

BÁO CÁO BÀI TẬP

Môn học: Bảo mật web và ứng dụng

Tên chủ đề: SQLi

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.O22.ATCL

STT	Họ và tên	MSSV	Email
1	Nguyễn Trần Đức Anh	20520392	20520392@gm.uit.edu.vn

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

BÁO CÁO CHI TIẾT

Rules!

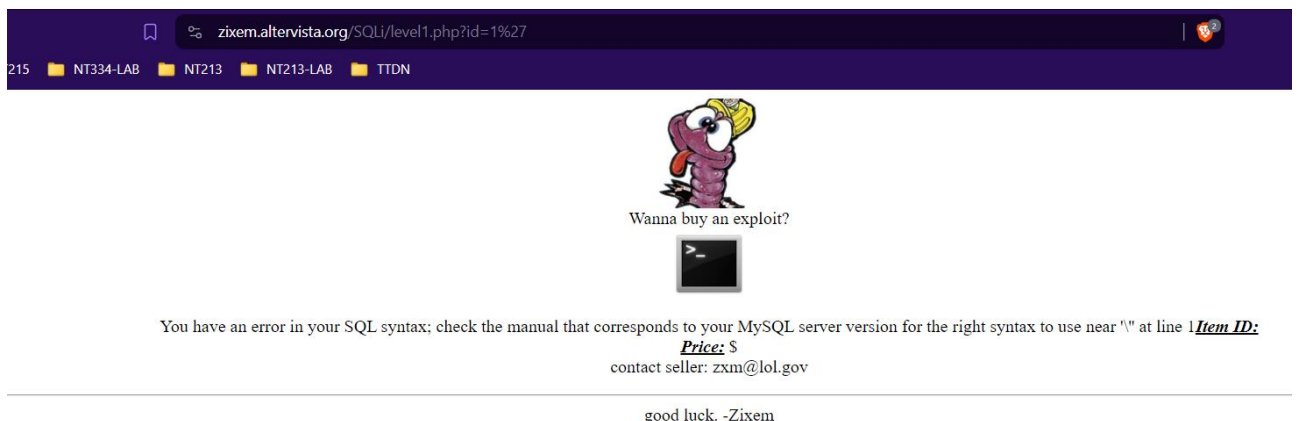
Use **only** UNION BASED!

Your mission is to select **only** the version & user and to take screenshot as proof.
Have Fun (:

[\[SQLi challenges\]](#)

A. Level 1 (Super Easy)

Ở lv1, ta có thể thấy truy vấn id=1 tại url, có thể có lỗi SQLi ở đây. Thêm dấu ' vào sau số 1 thì thấy xuất hiện lỗi.



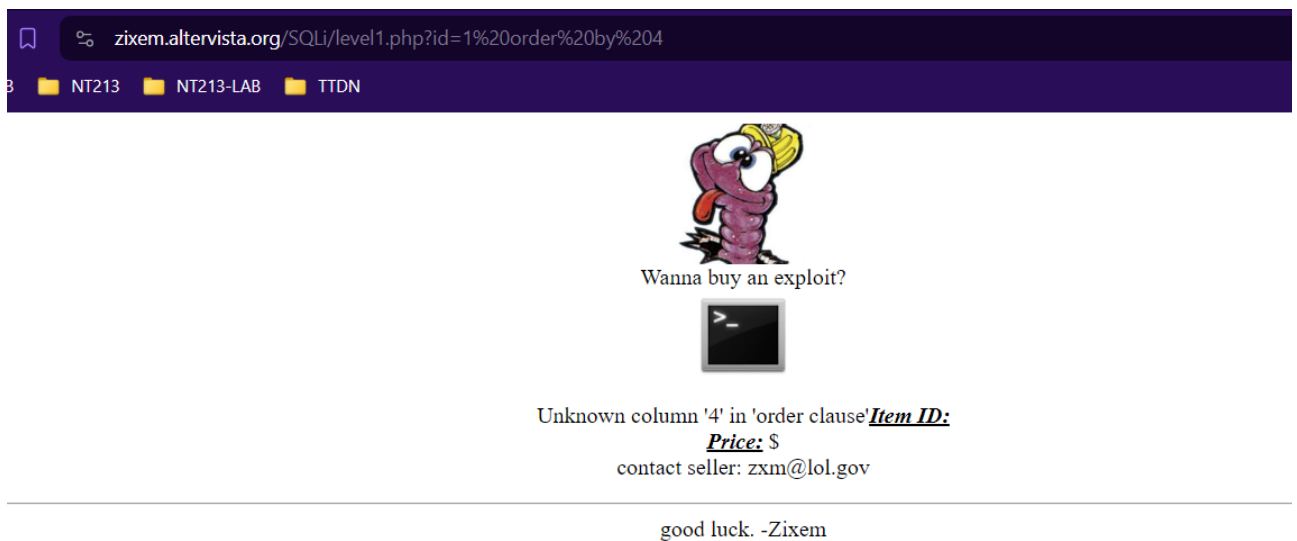
215 NT334-LAB NT213 NT213-LAB TTDN

Wanna buy an exploit?

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\" at line 1Item ID: Price: \$ contact seller: zxm@lol.gov

good luck. -Zixem

Đã có lỗi rồi thì ta đếm số cột của bảng thôi. Dùng order by đến khi xảy ra lỗi:

