Lab: SQL Injection

Important!

Please note that we have recently updated the VMs in the Network security section along with video instructions on how to install on Windows and MacOS systems. Please make sure that you are using the newer Kali Linux VMs that we have recently added to the Network Section. Easiest way to identify is by checking if you have the `Labs` folder on the Desktop which contains `main_script.sh` then you are on the right VM.

Pre-Requisite:

Before you can start the lab, you need to run the lab script which will setup everything. Open the **Labs** folder on Desktop then right-click and "Open Terminal Here". Or open a terminal and cd to Desktop/Labs folder, then issue the command:

```
sudo ./main_script.sh
```

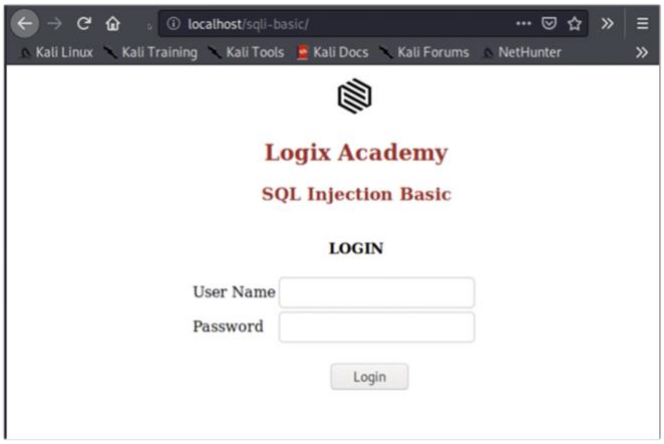
Select **SQL Injection Lab** option from the lab menu.

Purpose

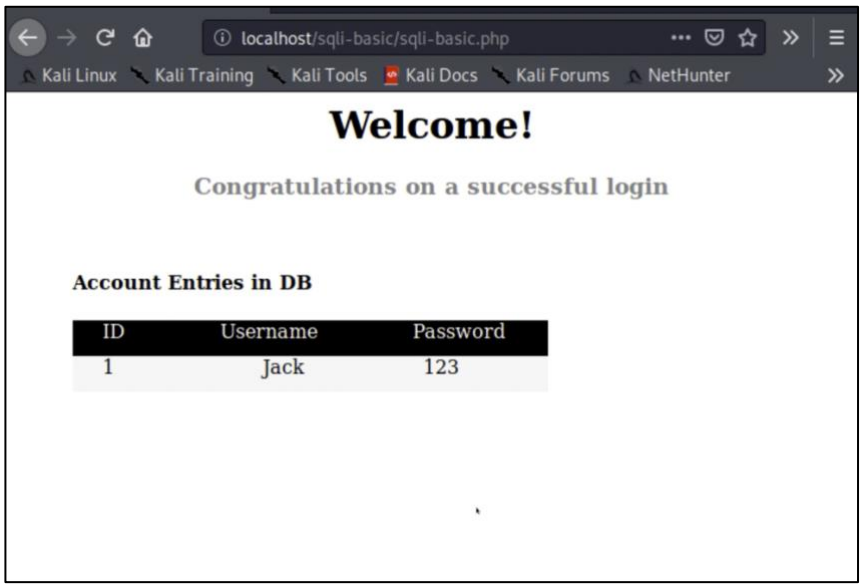
In this lab, we are going to demonstrate how an SQL injection is executed on a vulnerable website. You will also be required to carry out some SQL injection exercises.

SQL Injection Using Input Fields

1. Ensure that you have completed the pre-requisite step above (run *`main_script`* and select *`SQL Injection Lab`*)
2. Open the browser and open the URL: **localhost/sqli-basic**

