BÁO CÁO BÀI TẬP

**Môn học: Bảo mật Web và ứng dụng**

**Bài tập: SQLi**

*GVHD: Nghi Hoàng Khoa*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: NT213.O22.ATCL- Nhóm 3

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Bùi Hoàng Trúc Anh | 21521817 | 21521817@gm.uit.edu.vn |
| 2 | Lê Hoàng Oanh | 21521253 | 21521253@gm.uit.edu.vn |
| 3 | Nguyễn Ngọc Trà My | 21520353 | [21520353@gm.uit.edu.vn](mailto:21520772@gm.uit.edu.vn) |
| 4 | Huỳnh Minh Tân Tiến | 21521520 | 21521520@gm.uit.edu.vn |

1. **NỘI DUNG THỰC HIỆN:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Công việc** | **Kết quả tự đánh giá** |
| 1 | **Yêu cầu 1** | 100% |
| 2 | **Yêu cầu 2** | 100% |
| 3 | **Yêu cầu 3** | 100% |
| 4 | **Yêu cầu 4** | 100% |
| 5 | **Yêu cầu 5** | 100% |
| 6 | **Yêu cầu 6** | 100% |
| 7 | **Yêu cầu 7** | 100% |

**Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.**

BÁO CÁO CHI TIẾT

1. **Level 1 (Super Easy)**

**Ảnh có chứa văn bản, ảnh chụp màn hình, phim hoạt hình, Trang web

Description automatically generated**

Khi dùng order by để dò số lượng cột có trong bảng ta thấy khi nhập order by 4 thì nhận được lỗi, còn order by 3 thì không có lỗi. Như vậy bảng này gồm 3 cột.

Ảnh có chứa văn bản, ảnh chụp màn hình, phim hoạt hình, Trang web

Description automatically generated

Ảnh có chứa văn bản, ảnh chụp màn hình, phim hoạt hình, phần mềm

Description automatically generated

Chúng ta đã biết 1=1 là đúng còn 1=2 là sai như vậy nếu thêm AND 1=2 vào thì kết quả trả về sẽ rỗng.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, phim hoạt hình

Description automatically generated

Bây giờ chúng ta chỉ cần select để trả về thông tin của user và version:

Ảnh có chứa văn bản, ảnh chụp màn hình, phim hoạt hình, Website

Description automatically generated

1. **Level 2 (Easy)**

**A profile of a person with a puzzle piece in the middle

Description automatically generated**

Để trang in ra lỗi, chúng ta cần ngắt truy vấn sql và buộc ứng dụng đưa ra lỗi cho truy vấn không hợp lệ.

Ta có thêm kí tự ‘ vào cuối đường dẫn trang, thì trang sẽ hiện ra lỗi sau:

A silhouette of a person's head with a puzzle piece in the middle

Description automatically generated

Để thực hiện truy vấn đúng, chúng ta phải cân bằng truy vấn bằng cách thêm comment vào cuối đường dẫn.

Mọi thứ sau comments sẽ bị trình thông dịch SQL bỏ qua và chạy truy vấn thành công.

VD: select \* from username where id=‘1’-- -

Trong đó:

* '--' là cú pháp cho comment trong SQL. Khi SQL gặp dấu hai gạch ngang (--), nó sẽ hiểu rằng tất cả những gì sau nó trên cùng một dòng là một comment và sẽ bỏ qua chúng khi thực thi câu truy vấn.
* Việc sử dụng ‘-‘ giúp đóng chuỗi SQL đúng cách, đảm bảo rằng câu truy vấn là hợp lệ và không gây ra lỗi cú pháp.

Để lấy số cột ta có thể sử dụng ORDER BY. Chúng ta sẽ sử dụng cho đến khi gặp lỗi như “unknown column ’n’ in order clause’.

Thì khi ta thêm ORDER BY 5 vào cuối đường dẫn thì trang sẽ hiện ra lỗi sau. Vậy cái bảng có 4 cột.

A silhouette of a person's head with a puzzle piece in the middle

Description automatically generated

Khi truy vấn đầu tiên được đặt thành null và truy vấn thứ hai được chuyển với một số dữ liệu đầu vào do người dùng tạo ra. Ở đây chúng ta đã đặt phần đầu tiên của truy vấn là null và phần thứ hai là hợp lệ. Thì trình thông dịch SQL chỉ đưa ra kết quả của phần thứ hai.

SELECT \* FROM profiles WHERE SHOWPROFILE=-4’ UNION ALL SELECT 1,2,3,4--+-

A silhouette of a person's head with a puzzle piece in the middle

Description automatically generated

Ta có thể khai thác thông tin từ cột 1, 2, 3 của bảng.

Ở đây ta truy vấn user(), version() vào cột 2, 3 tương ứng của bảng.

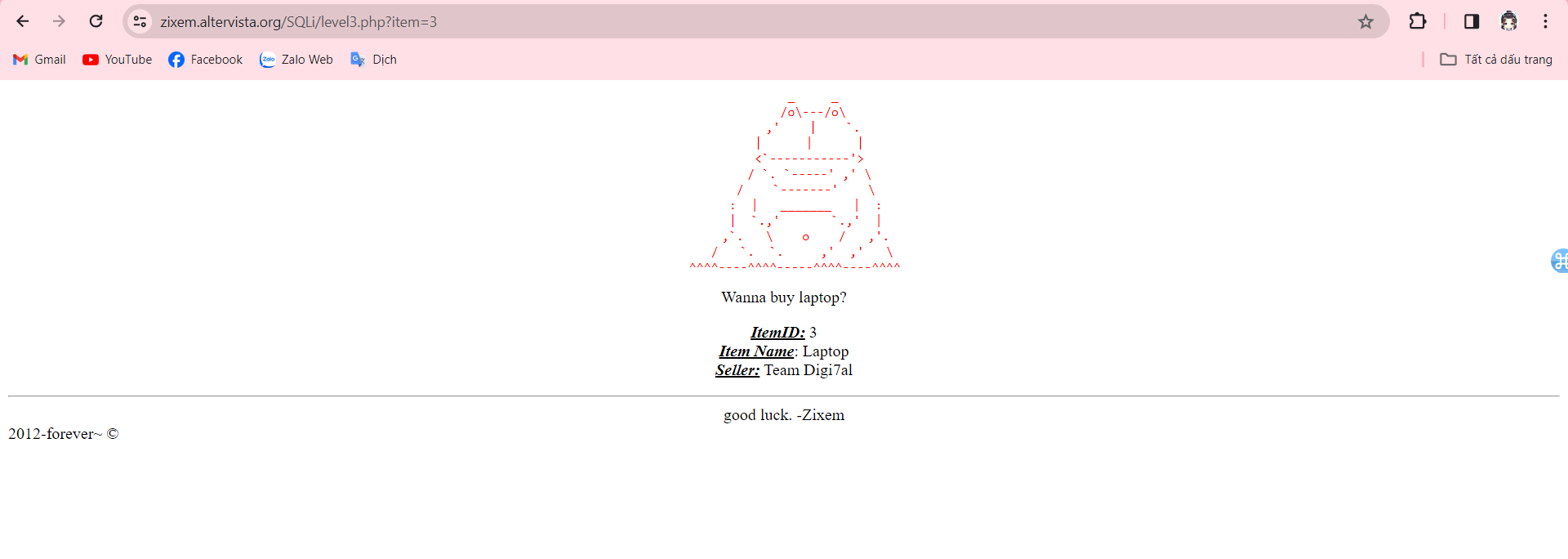
SELECT \* FROM profiles WHERE SHOWPROFILE=-4’ UNION ALL SELECT 1,user(),version(),4--+-

