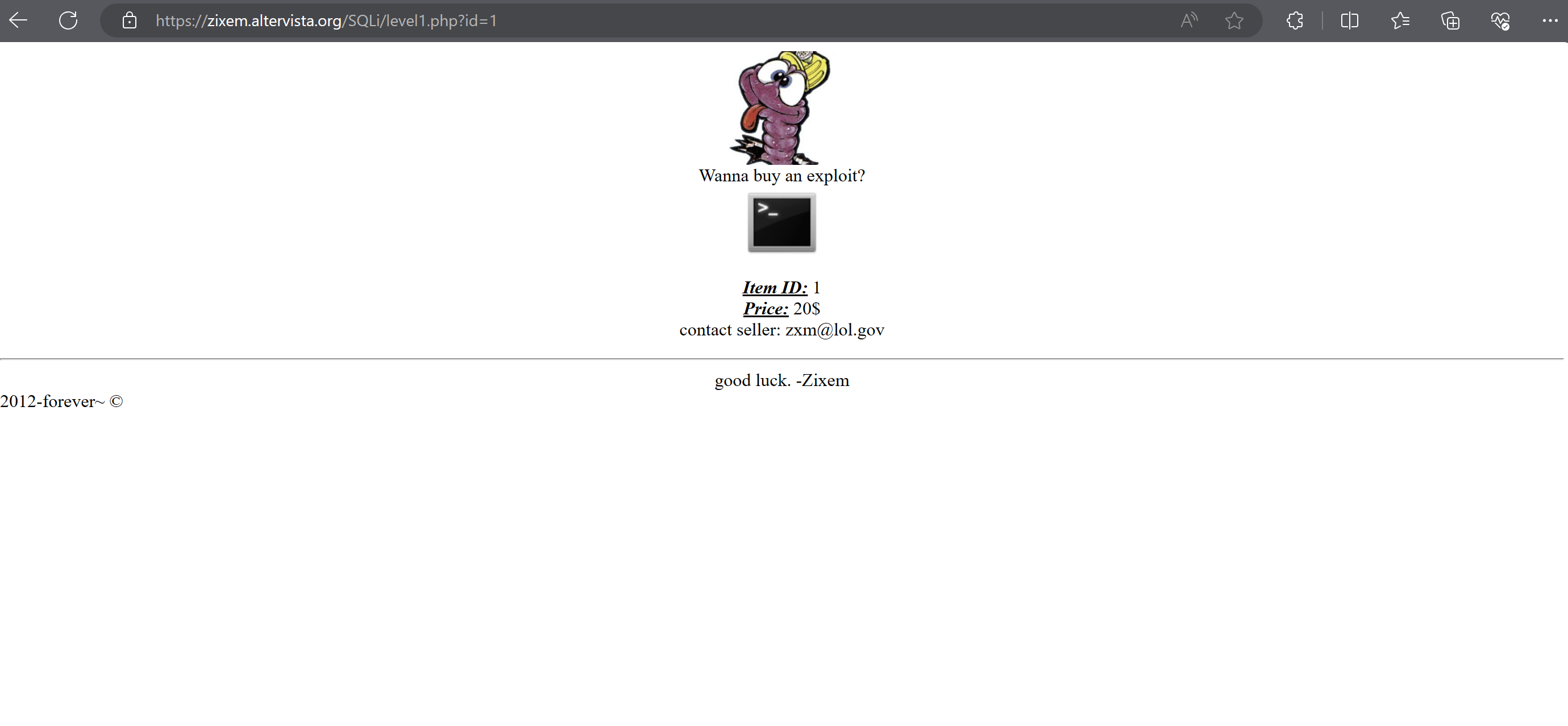
Level 1:

Ta thấy trang web có URL là: [**https://zixem.altervista.org/SQLi/level1.php?id=1**](https://zixem.altervista.org/SQLi/level1.php?id=1)