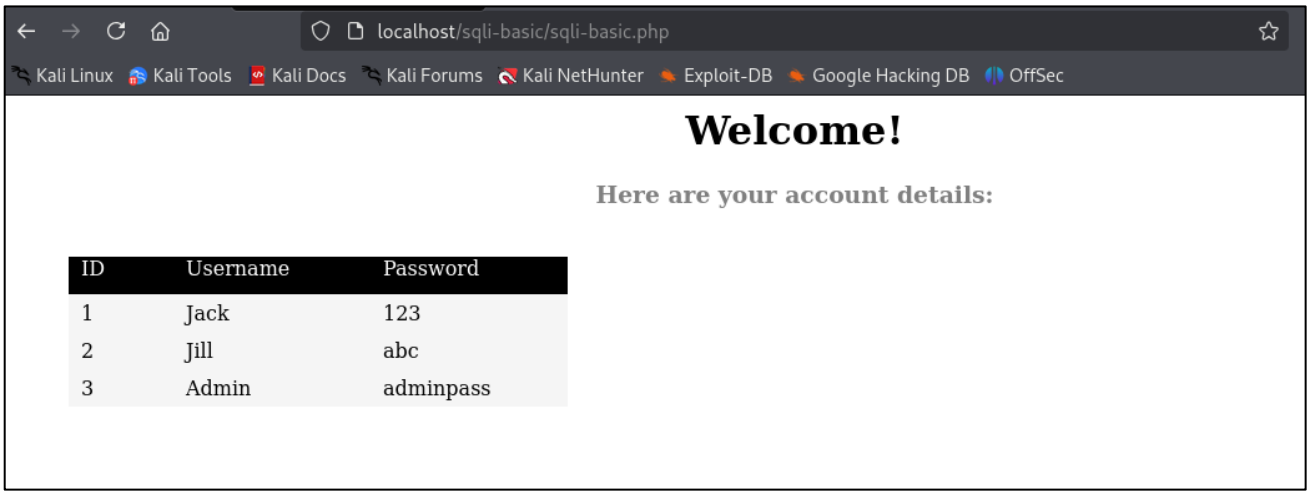


3. See the results for a legitimate user (user: Jack, password: 123):



4. Create a malicious SQL query using the following strings in username and password fields:

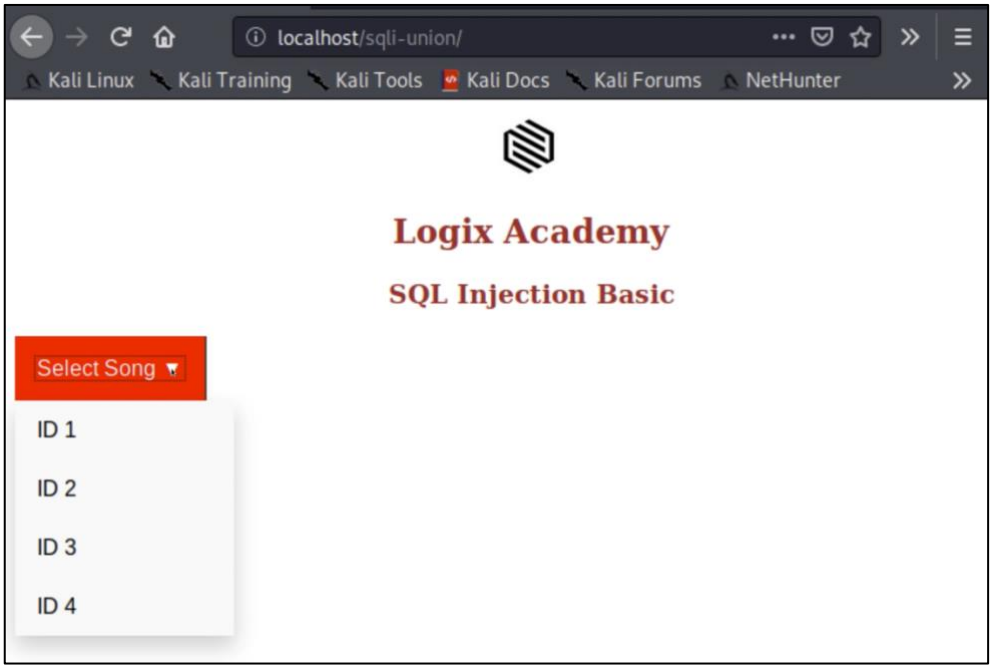
The results show that the malicious SQL query executed successfully and as a result, all the records in the Users table are displayed on the screen:



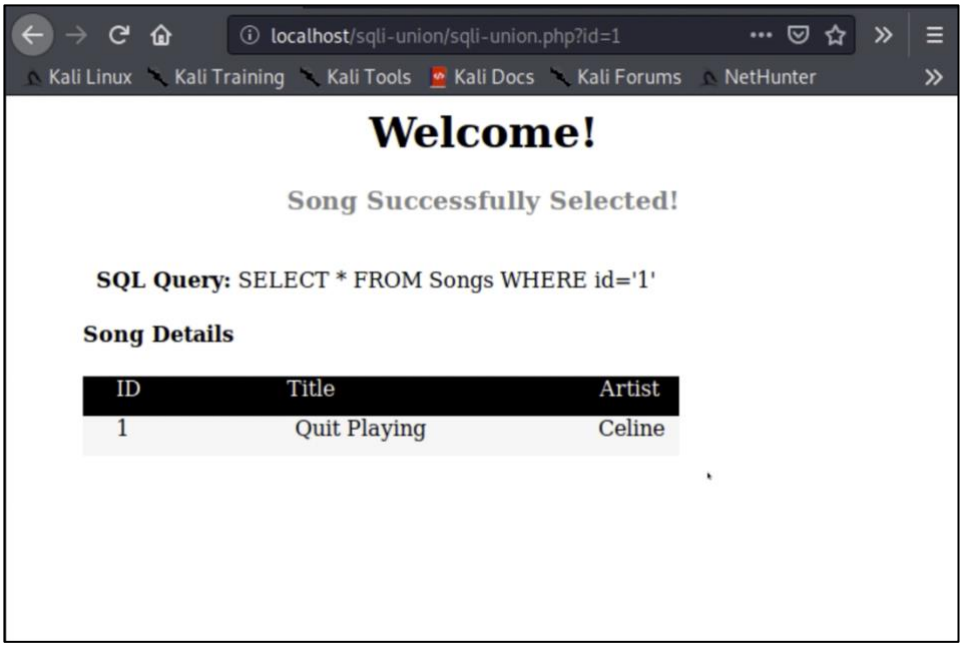
5. You can also craft a malicious SQL query by using blank for the last part of the query

SQL Injection By Modifying URL using OR Operator

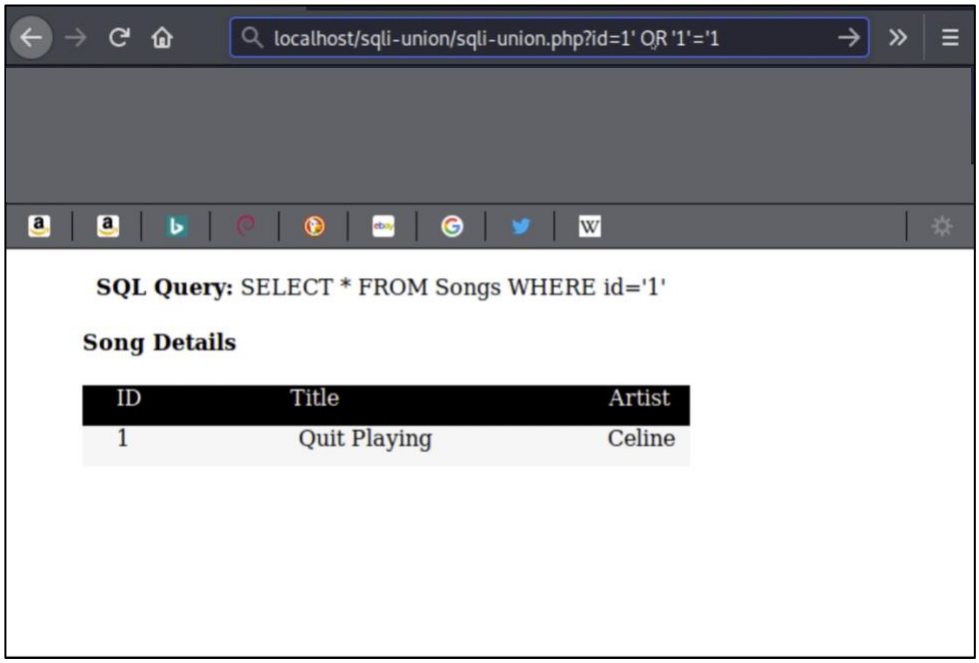
1. Open the browser and open the URL: **localhost/sqli-union** and select Song ID '1':



