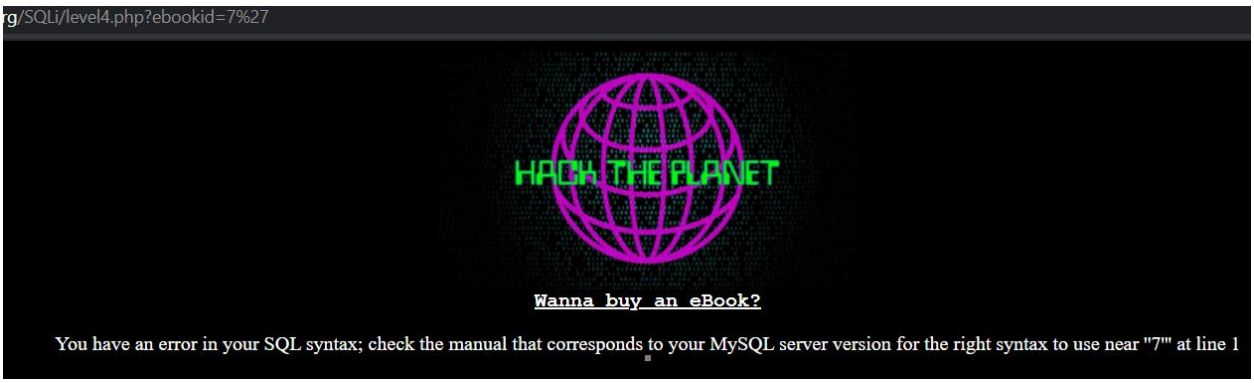
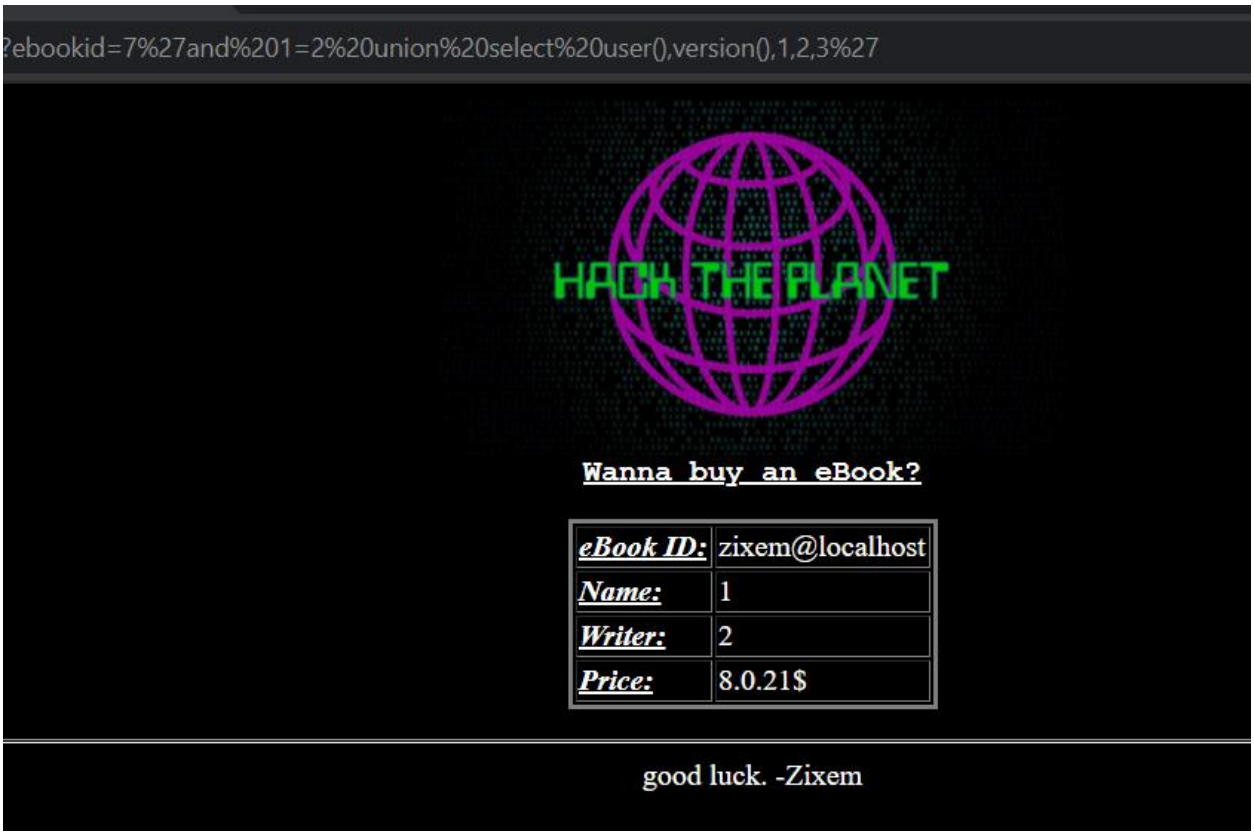
Đầu tiên kiểm tra kiểu input bằng thêm dấu ‘



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

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



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

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