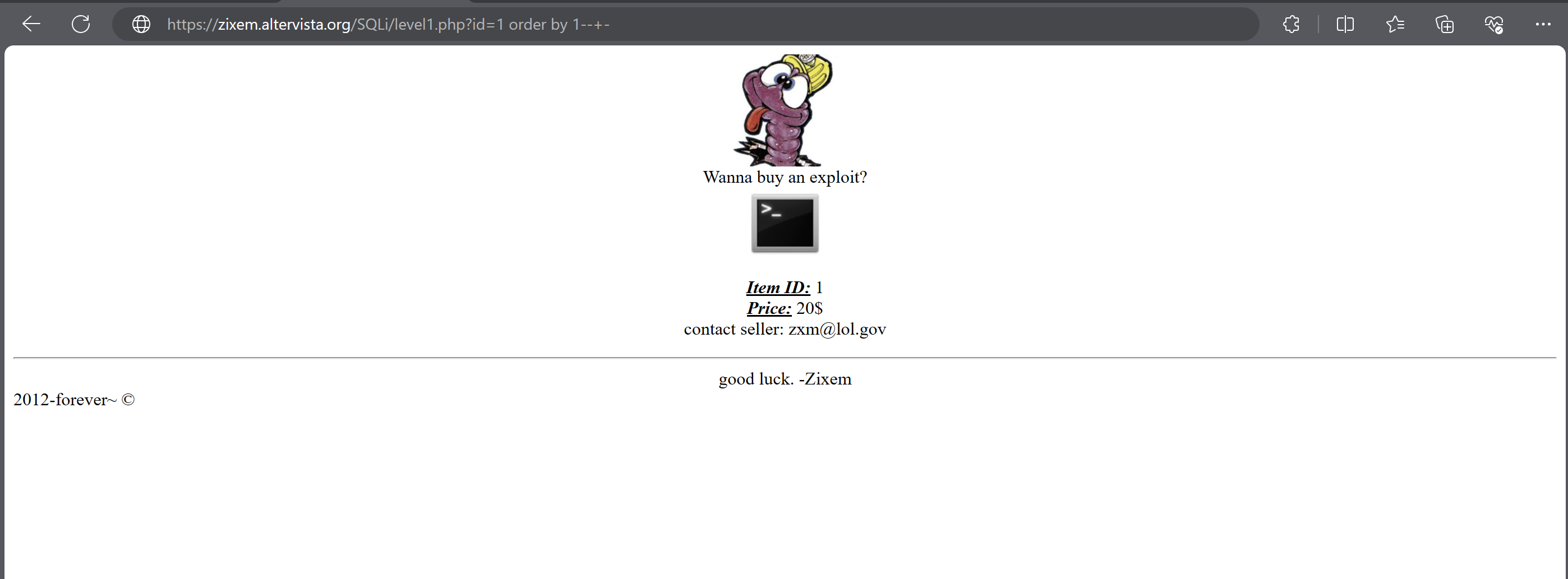


Ta thử thêm ký tự ‘ vào trong URL và quan sát kết quả

A screenshot of a computer

Description automatically generated

Ta nhận được dòng thông báo rằng cú pháp không hợp lệ. Tiếp theo, ta thực hiện tìm kiếm số lượng cột bằng order by