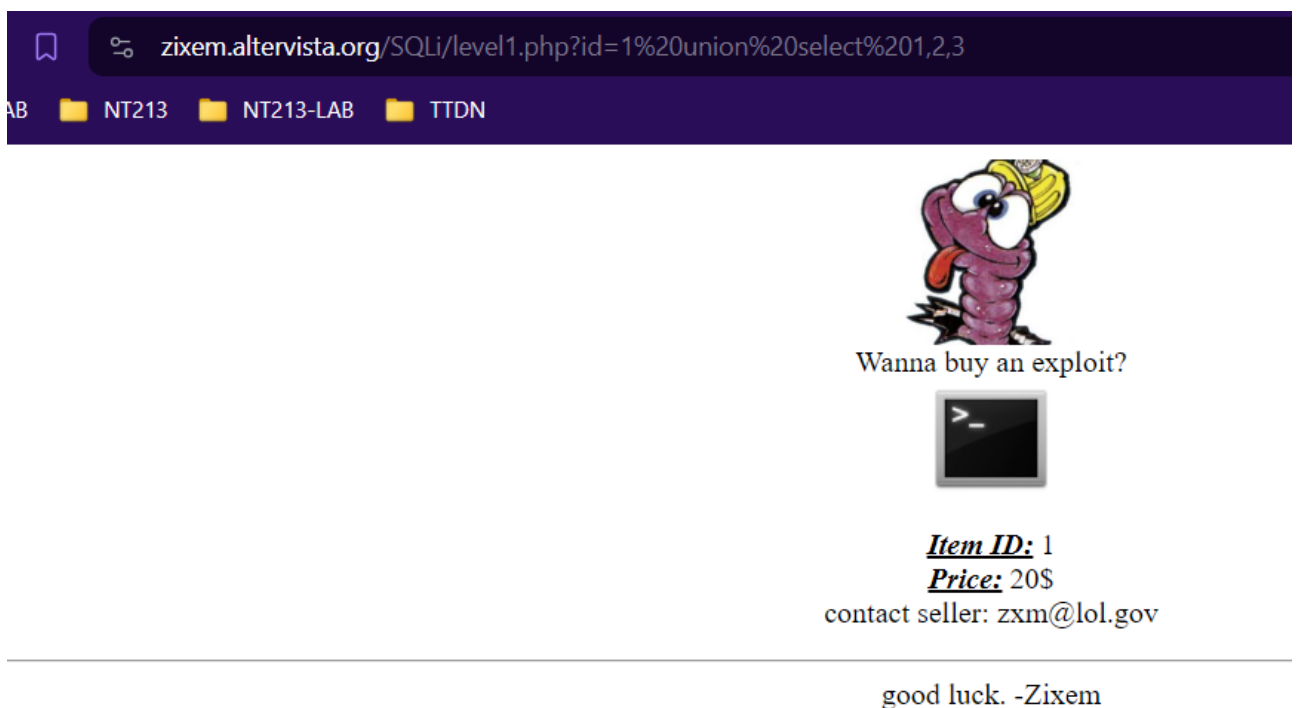


Wanna buy an exploit?

Unknown column '4' in 'order clause' **Item ID:**
Price: \$
 contact seller: zxm@lol.gov

good luck. -Zixem

Ở đây order by 4 lỗi thì có thể số cột bé hơn 4 (cụ thể là 3). Vậy thử union select xem có thể khai thác thông tin ở cột nào. Dùng "union select 1,2,3 -" nhưng không có gì xảy ra.

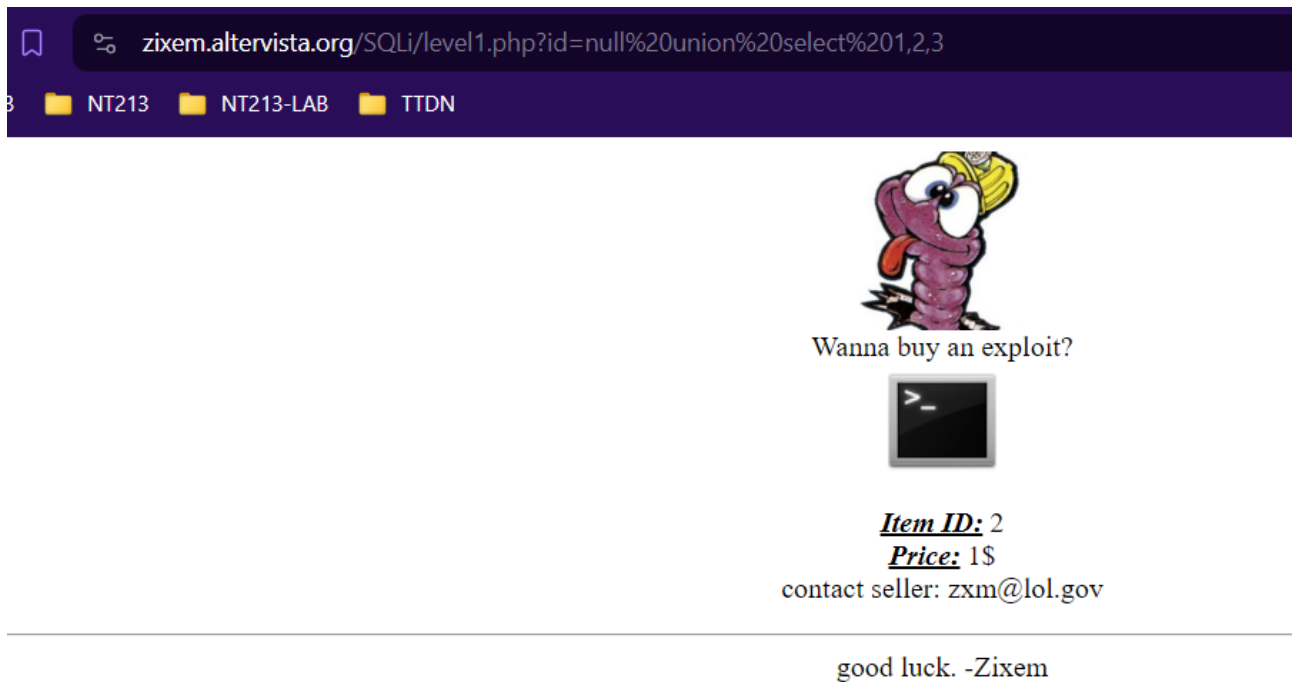


Wanna buy an exploit?