Thì ta có được kết quả sau:

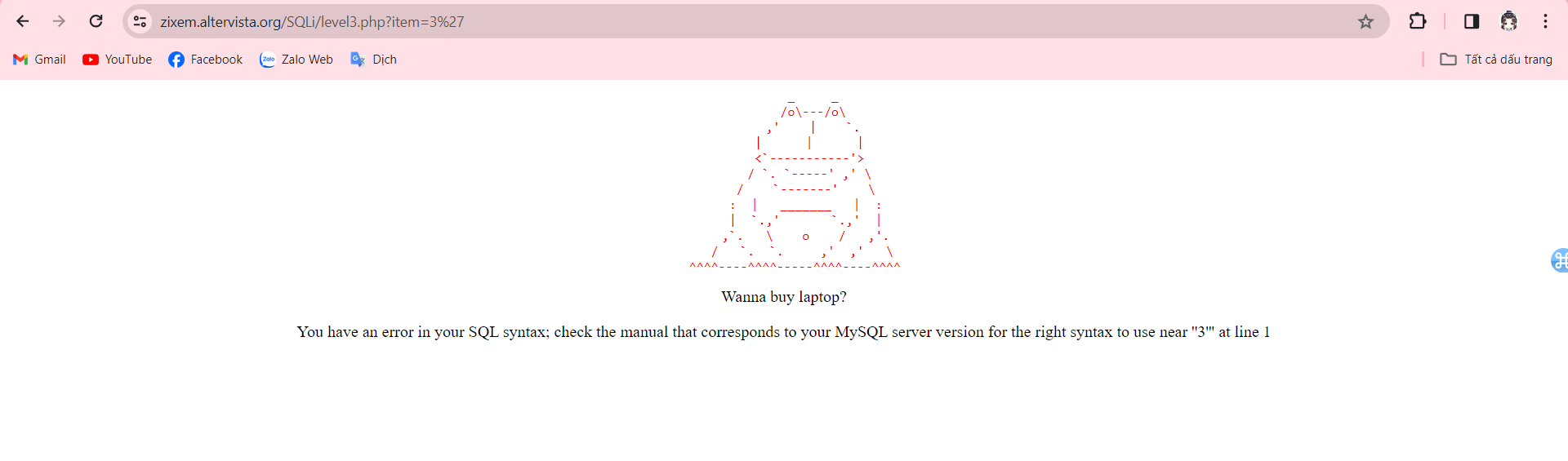
A silhouette of a person's head with a puzzle piece in the middle

Description automatically generated

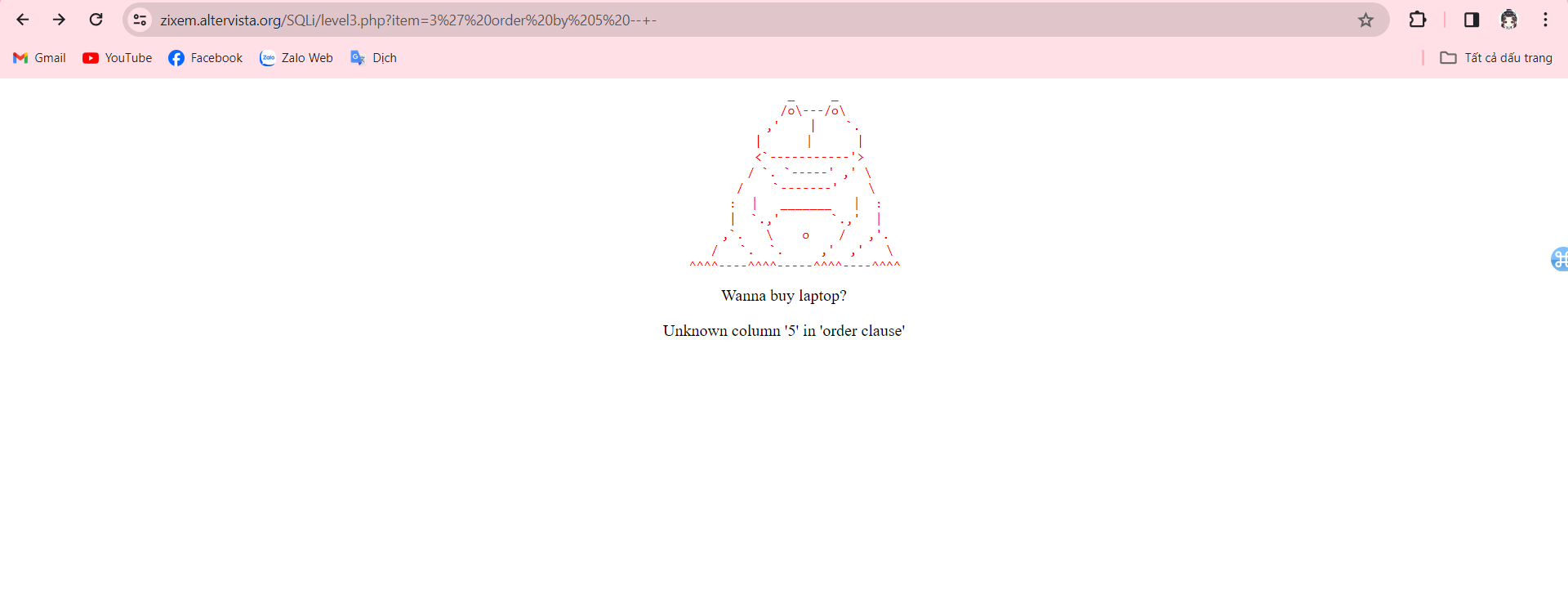
1. **Level 3 (Medium)**

Để trang in ra lỗi, chúng ta cần ngắt truy vấn sql và buộc ứng dụng đưa ra lỗi cho truy vấn không hợp lệ.

