BÀI TẬP CTF

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

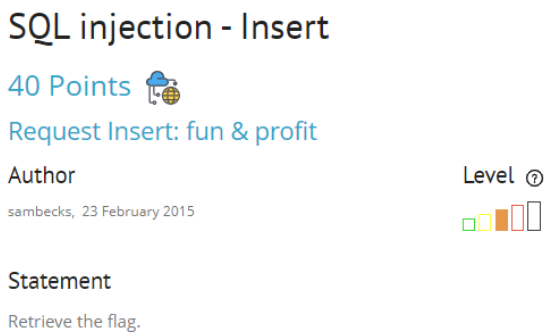
Giảng viên hướng dẫn: *Đỗ Hoàng Hiển*

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

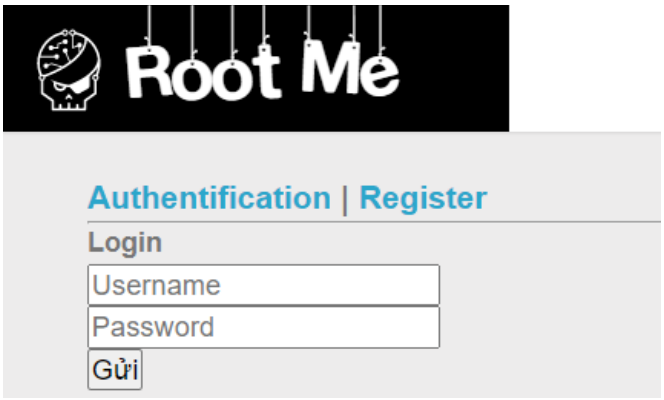
Challenge 8: SQL injection - Insert (level medium)

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

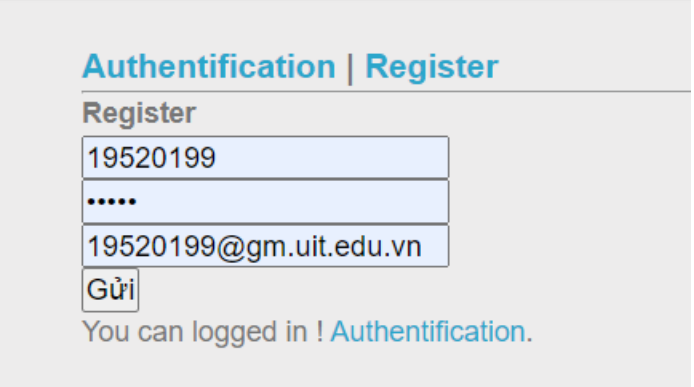
- Bài này yêu cầu ta lấy flag



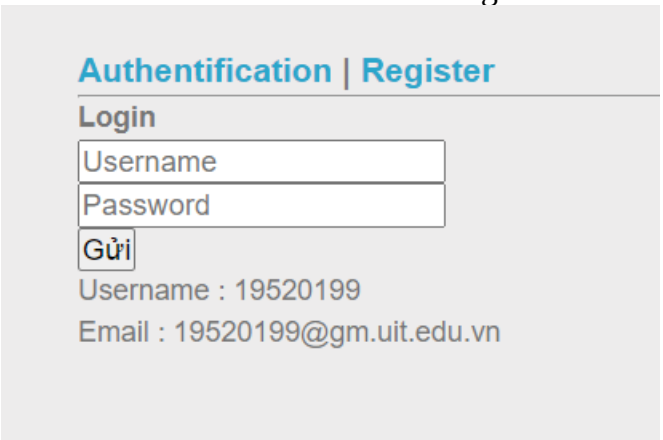
- Truy cập vào thử thách



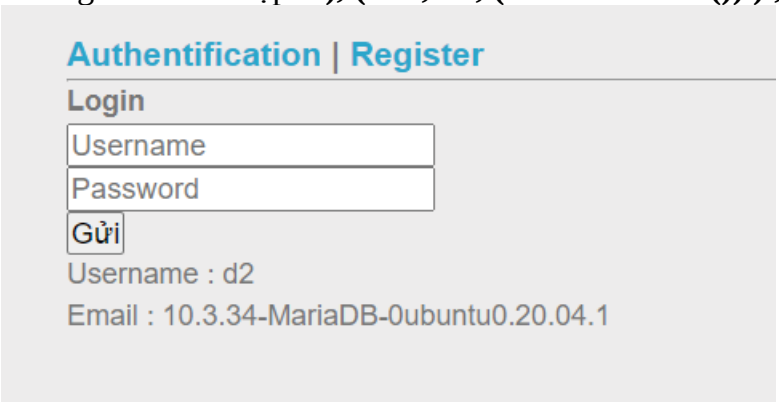
- Ta thấy có 2 tab là Authentification và Register
- Thử đăng ký 1 tài khoản