Item ID: 1
Price: 20\$
 contact seller: zxm@lol.gov

good luck. -Zixem

Tham khảo trên internet thì thấy ngta chỉ thay id = null thì có thể xảy ra lỗi

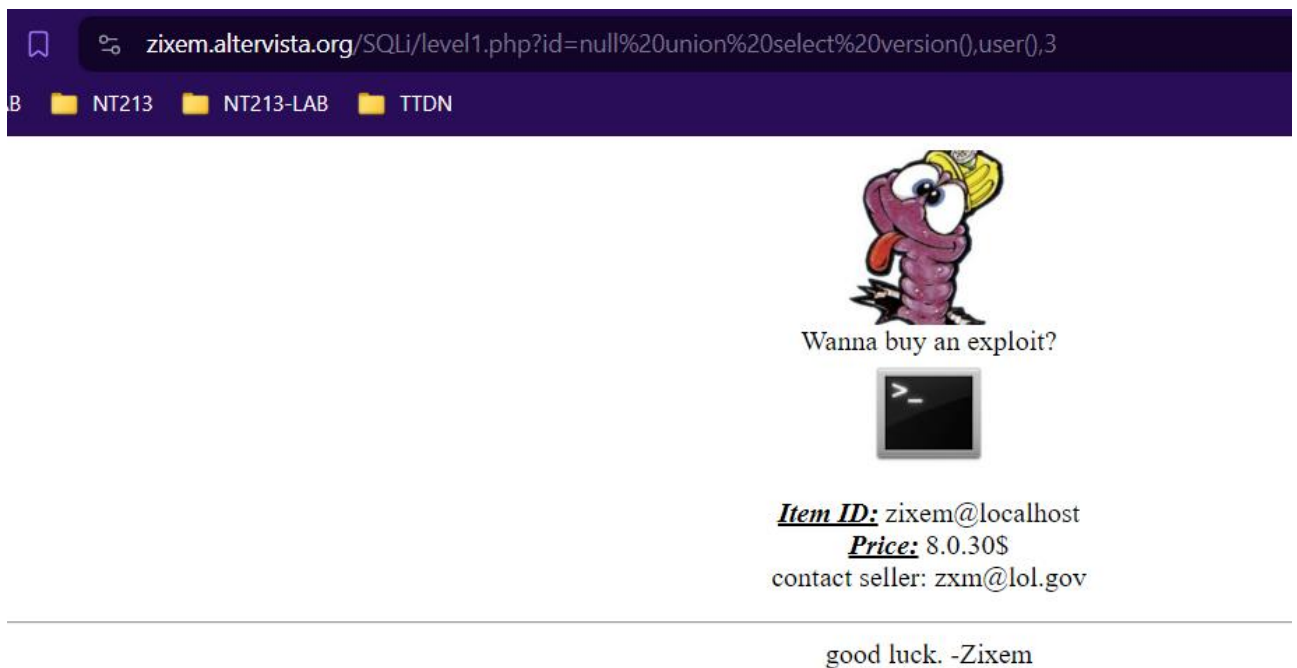


Wanna buy an exploit?

Item ID: 2
Price: 1\$
contact seller: zxm@lol.gov

good luck. -Zixem

Ở đây thấy số 1 và 2 ở Price và Item ID. Vậy có thể khai thác ở cột 1 và 2. Đề bài yêu cầu tìm version và user. Thử select 2 thông tin đó:



Wanna buy an exploit?

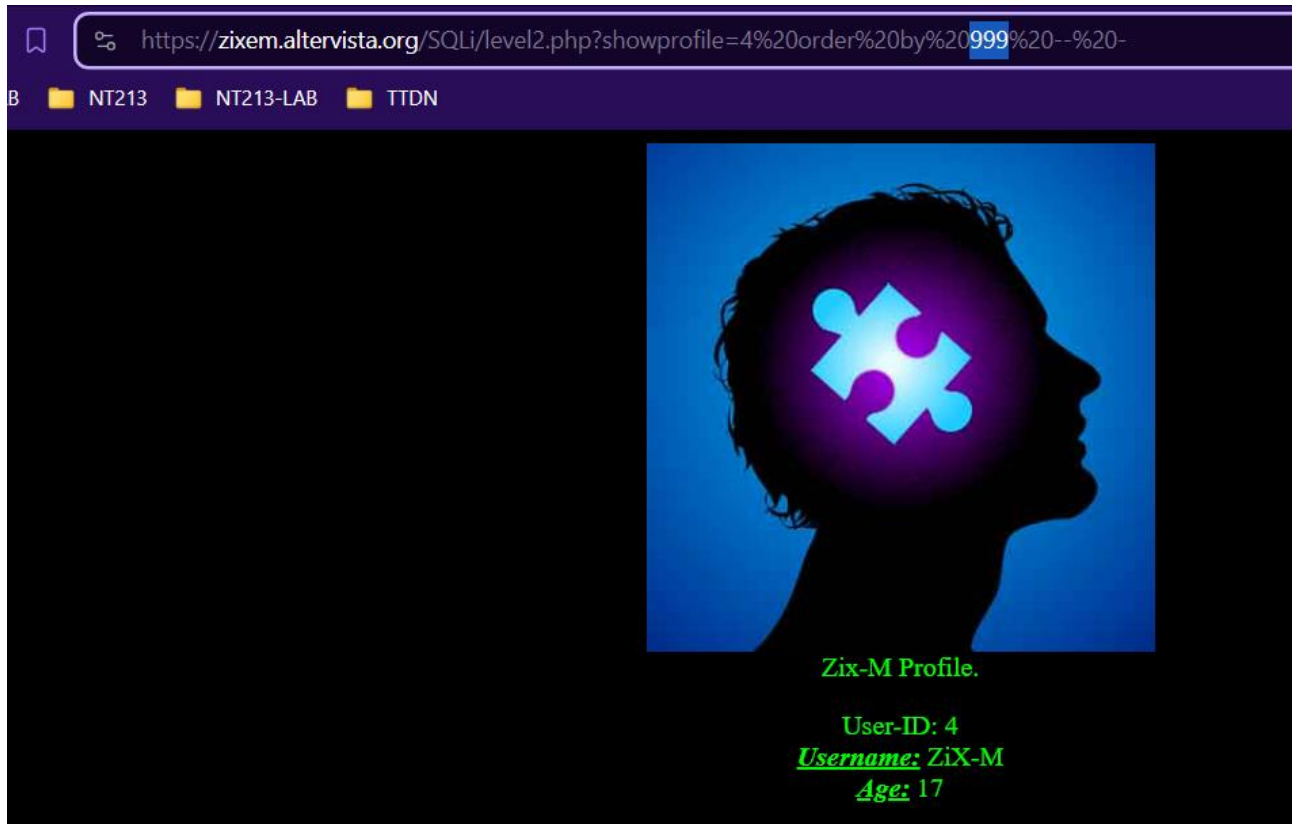
Item ID: zixem@localhost
Price: 8.0.30\$
contact seller: zxm@lol.gov