Ta có thêm kí tự ‘ vào cuối đường dẫn trang, thì trang sẽ hiện ra lỗi sau:

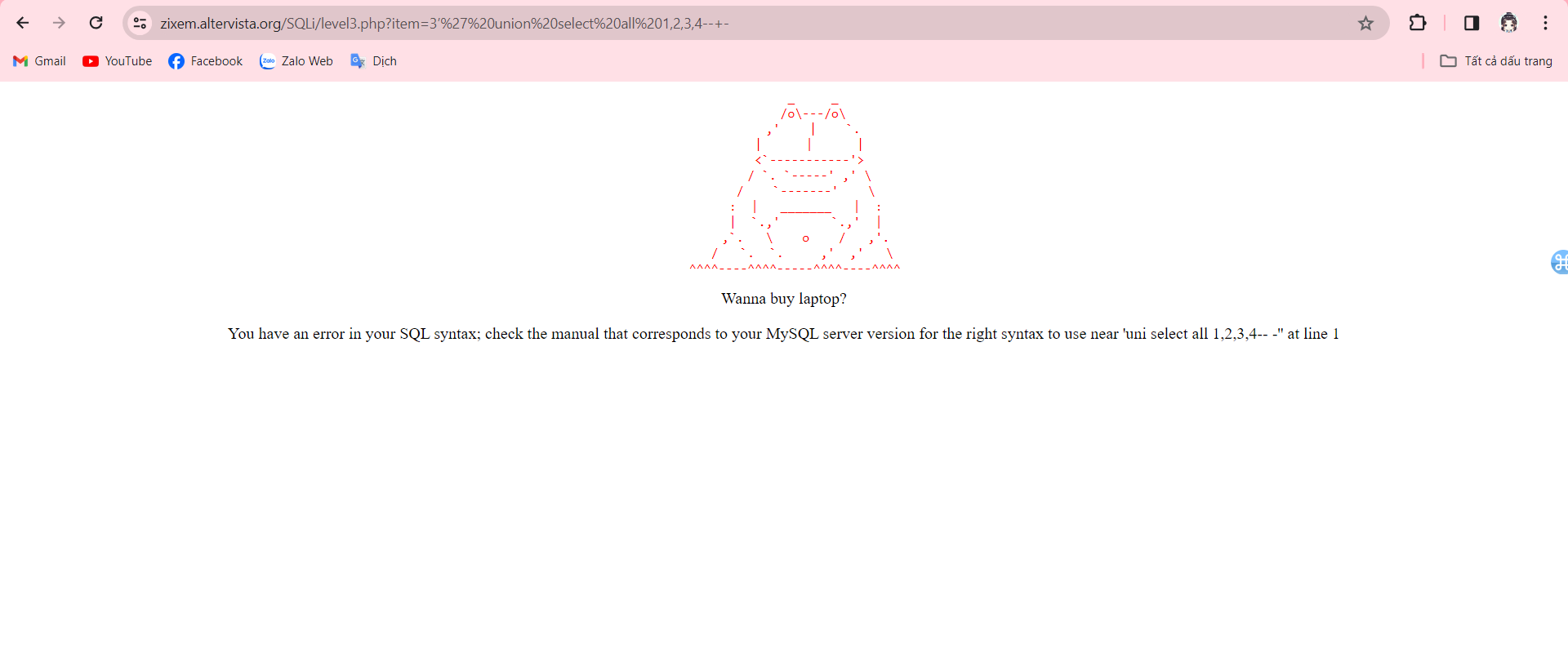
Để lấy số cột ta có thể sử dụng ORDER BY. Chúng ta sẽ sử dụng cho đến khi gặp lỗi như “unknown column ’n’ in order clause’.

Thì khi ta thêm ORDER BY 5 vào cuối đường dẫn thì trang sẽ hiện ra lỗi sau. Vậy cái bảng có 4 cột. Để câu truy vấn hợp lệ thì ta thêm dấu comment vào cuối câu