- Sau đó ta sang tab Authentification và tiến hành login với tài khoản vừa đăng ký

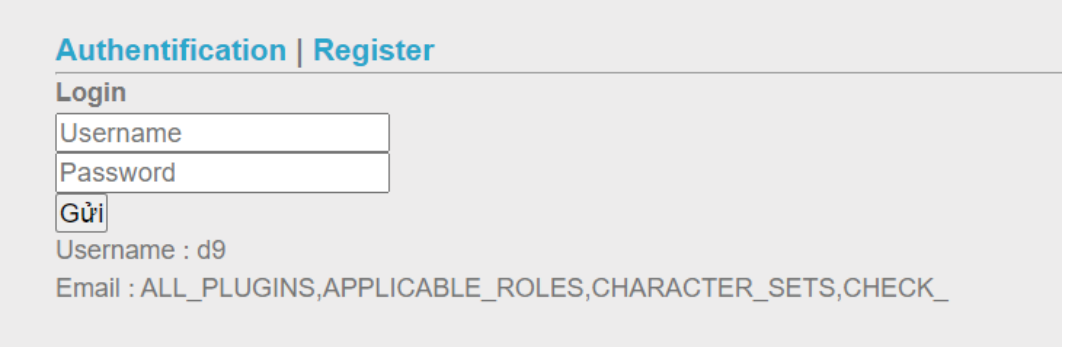


- Ta thấy username và email tương ứng của chúng ta xuất hiện sau khi bấm gửi
- Tìm hiểu về SQL Injection Insert thì ta biết được chúng ta sẽ cần truyền thêm 1 cặp giá trị vào data khi data được gửi lên server và nó sẽ lưu vào database
- Trường email là trường dễ bị tấn công, ta tiến hành đăng ký 1 tài khoản mới sao cho trong trường email ta nhập **1'), ('d2', '2', (select Version())) ;** -- -.



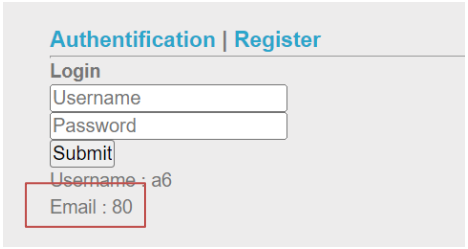
- Sau đó ta tiến hành đăng nhập với tài khoản d2 có password là 2 ta vừa tạo thì ta tìm thấy được version của database và server
- Dựa vào tên của database thì ta tìm được cú pháp truy vấp schema của nó.
- Tiếp theo ta tìm tên các table bằng việc nhập vào trường email như sau

1') , ('d9', '9', (select group_concat(table_name) from information_schema.tables)) ;
-- -



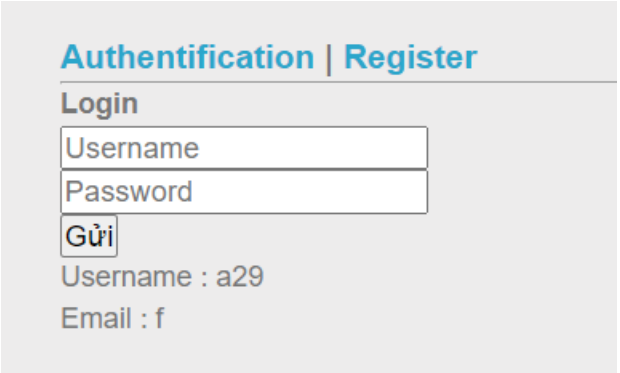
- Vì chương trình đã giới hạn số lượng được xuất ra, do đó ta sẽ phải tìm cách để xuất từng dòng table_name của schema này.
- Tiếp tục khai thác để tìm được số lượng các table

a'), ('a6', '1', (select group_concat(table_name) from information_schema.tables)) ; -- -



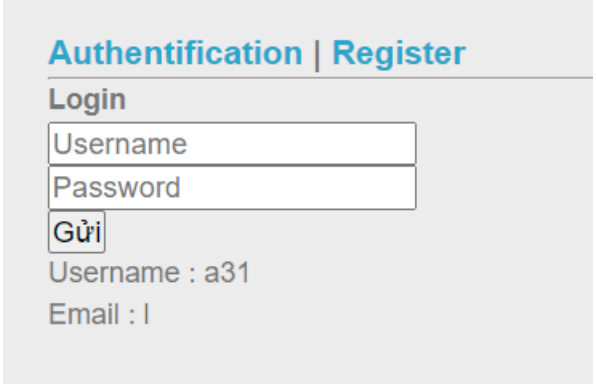
- Có thể thấy có tất cả 80 table.
- Có thể đoán là các table phía trên sẽ là mặc đinh, còn nếu thêm mới thì nó sẽ được add vào sau. Chúng ta sẽ kiểm tra các table phía gần cuối bằng các nhập vào trường email như sau