good luck. -Zixem

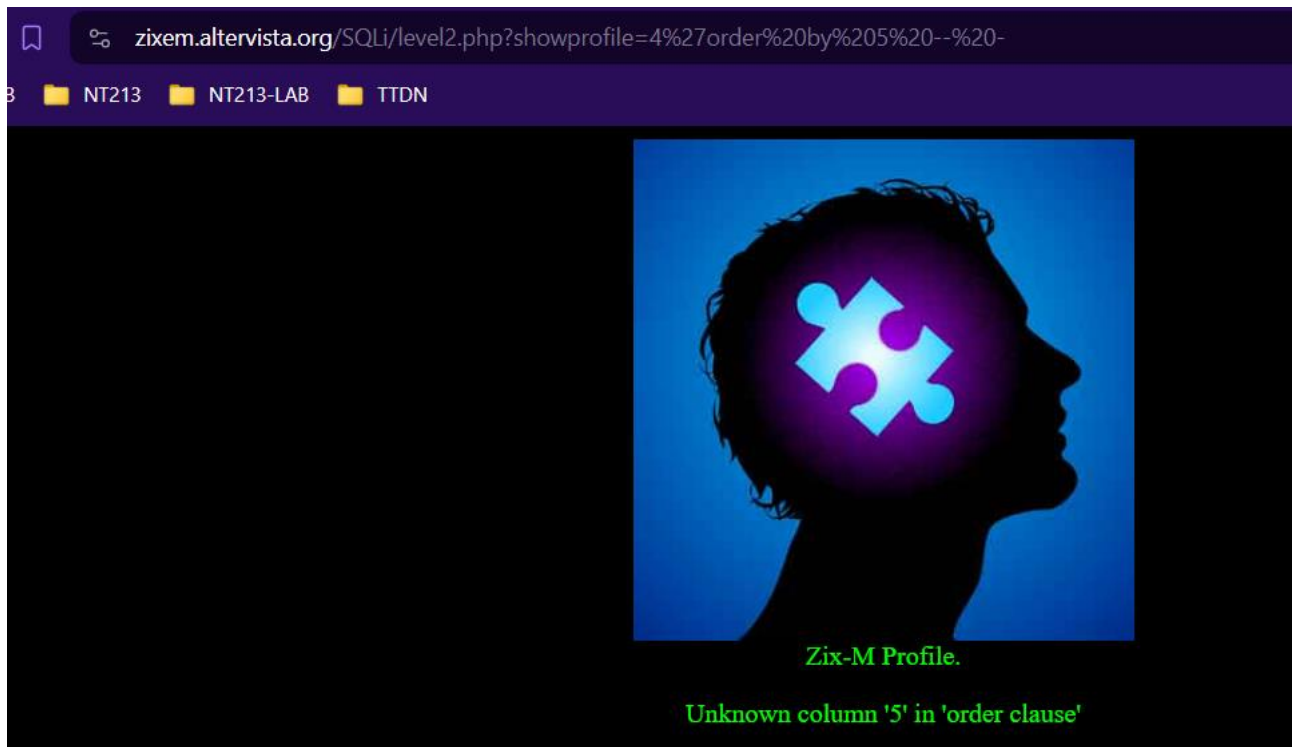
⇒ Thấy được 2 thông tin cần tìm “zixem@localhost” và “8.0.30”

B. Level 2 (Easy)

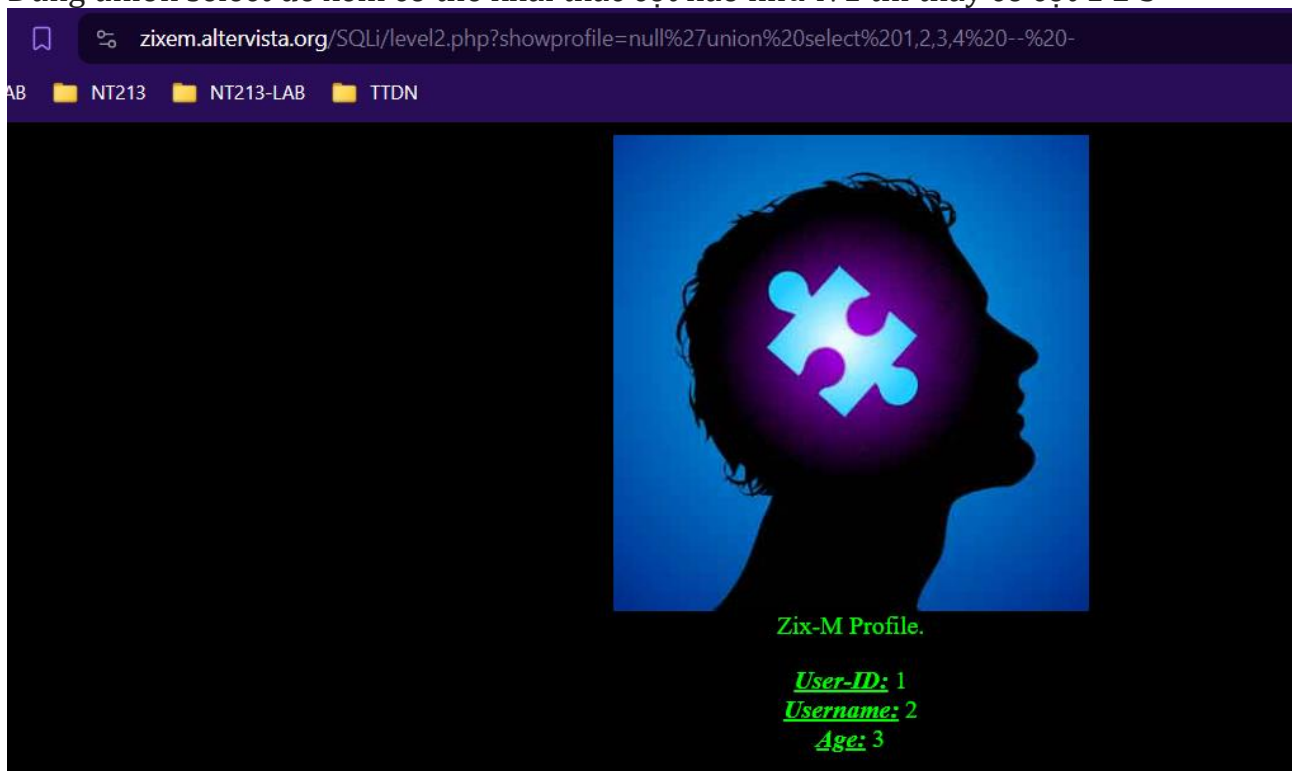
Thực hiện kiểm tra lỗi và order by như lv1 tuy nhiên không tìm ra được số cột