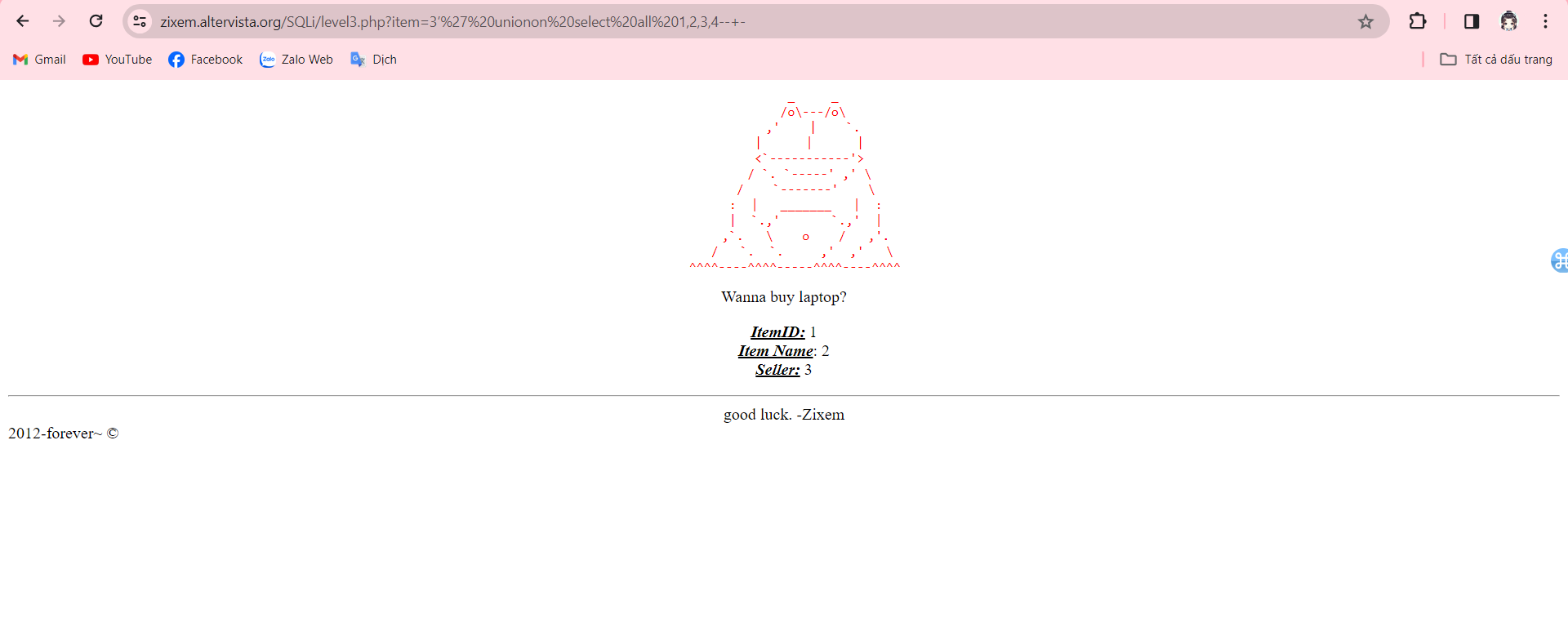


Ta thực hiện kiểm tra xem có thể khai thác được cột nào trong database:

[*https://zixem.altervista.org/SQLi/level3.php?item=3’*](https://zixem.altervista.org/SQLi/level3.php?item=3’) *union select all 1,2,3,4 --+-*



Ta nhận thấy chương trình báo lỗi 'uni select all 1,2,3,4-- -' nên ta thử thêm thành unionon



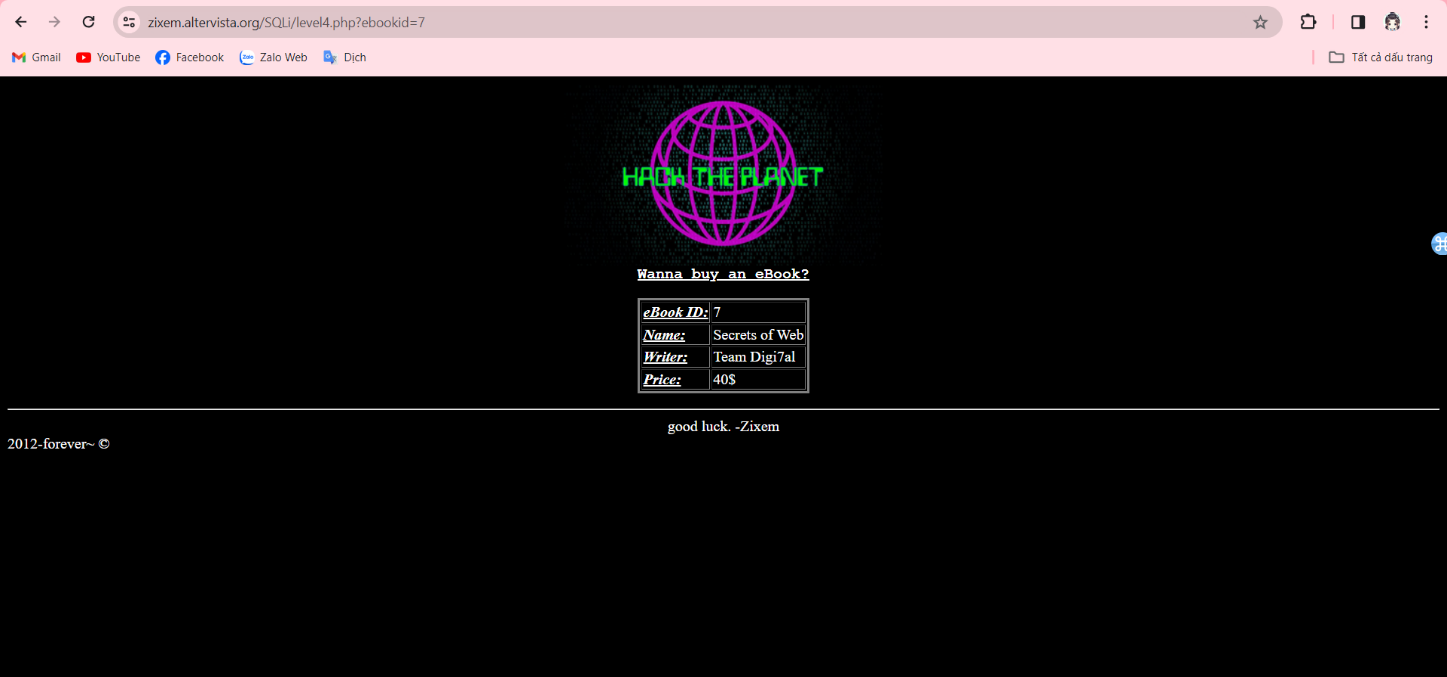
Ta nhận thấy có thể khai thác được 3 cột trong database -> Tiến hành khai thác

*https://zixem.altervista.org/SQLi/level3.php?item=*-3’ unionon select version(),user(),database(),4 --+-.

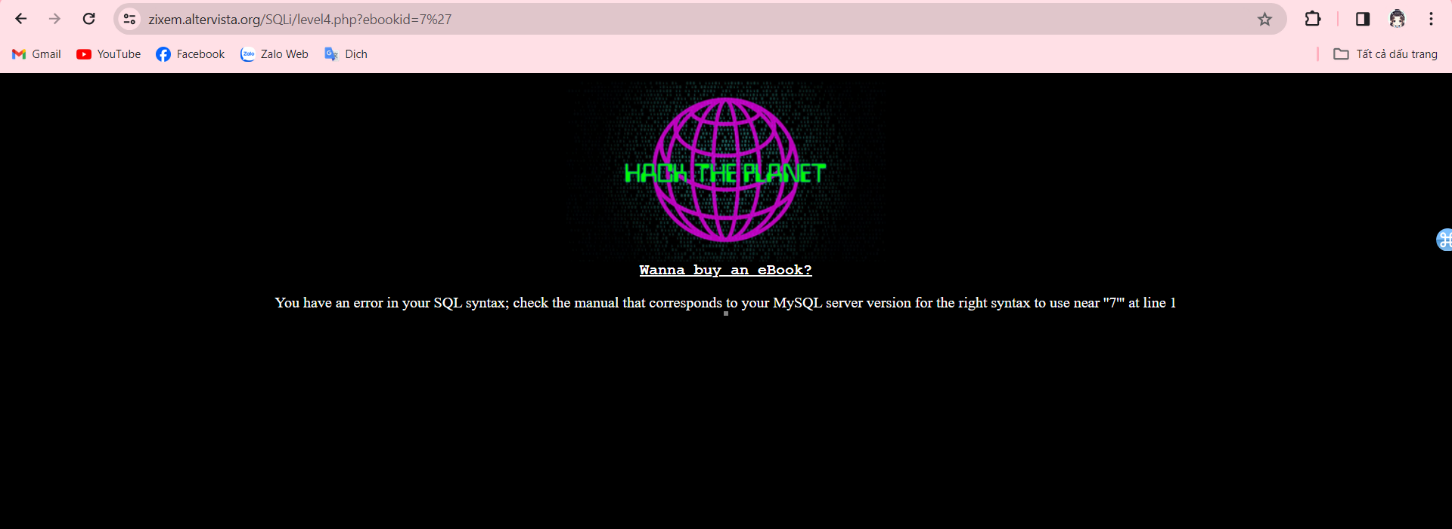
Kết quả:



1. **Level 4 (Normal)**

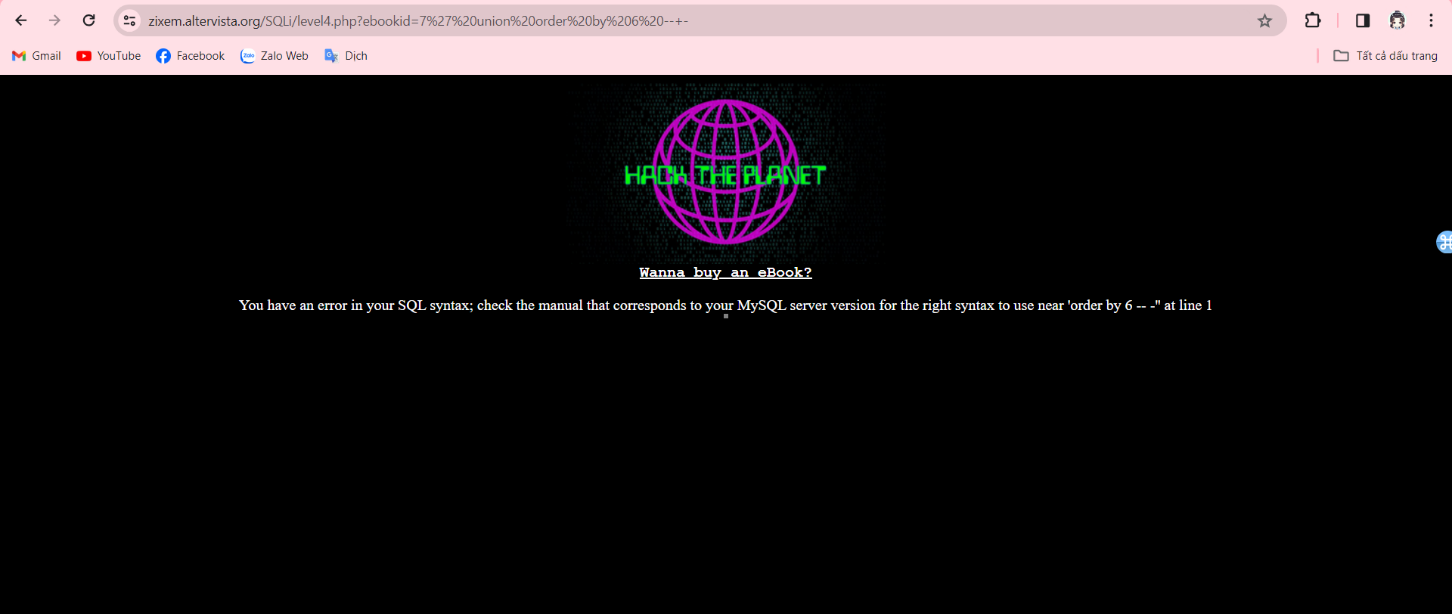


Ta bắt đầu bằng việc thêm vào dấu ‘ để kiểm tra có lỗi hay không

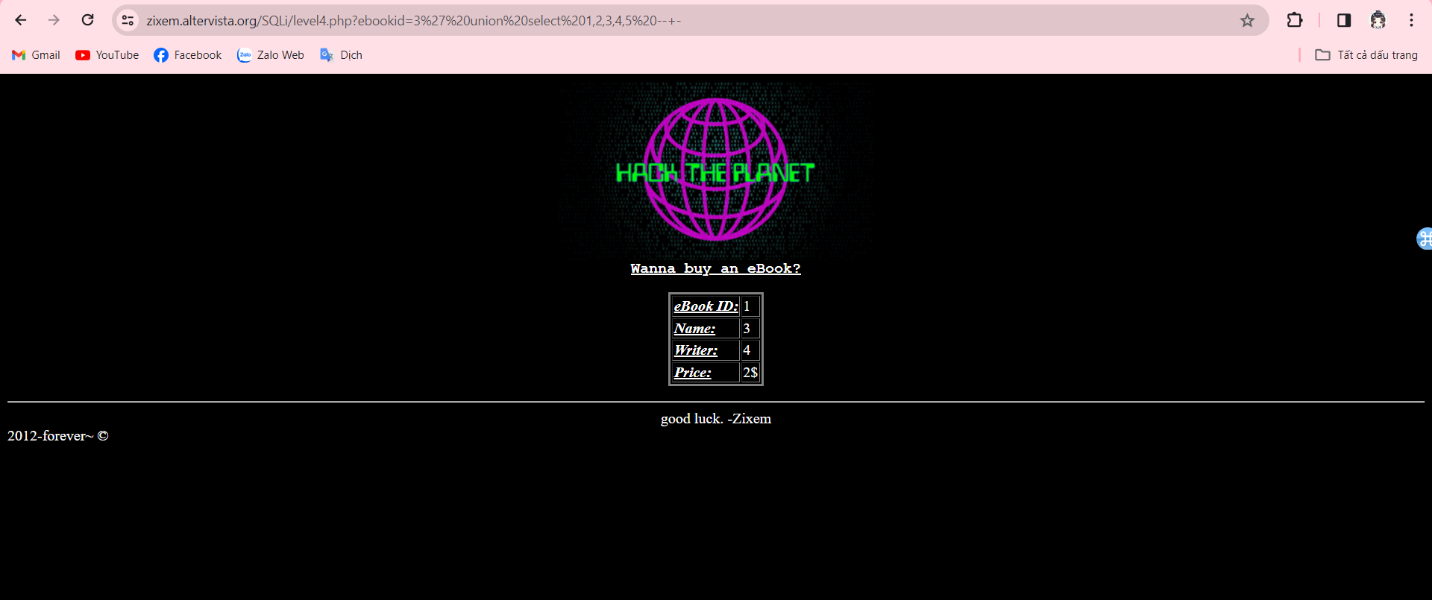


Thêm vào order by để kiểm tra số cột: [*https://zixem.altervista.org/SQLi/level4.php?ebookid=7*](https://zixem.altervista.org/SQLi/level4.php?ebookid=7)*' order by 1 --+-*

