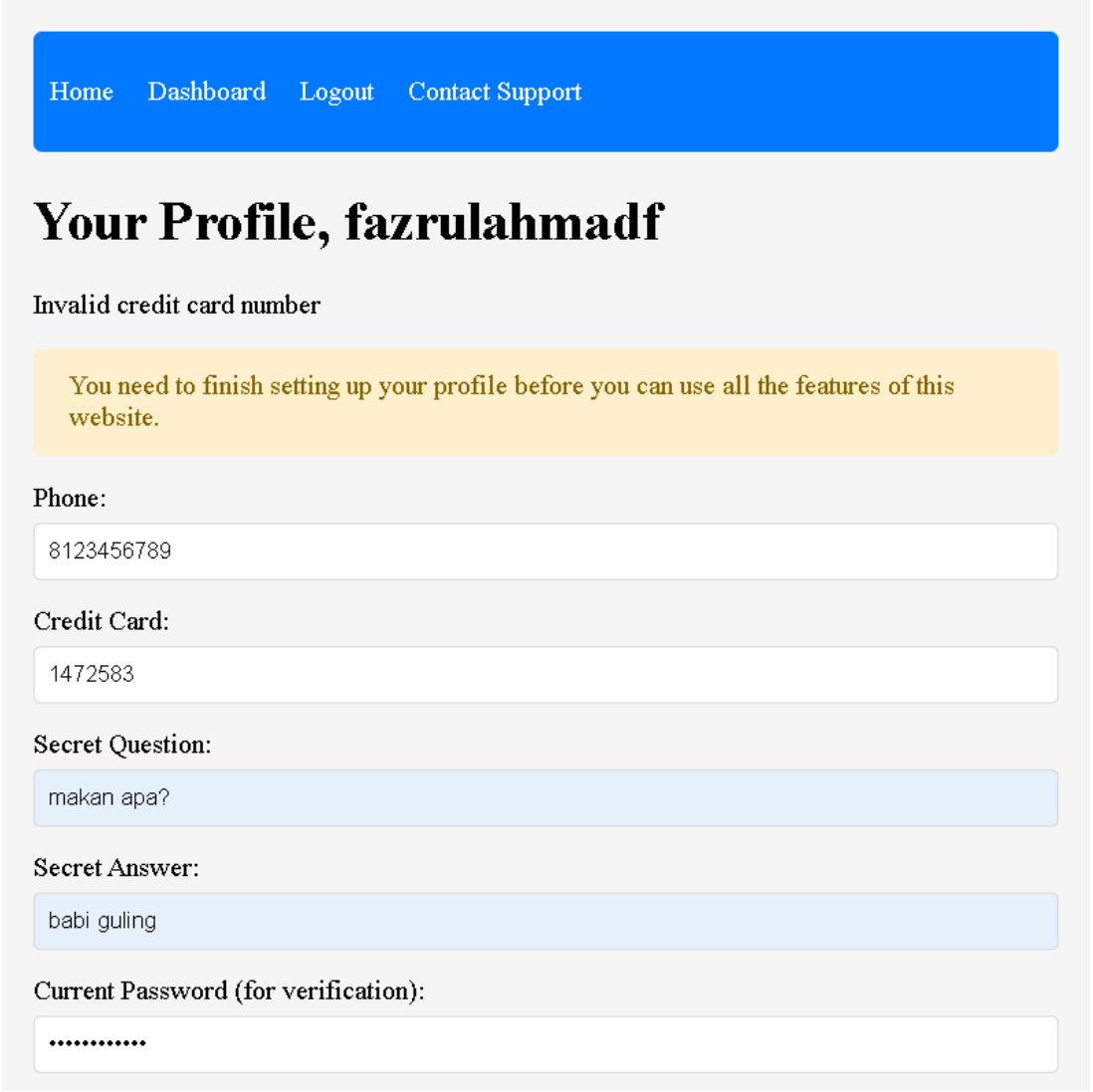
Dokumentasi Modul 3

A. Problem saat login



Saya udah coba berkali-kali untuk credit card number, tetep gak bisa updateprofile, pesan errornya invalid credit card number