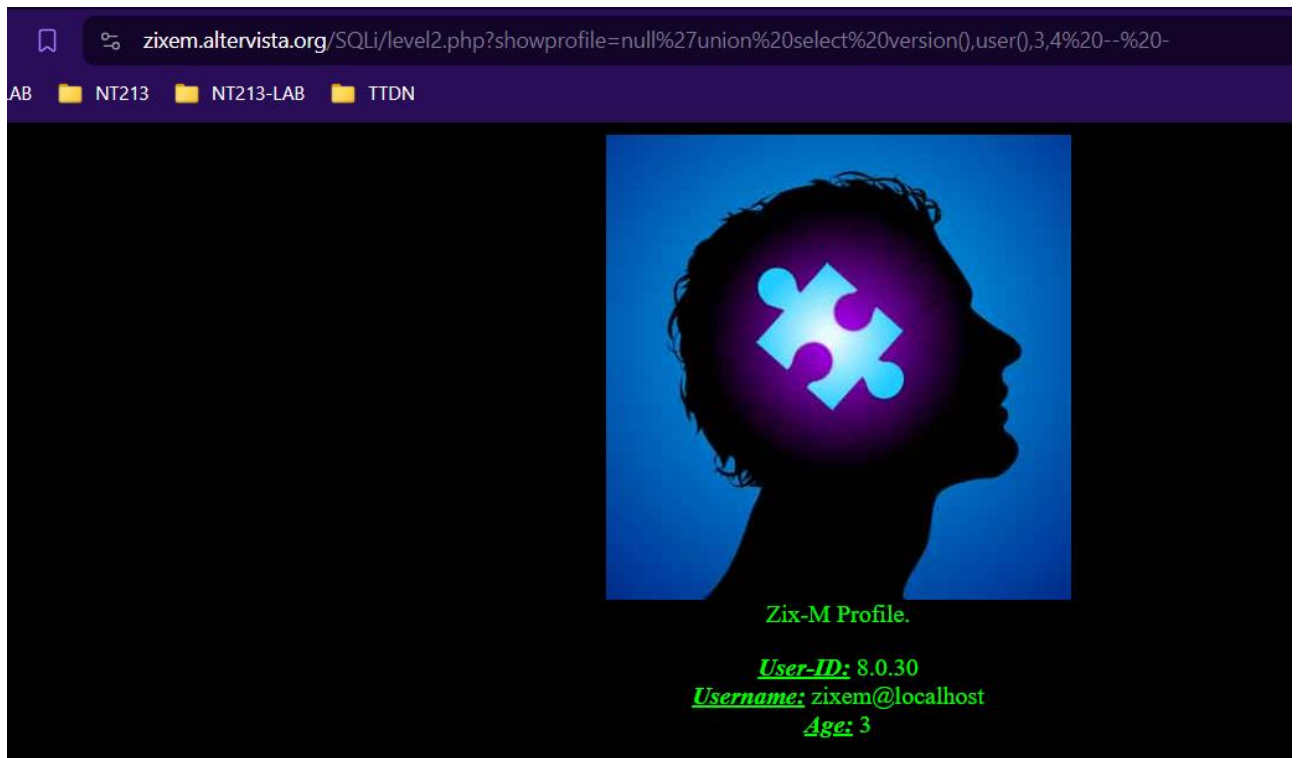
Có thể đầu vào của truy vấn này là chuỗi gì đó nên cần dấu ' để kết thúc chuỗi. Thêm dấu ' sao số 4. Và tìm ra được lỗi tại 5 cột => có 4 cột. "--" ở cuối để chú thích và đảm bảo chú thích không có gì hoặc không vấn vế sau đó



