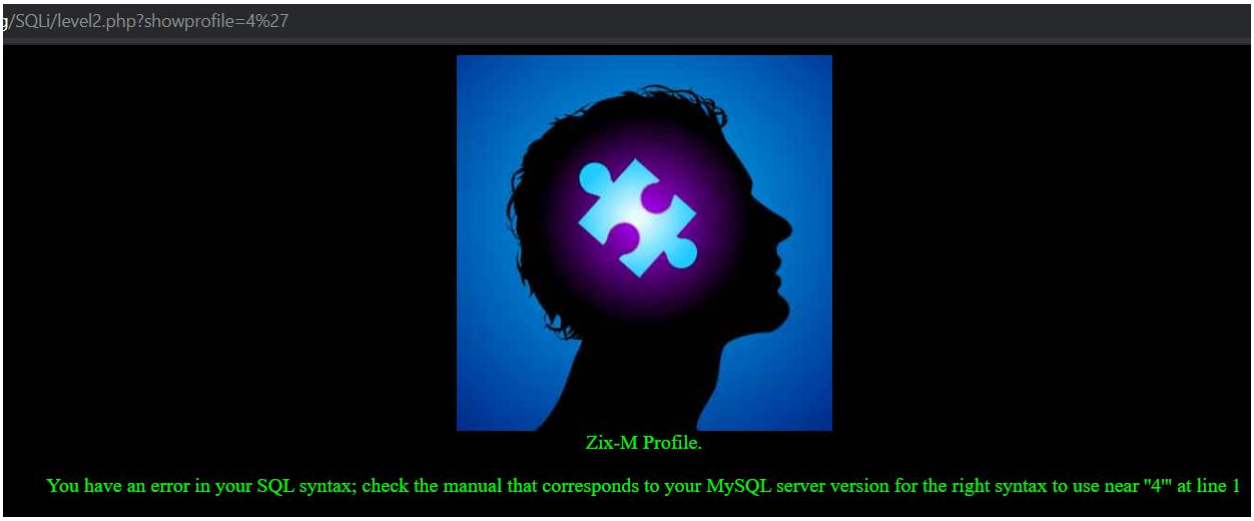
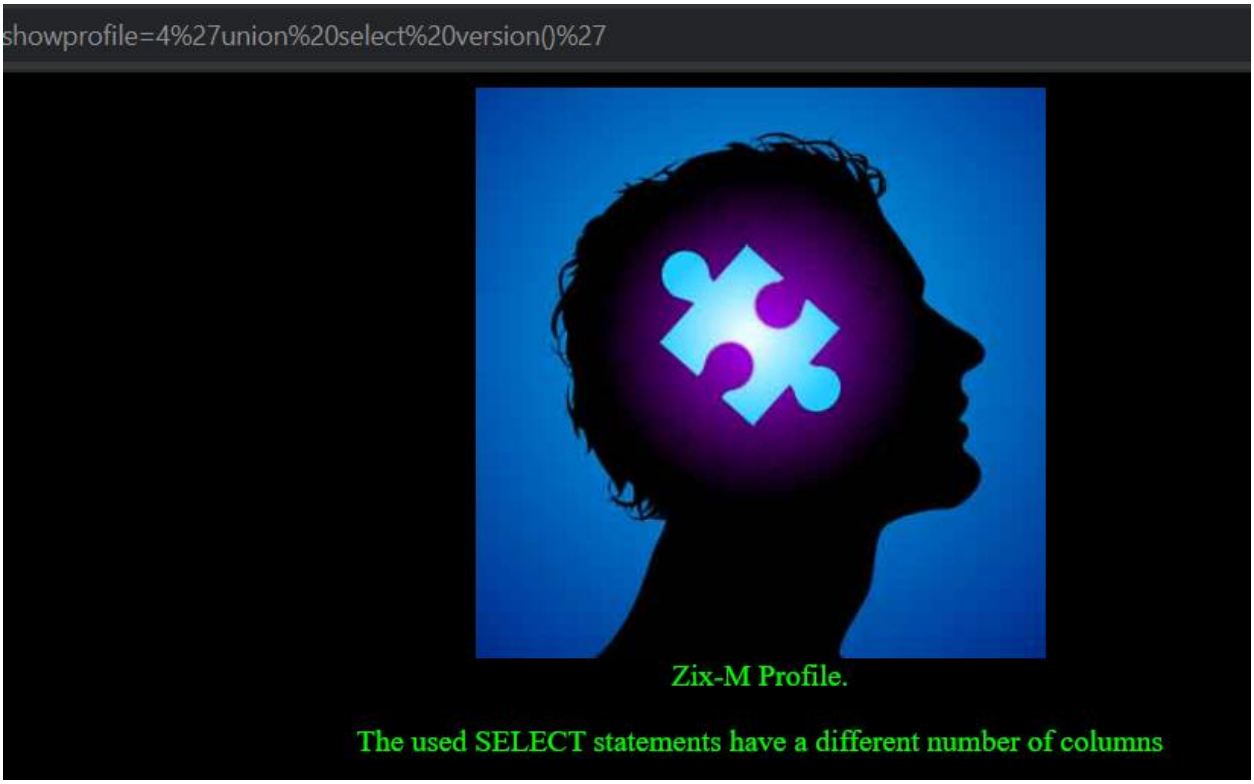
Đầu tiên thử thêm dấu ‘ để kiểm tra input đầu vào.