Tiến hành kiểm tra ta gặp lỗi ở cột thứ 6, vậy database có 5 cột



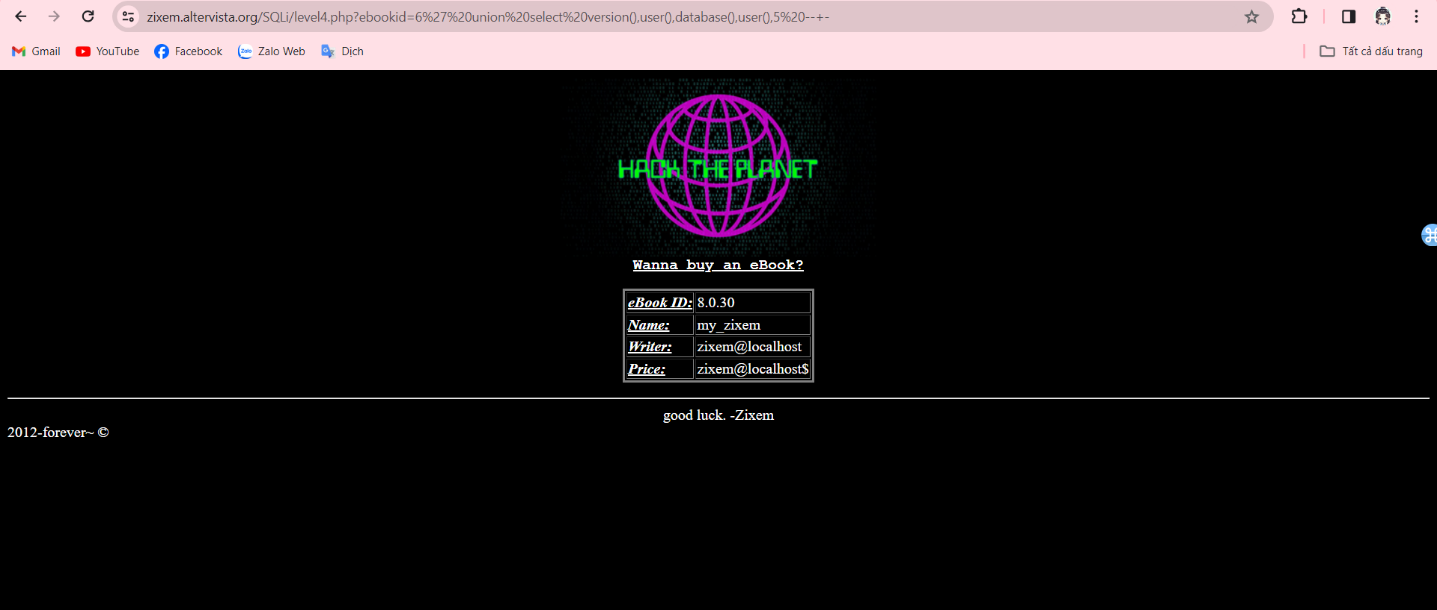
Kiểm tra xem ta có thể khai thác được bao nhiêu cột:



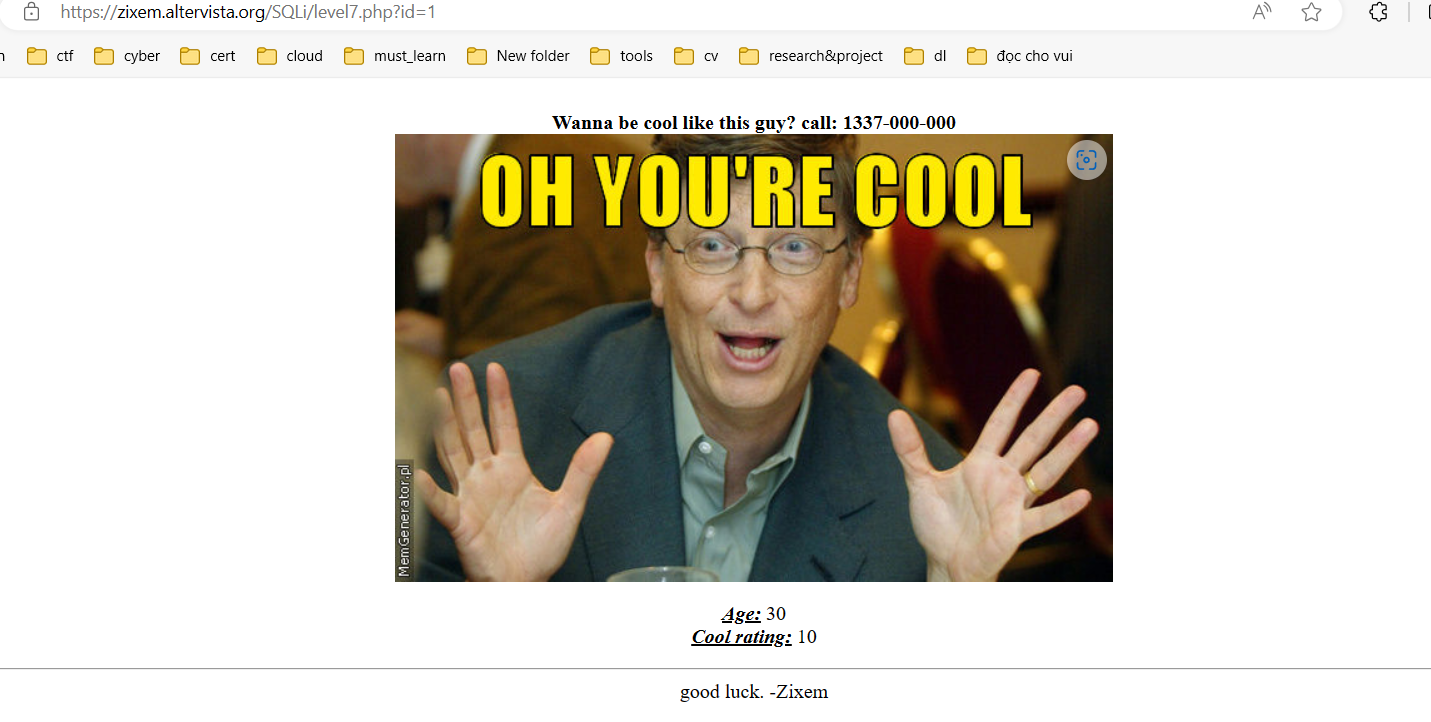
Ta có thể khai thác được 4 cột -> Tiến hành khai thác