Dùng union select để xem có thể khai thác cột nào như lv1 thì thấy có cột 1 2 3



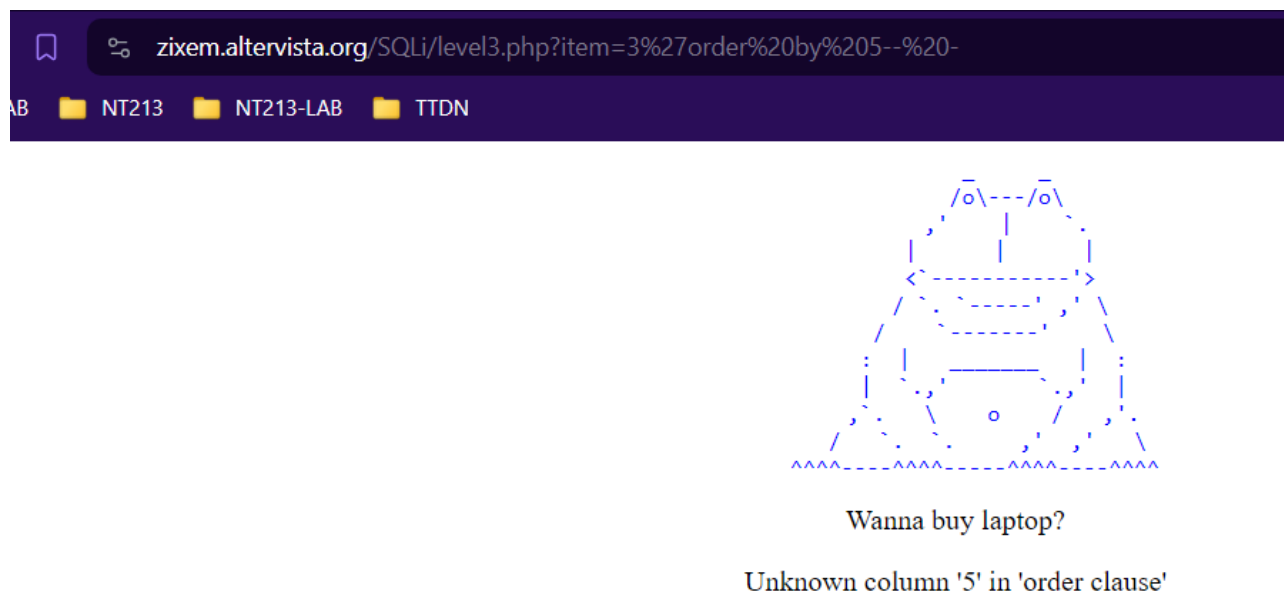
Thử tìm ở cột 1 2 thì được luôn



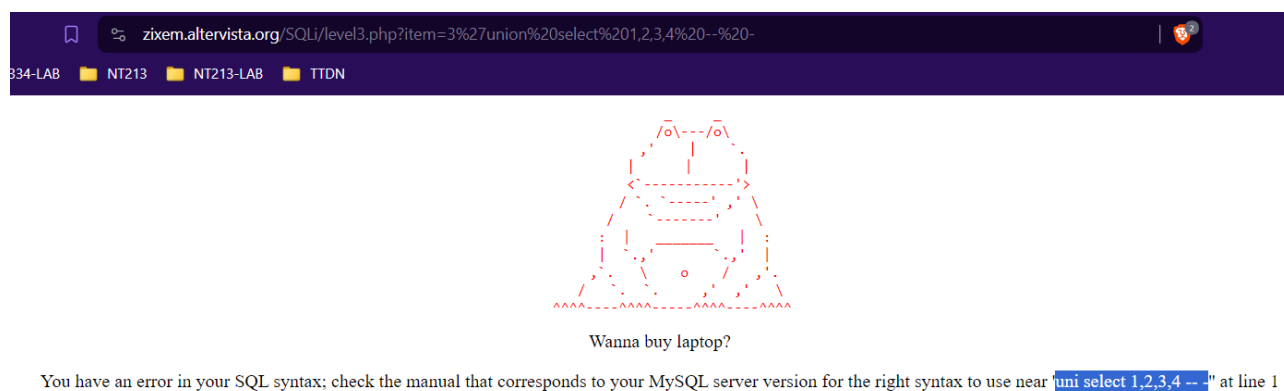
⇒ Thấy được 2 thông tin cần tìm “zixem@localhost” và “8.0.30”

C. Level 3 (Medium)

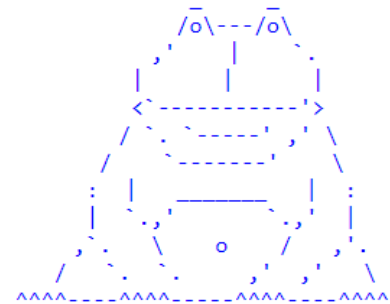
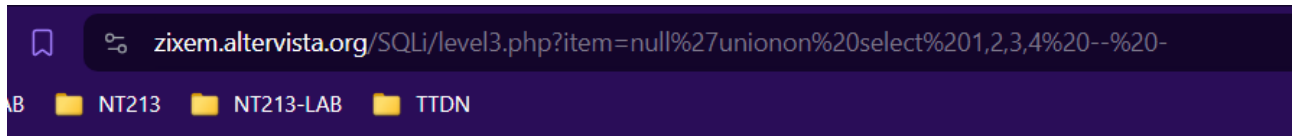
Kiểm tra tương tự lv2 thì thấy số cột là 4



Dùng union select thử xem khai thác được cột nào



Tuy nhiên chỗ này bị lỗi, không xem được như bài trước. Xem thông báo thì thấy chuỗi ta nhập bị mất “on” chỗ “union”. Vậy thêm thử “on” sau “union”



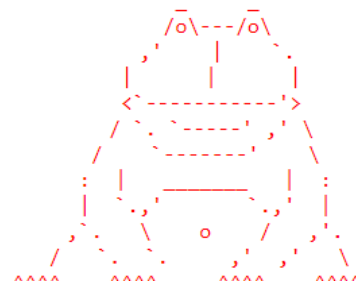
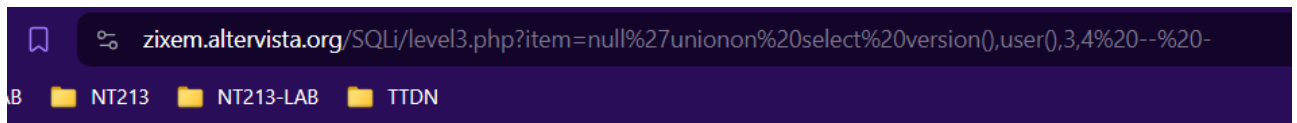
Wanna buy laptop?

ItemID: 1

Item Name: 2

Seller: 3

Được rồi, giờ thì kiểm version với user thôi



Wanna buy laptop?