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

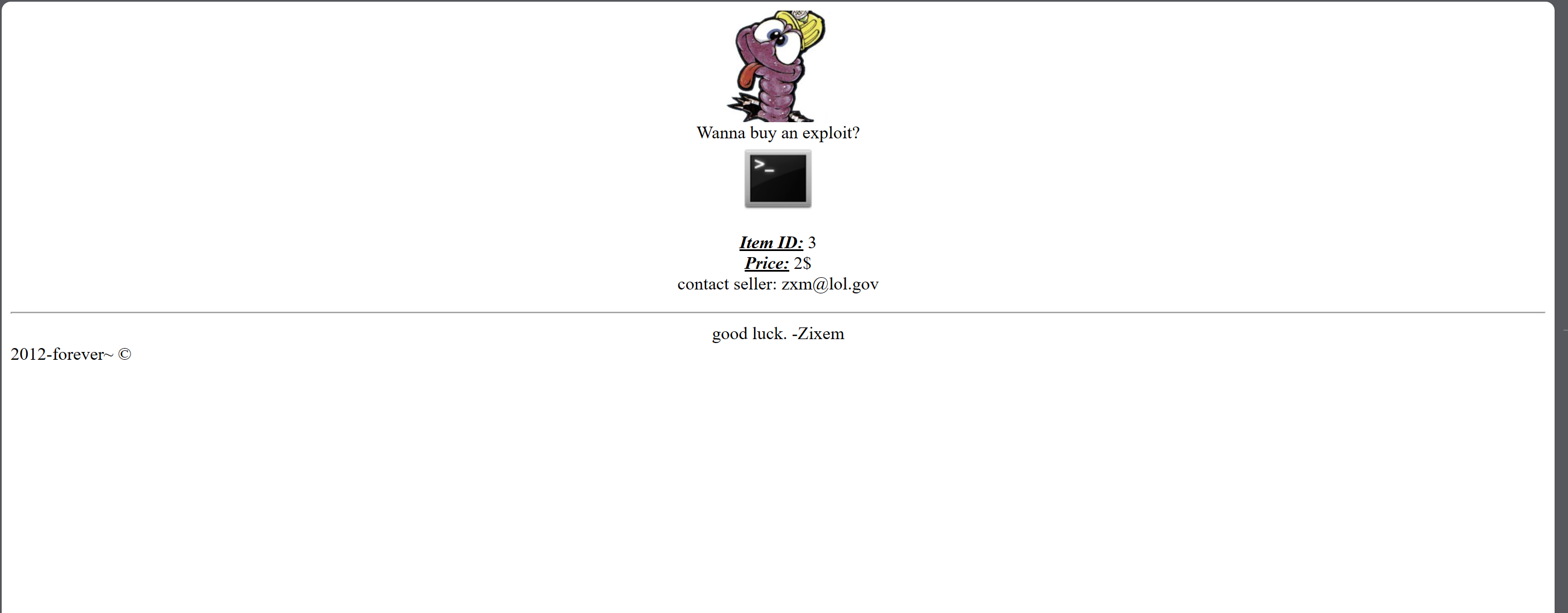
Ta thấy khi thực hiện order by đến cột thứ 4, ta nhận được thông báo “Unknown column '4' in 'order clause'”. Điều đó có nghĩa rằng có dữ liệu mà ta đang tương tác chứa 3 cột.

Ngoài ra, ta cũng có thể sử dụng phương thức group by để tiết kiệm thời gian tìm kiếm cột

A screenshot of a computer

Description automatically generated

Vì phần tử id ta không sử dụng đến, nên taa vô hiệu hóa id băng cách thêm biểu thức ‘1=2’ đằng sau id=1. Sau đó ta sử dụng lệnh ‘union select 2,3,4--+-’ để chèn 2,3,4 vào kết quả câu truy vấn.



Ta thấy chỉ có giá trị 3 và 2 xuất hiện lần lượt ở Item ID và Price, tức chỉ có 2 cột được hiển thị. Đề bài yêu cầu ta tìm kiếm user và version nên ta tiến hành thay đổi URL thành như hình dưới và nhận về kết quả

A screenshot of a computer

Description automatically generated

Ta nhận được kết quả user là zixem@localhost, version là 8.0.30. Vậy ta đã hoàn thành level 1.

Level 9

Ta có URL như sau: <https://zixem.altervista.org/SQLi/lvl9.php?id=1>

A screenshot of a computer

Description automatically generated

Ta thử thêm dấu ‘ vào sau URL để xem có điều gì xảy ra



Ta cũng nhận được 1 lỗi cú pháp như level trước. Bây giờ chúng ta bắt đầu tìm kiếm các cột, bắt đầu từ 1 cột, ta nhận được thông báo “different number of columns”

**A screenshot of a computer

Description automatically generated**

Tiếp theo ta thử 2 cột, ta thấy thông báo trên đã biến mất, vậy nên ta có thể suy đoán dữ liệu này bao gồm 2 cột. Để chắc chắn hơn, ta thử 3 và 4 cột



A screenshot of a computer

Description automatically generated

Như vậy, ta có thể kết luận rằng có 2 cột chứa trong dữ liệu này. Yêu cầu của đề bài là hiển thị ra /etc/passwd file. Ta thử đổi ký tự sau ngoặc đơn đầu tiên thành đường dẫn và xem kết quả.

A screenshot of a computer

Description automatically generated

Vậy ta đã hoàn thành level này