B. Information Gathering

Saya menggunakan command whois untuk mendapatkan informasi tentang websitenya

```
inetnum:        167.172.0.0 - 167.172.255.255
netname:        DigitalOcean
descr:          DigitalOcean, LLC
country:        US
org:            ORG-DOI2-RIPE
admin-c:        PT7353-RIPE
tech-c:         PT7353-RIPE
status:         LEGACY
mnt-by:         RIPE-NCC-LEGACY-MNT
mnt-by:         digitalocean
created:        2003-06-26T15:46:32Z
last-modified:  2019-05-01T16:19:07Z
source:         RIPE

organisation:   ORG-DOI2-RIPE
org-name:       DigitalOcean, LLC
country:        US
org-type:       LIR
address:        101 Avenue of the Americas, 10th Floor
address:        New York
address:        10013
address:        UNITED STATES
phone:          +1 888 890 6714
mnt-ref:        digitalocean
mnt-ref:        RIPE-NCC-HM-MNT
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         digitalocean
abuse-c:        AD10778-RIPE
language:       EN
created:        2012-11-29T14:59:01Z
last-modified:  2020-12-16T13:24:44Z
source:         RIPE # Filtered

person:         DigitalOcean Network Operations
address:        101 Ave of the Americas, FL2
address:        New York, NY, 10013
address:        United States of America
phone:          +13478756044
nic-hdl:        PT7353-RIPE
mnt-by:         digitalocean
created:        2015-03-11T16:37:07Z
last-modified:  2022-08-23T13:31:16Z
source:         RIPE # Filtered
org:            ORG-DOI2-RIPE

% This query was served by the RIPE Database Query Service version 1.112 (ABERDEEN)
```

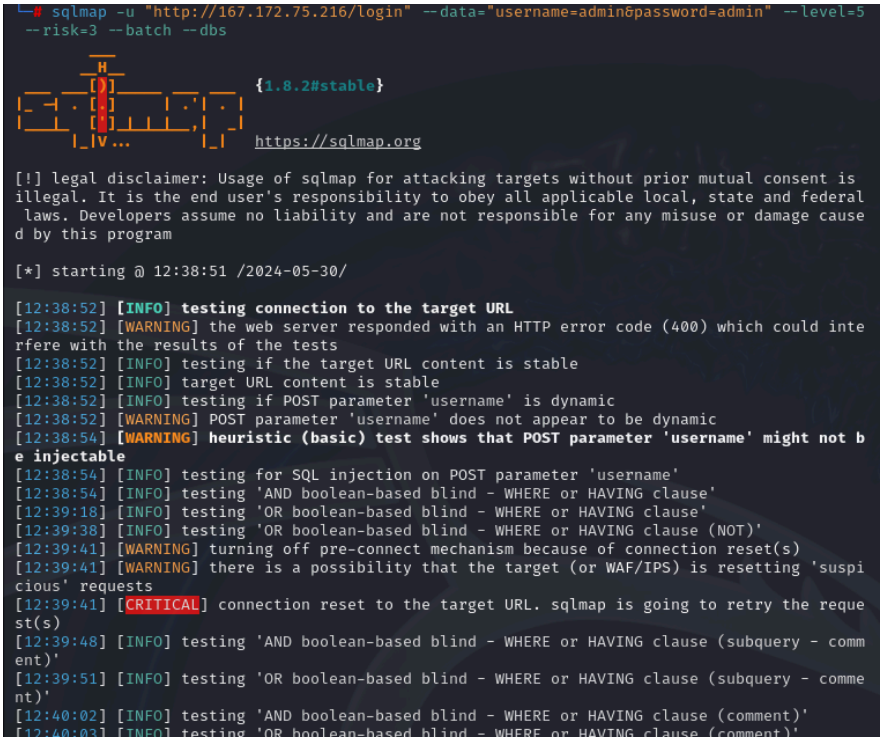
C. Gobuster

Menggunakan gobuster untuk mengetahui directory lists

```
└─# gobuster dir -u http://167.172.75.216/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://167.172.75.216/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/profile              (Status: 302) [Size: 28] [--> /login]
/register             (Status: 200) [Size: 1399]
/dashboard            (Status: 302) [Size: 28] [--> /login]
/login                (Status: 200) [Size: 905]
/css                  (Status: 301) [Size: 173] [--> /css/]
/js                   (Status: 301) [Size: 171] [--> /js/]
/logout               (Status: 302) [Size: 28] [--> /login]
/Hannes_Alfv%E9n      (Status: 400) [Size: 1016]
/Alfv%E9n_wave        (Status: 400) [Size: 1014]
/Enciclopedia_Libre_Universal_en_Espa%F1ol (Status: 400) [Size: 1042]
/mosquitologof%FCrshopfigurklein_3 (Status: 400) [Size: 1034]
Progress: 97590 / 141709 (68.87%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 97665 / 141709 (68.92%)
===============================================================
Finished
===============================================================
```

D. SQL I

Mencoba menggunakan SQLi dan hasilnya seperti ini:



Lalu saya mencoba menggunakan **--level=5 --risk=3 --tamper=space2comment --batch --dbs** dan hasilnya seperti ini:

Respon tersebut menunjukkan bahwa server mengembalikan error 400 Bad Request, yang mungkin disebabkan oleh skrip tamper atau masalah lain dengan format requesttingnya. Selain itu, parameter tersebut tidak tampak dapat diinject berdasarkan tes awal.