ItemID: 8.0.30

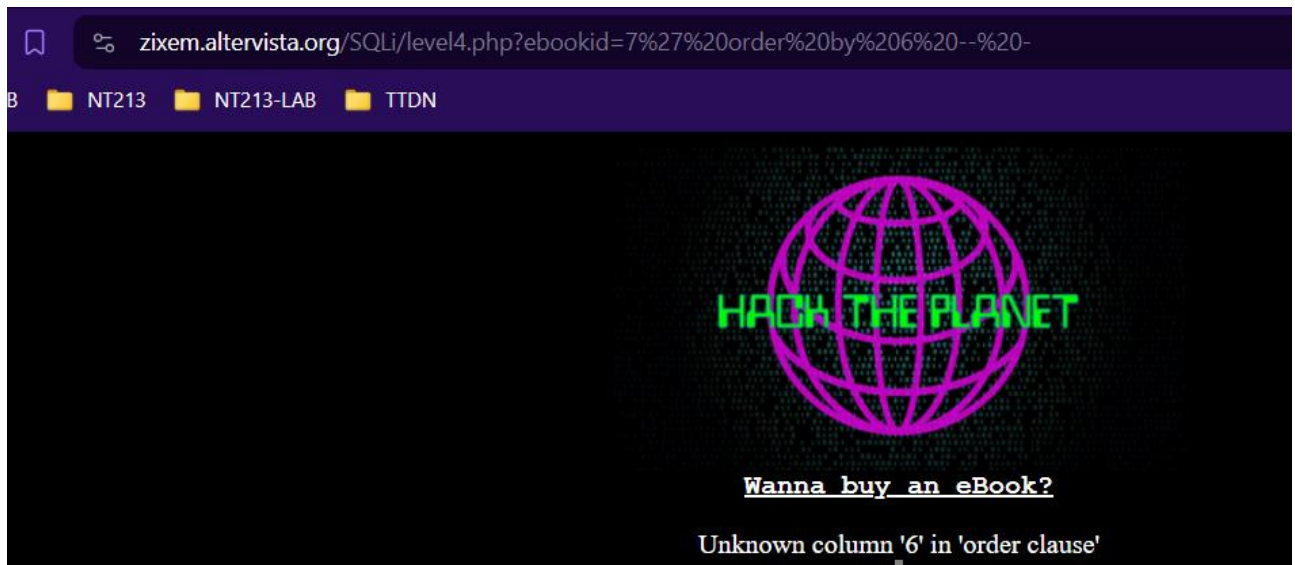
Item Name: zixem@localhost

Seller: 3

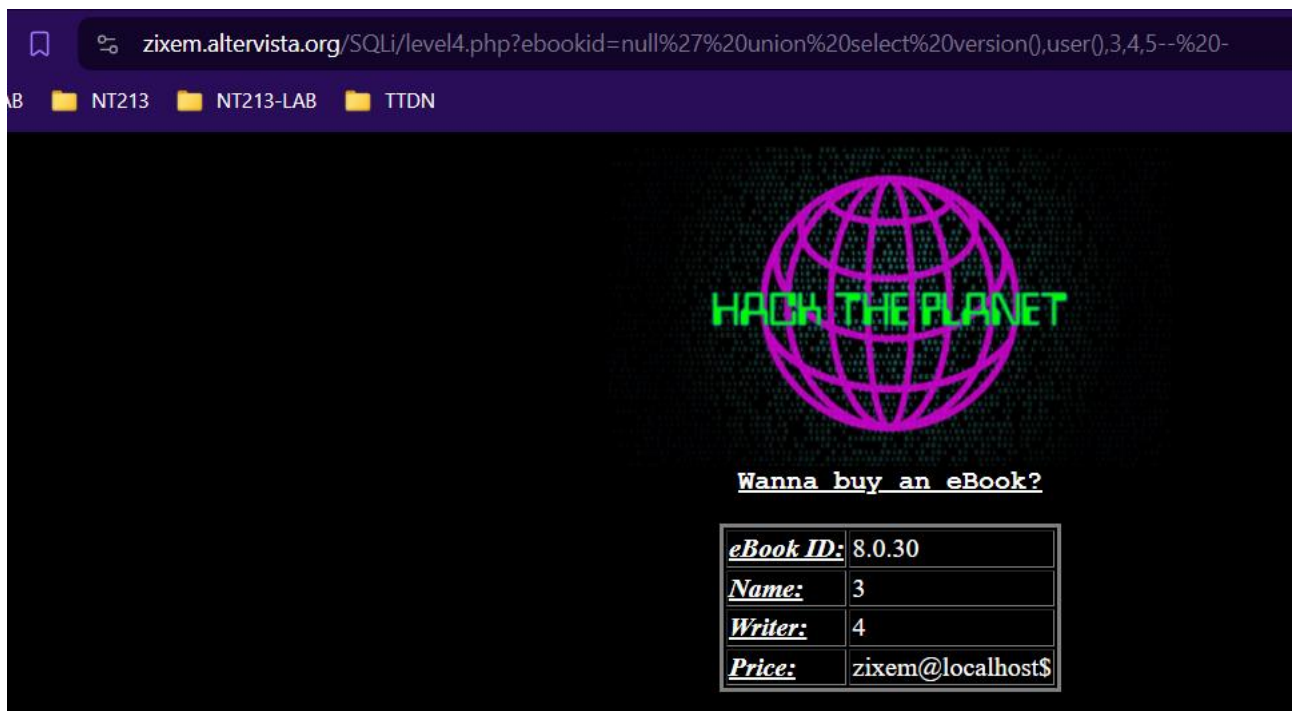
⇒ Thấy được 2 thông tin cần tìm “zixem@localhost” và “8.0.30”

D. Level 4 (Normal)

Làm tương tự lv trên thì thấy số cột là 5



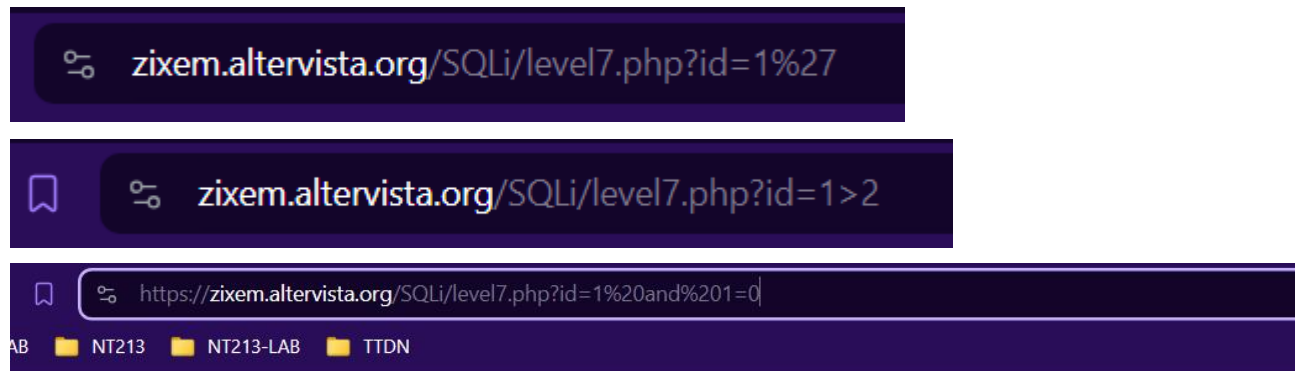
Tìm kiếm như bình thường luôn



⇒ Thấy được 2 thông tin cần tìm “zixem@localhost” và “8.0.30”