*https://zixem.altervista.org/SQLi/level4.php?ebookid=-7' union select version(),user(),database(),user(),5 --+-*

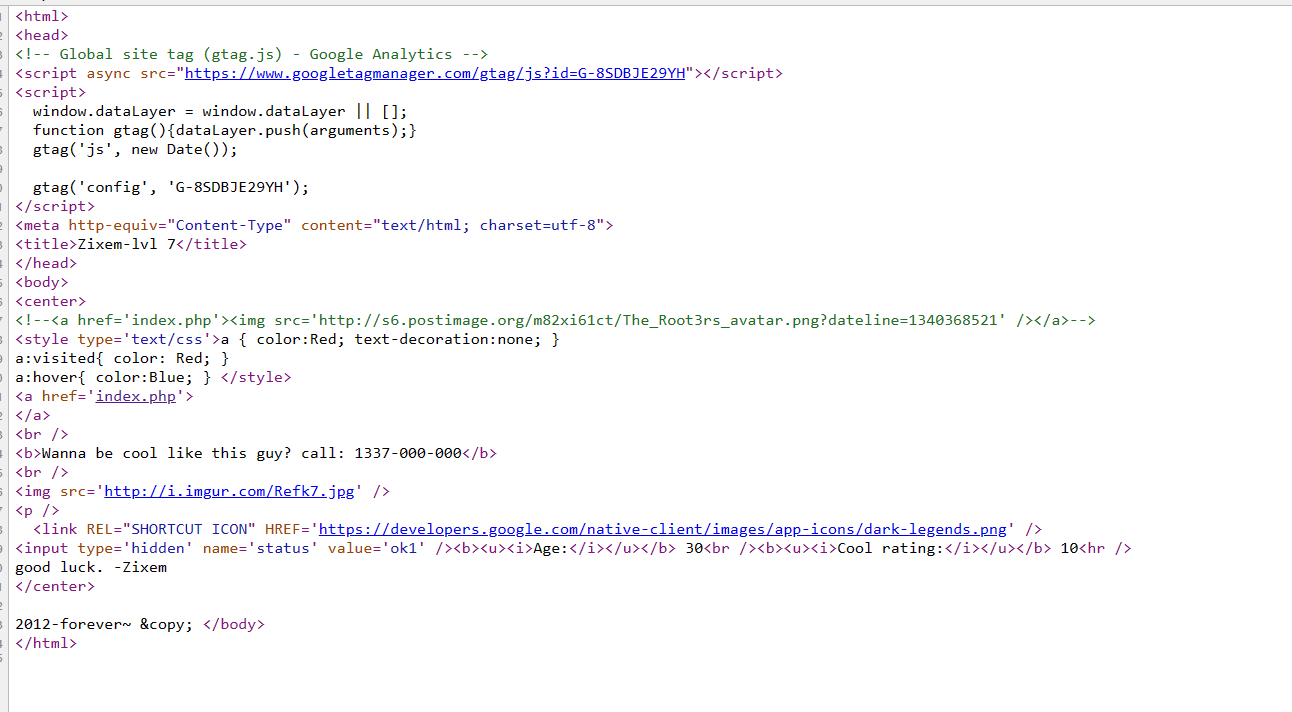
Kết quả:



1. **Level 7 (Medium)**



Đầu tiên, inspect code, kiểm tra source của web có những gì



Thử trước với một payload injection đơn giản để kiểm tra xem kết quả trả ra là gì

Payload: 1 AND 1=2 UNION SELECT 1,2,3--

Kết quả trả về trong trường hidden là



Với trường hidden trong source code với giá trị ok2. Bây giờ hãy thay đổi số 2 trong payload thành user() để xem người dùng:

Payload: 1 AND 1=2 UNION SELECT 1,user(),3--



Lúc này trong trường hidden đã có value là okzixem@localhost

Ta có thể thay đổi trường user() thành version và kiểm tra lại xem payload có thể inject và lấy được giá trị version không, và kết quả trả về là:

Payload: 1 AND 1=2 UNION SELECT 1,version(),3--



Version: ok8.0.30

1. **Level 8 (Hard)**

Ảnh có chứa văn bản, ảnh chụp màn hình, phim hoạt hình, Hệ điều hành

Description automatically generated

Đầu tiên ta thử bằng cách thêm and 1=1--

Ảnh có chứa văn bản, phim hoạt hình, hình mẫu, ảnh chụp màn hình

Description automatically generated

Kết quả trả về từ màn hình là “hacking attempt” cho thấy đã có filter hoặc cái gì đó được bật lên để ngăn chặn SQL Injection.

Sau một thời gian tìm hiểu, thì chúng ta nhận ra trang web sẽ hiển thị thông báo trên khi phát hiện ra khoảng trắng trong URL.

Dù đã thử đổi khoảng trắng thành các ký tự khác như:

* Dấu cộng (+): Đây là một ký tự đơn giản được sử dụng trong các chuỗi văn bản hoặc URL.
* Dấu cách được mã hóa URL (%20): Đây là ký tự dấu cách được mã hóa trong các URL để đảm bảo tính nhất quán và hỗ trợ truy cập qua mạng.
* Null byte (%00): Đây là ký tự null, không có hiển thị và thường được sử dụng để kết thúc một chuỗi ký tự.
* Dấu xuống dòng (%0a): Đây là ký tự xuống dòng, được sử dụng để di chuyển con trỏ xuống dòng tiếp theo trong văn bản.
* Dấu tab (%09): Đây là ký tự tab, được sử dụng để tạo khoảng cách giữa các phần trong văn bản hoặc dữ liệu.
* Dấu xuống dòng màn hình (%0d): Đây là ký tự xuống dòng màn hình, thường được sử dụng cùng với ký tự xuống dòng để tạo một xuống dòng hoàn chỉnh trong văn bản.