1') , ('a29', '1', (select char(ascii(table_name)) from information_schema.tables limit 79, 1)) ; -- -



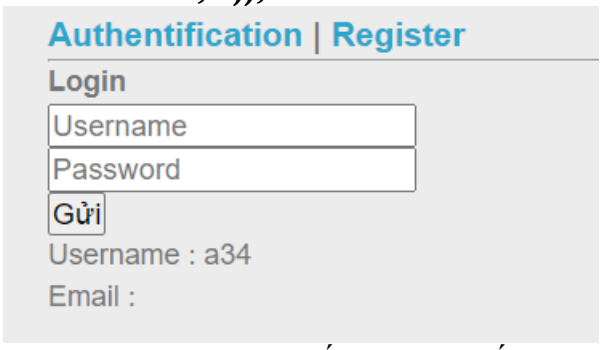
- Kết quả chỉ hiện một chữ cái là f với table thứ 79. Có thể đây là chữ f trong chữ flag nên ta sẽ tiếp tục kiểm tra table này.
- Tiếp tục khai thác như sau

1'), ('a31', '1',(select char(ascii(replace(table_name, 'f', ''))) from information_schema.tables limit 79, 1)); -- -



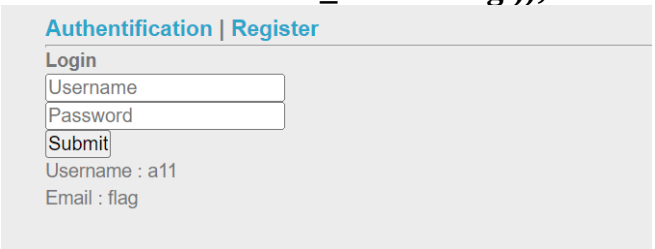
- Ta có với ascii("abc") thì sẽ trả về 97. ascii("bc") sẽ trả về 98, vậy chúng ta sẽ tìm tay từng kí tự trong tên của table bằng replace. Ta có replace("abc","a","") sẽ trả về "bc".
- Như vậy chúng ta sẽ tìm từng chữ cái của table_name bằng cách replace dần dần.

1'), ('a34', '1',(select char(ascii(replace(table_name, 'flag', ''))) from information_schema.tables limit 79, 1)); -- -



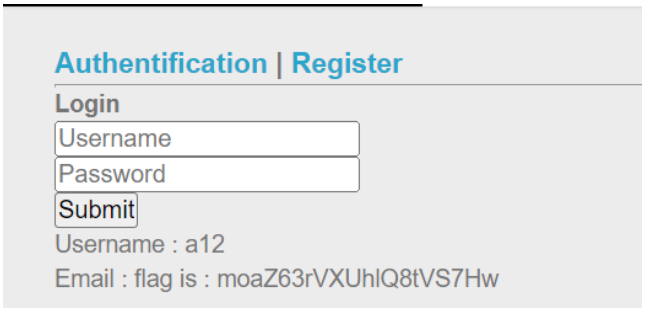
- Sau khi replace tới được flag thì kí tự tiếp theo đã trống, như vậy table_name là flag. Tiếp theo ta đi tìm column_name

1'), ('a11', '1', (select group_concat(column_name) from information_schema.columns where table_name='flag')); -- -

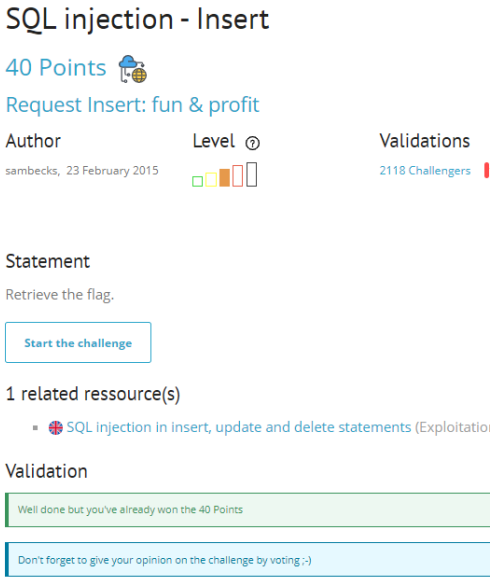


- Tương tự tìm table_name, tuy nhiên may mắn hơn là chỉ có 1 table nên không bị vượt quá kích thước output. Như vậy chúng ta đã tìm được table_name và column_name.
- Cuối cùng tìm flag, ta thực hiện truy vấn để tìm flag trong table và columns tìm được

1'), ('a12', '1', (select flag from flag)); -- -



- Ta tìm được flag là moaZ63rVXUhlQ8tVS7Hw, submit nó và ta thành công vượt qua thử thách



FLAG: moaZ63rVXUhlQ8tVS7Hw