E. Level 7 (Medium)

Gòi gòi xog gòi, kiểm tra từ từ luôn không thấy lỗi



Age: 30
Cool rating: 10

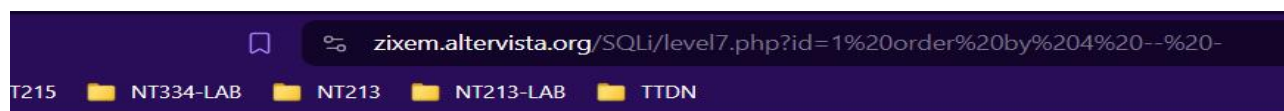
Level developed by Zixem

Xem page source và thấy ở chỗ này có thể `<input>` bị ẩn có giá trị trước và sau lỗi là "ok1" và "error"

```
<link rel="SHORTCUT ICON" href="https://developers.google.com/dark-legends.png">
<input type="hidden" name="status" value="ok1">

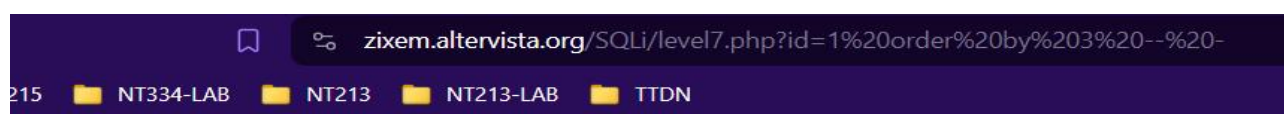
<link rel="SHORTCUT ICON" href="https://developers.google.com/dark-legends.png">
<input type="hidden" name="status" value="error">
```

Rồi có lỗi thì (nhận) khai thác thôi.



Age: 30
Cool rating: 10

Level developed by Zixem



Age: 30
Cool rating: 10

good luck. -Zixem

Tìm kiếm số cột thì thấy ở giữa 3 và 4 có sự khác biệt, chắc là 3 cột rồi.

Dùng union select tìm cột để khai thác:

Khi select 1,2,3 thì thấy chỗ giá trị thẻ <input> thay đổi, hiện số 2

```
<link rel="SHORTCUT ICON" href="https://developers.google.com/dark-legends.png">
<input type="hidden" name="status" value="ok2">
```

Khi select 1,3,3 thì hiện số 3. Vậy chỉ có thể khai thác ở cột thứ 2 thôi

```
<link rel="SHORTCUT ICON" href="https://developers.google.com/dark-legends.png">
<input type="hidden" name="status" value="ok3">
```

Truy vấn version() và user() thì có được kết quả

```
<link rel="SHORTCUT ICON" href="https://developers.google.com/dark-legends.png">
```

```
<input type="hidden" name="status" value="okzixem@localhost">
```

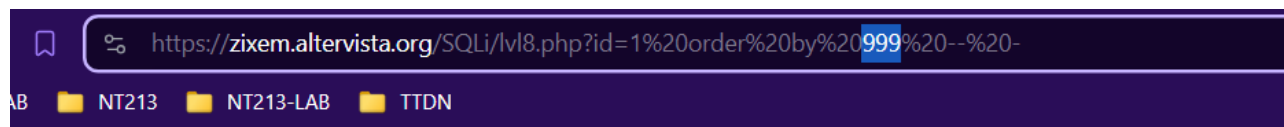
```
<link rel="SHORTCUT ICON" href="https://developers.google.com/dark-legends.png">
```

```
<input type="hidden" name="status" value="ok8.0.30">
```

⇒ Thấy được 2 thông tin cần tìm **“zixem@localhost”** và **“8.0.30”**

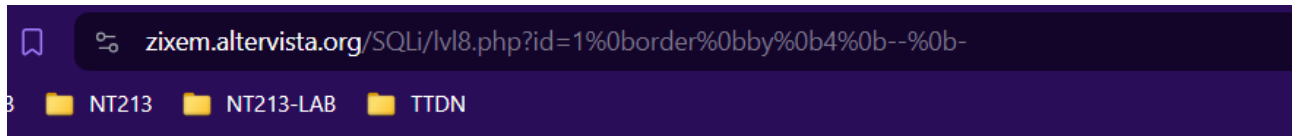
F. Level 8 (Hard)

Kiểm tra số cột bằng order by nhưng chỉ hiển thị Hacking attempt. Union select cũng chỉ hiện như vậy luôn



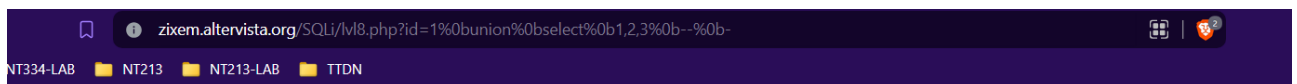
Hacking attempt

Lại tham khảo internet thì chỗ này bị encode khoảng trắng kiểu khác. Thay khoảng trắng thành %0b thì có được số cột là 3



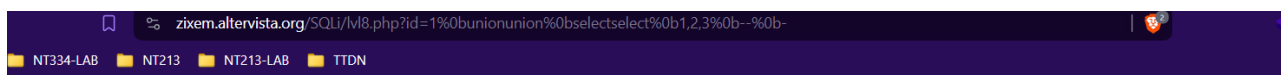
Unknown column '4' in 'order clause' ID:
Age:

Dùng union select thì nó mất union select luôn



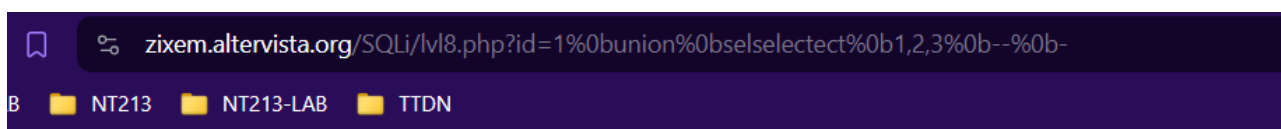
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1,2,3--' at line 1 ID:
Age:

Double 2 union select lên thử



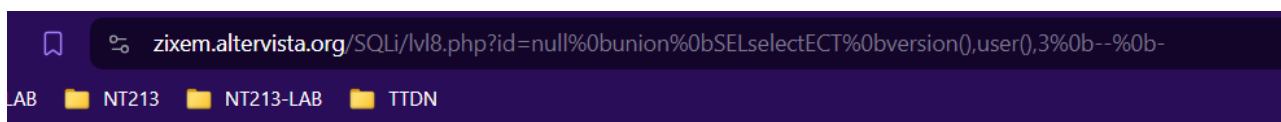
You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'unionunion 1,2,3--' at line 1 **ID:**
Age:

Lỗi ở đây rồi. Sửa chỗ select thì khai thác được rồi



ID: 1
Age: 20

Khai thác như bình thường thì ra kết quả



ID: zixem@localhost
Age: 8.0.30

⇒ Thấy được 2 thông tin cần tìm “**zixem@localhost**” và “**8.0.30**”