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, phim hoạt hình

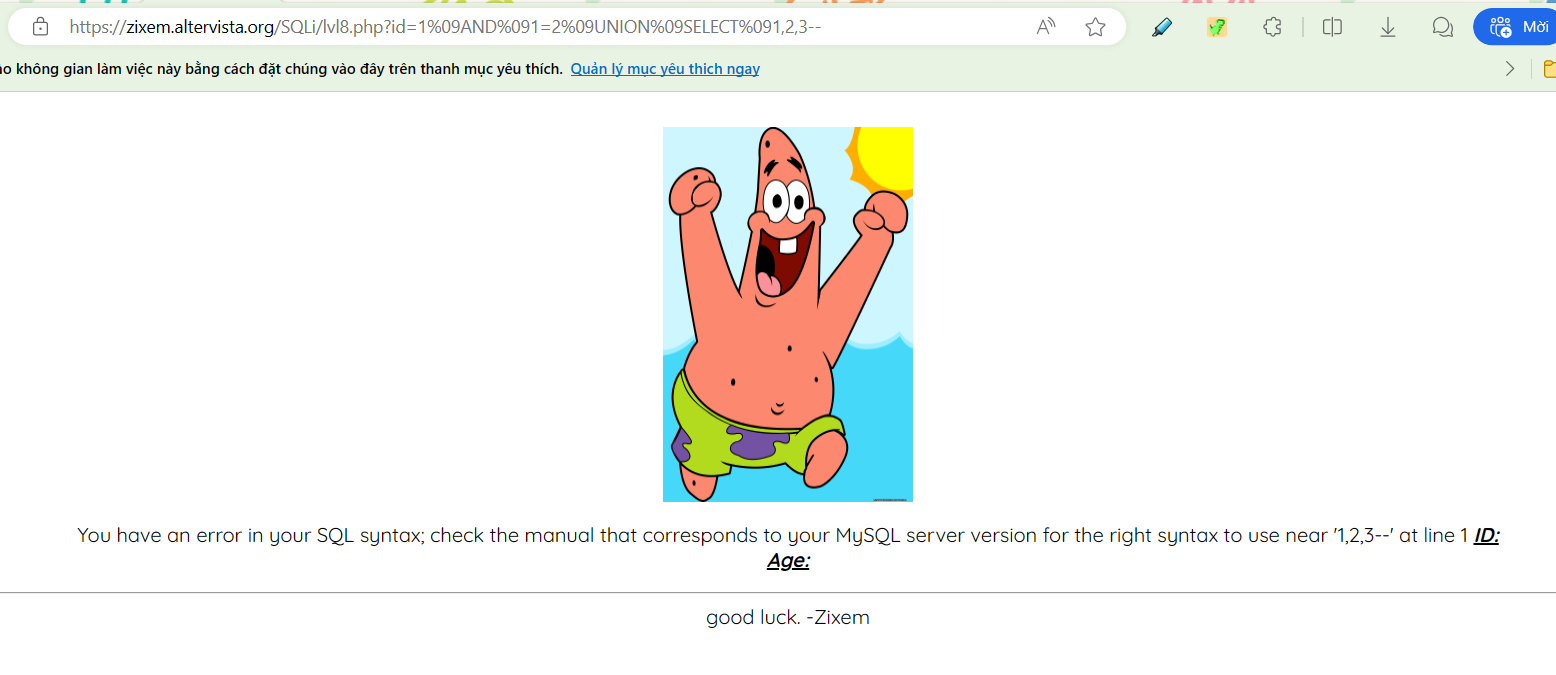
Description automatically generated

Ảnh có chứa văn bản, ảnh chụp màn hình, phim hoạt hình, hình mẫu

Description automatically generated

Sau khi thử ta nhận thấy chỉ có %09 không xuất hiện lỗi.

Khi thử dùng union select thì nhận được kết quả trả về như sau:



Có vẻ như SELECT đã bị bỏ qua, trong một challenge ở trên thì ON của UNION đã bị bỏ qua nên chúng ta phải viết thành UNIONON. Áp dụng điều này vào challenge này chúng ta sẽ viết thành SELSELECTECT như vậy cho dù SELECT bị bỏ qua thì những chữ còn lại vẫn có thể ghép thành SELECT:



Kết quả đã được trả về và không bị lỗi syntax. Bây giờ chúng ta sẽ thử để kết quả trả về là thông tin của user và version

Ảnh có chứa văn bản, ảnh chụp màn hình, hình mẫu, phim hoạt hình

Description automatically generated

1. **Level 9 (Medium)**

**A screenshot of a computer

Description automatically generated**

Khi mới vào trang ta được giao ngay nhiệm vụ là hiển thị tập tin theo đường dẫn: /etc/passwd

Thử thêm ‘ vào cuối đường dẫn. Ta sẽ thấy trang hiện ra lỗi.

A screenshot of a computer

Description automatically generated

Để lấy số cột ta có thể sử dụng ORDER BY. Chúng ta sẽ sử dụng cho đến khi gặp lỗi như “unknown column ’n’ in order clause’.

Thì khi ta thêm ORDER BY vào cuối đường dẫn thì trang sẽ hiện ra lỗi sau. Vậy cái bảng có 2 cột.

A screenshot of a computer

Description automatically generated

Khi truy vấn đầu tiên được đặt thành null và truy vấn thứ hai được chuyển với một số dữ liệu đầu vào do người dùng tạo ra. Ở đây chúng ta đã đặt phần đầu tiên của truy vấn là null và phần thứ hai là hợp lệ. Thì trình thông dịch SQL chỉ đưa ra kết quả của phần thứ hai.

SELECT \* FROM table WHERE id=-1’ UNION ALL SELECT 1,2--+-

A screenshot of a computer

Description automatically generated

Ta có thể khai thác thông tin từ cột 1 của bảng.

Bây giờ tất cả những gì chúng ta cần là liệt kê tệp ‘/etc/passwd’. Thêm ‘../etc/passwd/’ thay vì 1 vào URL để truy cập file passwd, thì ta sẽ hoàn thành challenge.

SELECT \* FROM table WHERE id=-1’ UNION ALL SELECT ‘../etc/passwd/’,2--+-

A close up of a text

Description automatically generated