Kết quả cho thấy input là chuỗi nên ta cần thêm dấu ‘ để bypass query.

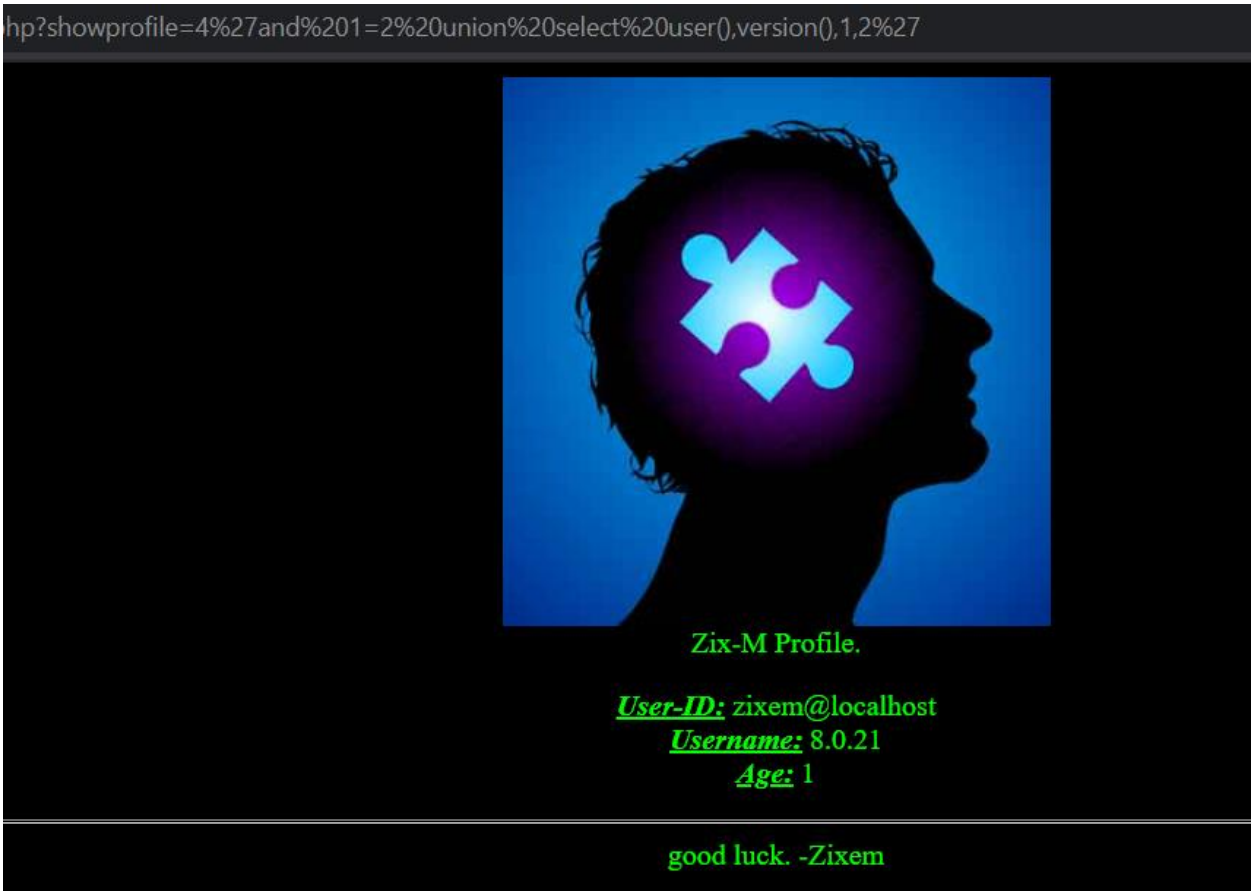
Payload: `showprofile=4'union select version()'`



Kết quả chứng tỏ query inject thành công nhưng chưa cùng số cột nên không show ra kết quả được.

Ta có thể dùng order by để dò tìm số cột hoặc làm luôn trong phần union select

Thử với `showprofile=4'union select user(),version(),1,2'` thì kết quả cho thấy table có 4 cột.



Dùng điều kiện `and 1=2` để bỏ kết quả của query ban đầu.

Payload: `‘and 1=2 union select user(),version(),1,2’`