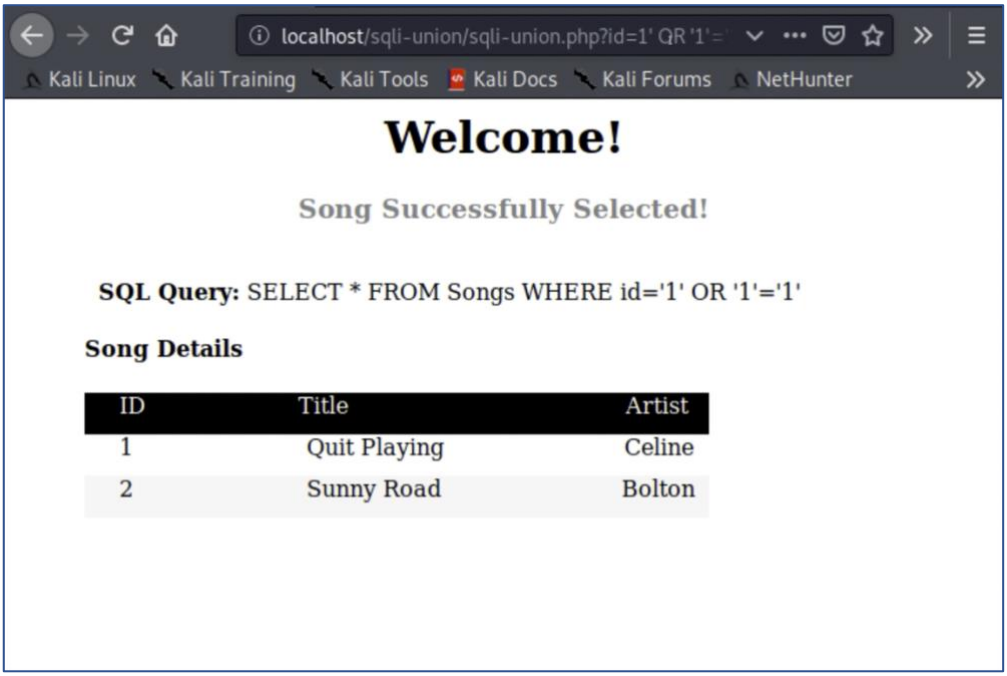
The results show details of the selected song:



2. Craft the malicious SQL query by inserting it directly in the URL:
   localhost/sqli-union/sql-union.php?id=1' OR '1'='1



The results show details of the selected song:

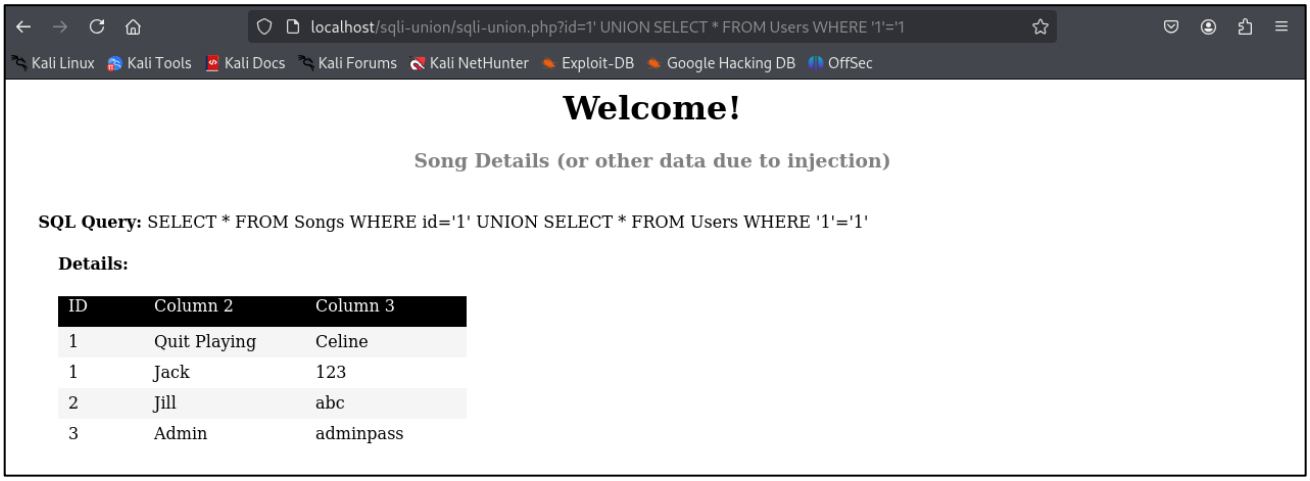


LOGIX ACADEMY

SQL Injection By Modifying URL using UNION Operator

1. You can also craft the malicious SQL query by using the UNION operator:
   localhost/sqli-union/sql-union.php?id=1' UNION SELECT * FROM Users WHERE '1'='1

The UNION operator basically joins two queries into one and as the results show, we get results both for the Songs table as well as a listing of all the records in the User table. The formatting is not aligned because we are actually seeing two different types of output:



Task:

- Craft a malicious SQL query which displays all the Songs in the Songs table, but you must:
  - Insert SQL injection directly in the URL **AND**
  - Use **ONLY** the Union Operator (You can't use OR)

(Solution on the next page)

LOGIX ACADEMY

Solution:

- You should first select any song e.g., ID='1' from the dropdown menu to the correct URL to modify and then insert the injection in the URL as follows:

  localhost/sqli-union/sql-union.php?id=1' UNION SELECT * FROM Songs WHERE '1'='1

  OR

  localhost/sqli-union/sql-union.php?id=1' UNION SELECT * FROM Songs WHERE ''='