**SQL INJECTION**

**Drugs:**

<<!DOCTYPE html>

<html>

<head>

<!-- Required meta tags -->

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

<style>

h1 {

background-color: #d3d3d3;

padding:10px;

}

</style>

<!-- Bootstrap CSS -->

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta/css/bootstrap.min.css" integrity="sha384-/Y6pD6FV/Vv2HJnA6t+vslU6fwYXjCFtcEpHbNJ0lyAFsXTsjBbfaDjzALeQsN6M" crossorigin="anonymous">

</head>

<body>

<div class="container-fluid">

<div class="page-header">

<br>

<h1 style="text-align:center">Pharmacy</h1>

<br>

<hr>

</div>

<div class="col-md-4 text-center">

<button type="button" class="btn btn-default center-block"><a href="pharmacy.php">HOME</a>

</button>

<form action="connect.php" method="post">

Enter the drug name: <input type="text" placeholder="search the drug" id="trade\_name" name="trade\_name"/>

<button type="submit" value="submit" name="submit" id="submit">SUBMIT</button>

</form>

<?php "include connect.php" ;

?>

</div>

</div>

<!-- Optional JavaScript -->

<!-- jQuery first, then Popper.js, then Bootstrap JS -->

<script src="https://code.jquery.com/jquery-3.2.1.slim.min.js" integrity="sha384-KJ3o2DKtIkvYIK3UENzmM7KCkRr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" crossorigin="anonymous"></script>

<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.11.0/umd/popper.min.js" integrity="sha384-b/U6ypiBEHpOf/4+1nzFpr53nxSS+GLCkfwBdFNTxtclqqenISfwAzpKaMNFNmj4" crossorigin="anonymous"></script>

<script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta/js/bootstrap.min.js" integrity="sha384-h0AbiXch4ZDo7tp9hKZ4TsHbi047NrKGLO3SEJAg45jXxnGIfYzk4Si90RDIqNm1" crossorigin="anonymous"></script>

</body>

</html>

**COMPANY:**

<<!DOCTYPE html>

<html>

<head>

<!-- Required meta tags -->

<meta charset="utf-8">

<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">

<style>

h1 {

background-color: #d3d3d3;

padding:10px;

}

</style>

<!-- Bootstrap CSS -->

<link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta/css/bootstrap.min.css" integrity="sha384-/Y6pD6FV/Vv2HJnA6t+vslU6fwYXjCFtcEpHbNJ0lyAFsXTsjBbfaDjzALeQsN6M" crossorigin="anonymous">

</head>

<body>

<div class="container-fluid">

<div class="page-header">

<br>

<h1 style="text-align:center">Pharmacy</h1>

<br>

<hr>

</div>

<div class="col-md-4 text-center">

<button type="button" class="btn btn-default center-block"><a href="pharmacy.php">HOME</a>

</button>

<form action="connect.php" method="post">

Enter the company name: <input type="text" placeholder="search the company" id="c\_name" name="c\_name"/>

<button type="submit" value="submit1" name="submit1" id="submit1">SUBMIT</button>

</form>

<?php "include connect.php" ;

?>

</div>

</div>

<!-- Optional JavaScript -->

<!-- jQuery first, then Popper.js, then Bootstrap JS -->

<script src="https://code.jquery.com/jquery-3.2.1.slim.min.js" integrity="sha384-KJ3o2DKtIkvYIK3UENzmM7KCkRr/rE9/Qpg6aAZGJwFDMVNA/GpGFF93hXpG5KkN" crossorigin="anonymous"></script>

<script src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.11.0/umd/popper.min.js" integrity="sha384-b/U6ypiBEHpOf/4+1nzFpr53nxSS+GLCkfwBdFNTxtclqqenISfwAzpKaMNFNmj4" crossorigin="anonymous"></script>

<script src="https://maxcdn.bootstrapcdn.com/bootstrap/4.0.0-beta/js/bootstrap.min.js" integrity="sha384-h0AbiXch4ZDo7tp9hKZ4TsHbi047NrKGLO3SEJAg45jXxnGIfYzk4Si90RDIqNm1" crossorigin="anonymous"></script>

</body>

</html>

**CONNECT:**

<?php

$servername = "localhost";

$username = "root";

$password = "";

$dbname = "pharmacy";

// Create connection

$conn = new mysqli($servername, $username, $password, $dbname);

// Check connection

if ($conn->connect\_error) {

die("Connection failed: " . $conn->connect\_error);

}

if(isset($\_POST['submit']))

{

session\_start();

$trade\_name=$\_POST['trade\_name'];

**$sql="Select \* from drug where trade\_name='$trade\_name'";**

$result = $conn->query($sql);

if ($result->num\_rows > 0)

{

echo"<table class='table table-striped'><tbody>";

while($row = $result->fetch\_assoc())

{

echo " <tr><td>NAME: </td><td>". $row["trade\_name"]. " </td></tr><tr><td>CONTENT: </td><td>". $row["content"]." </td></tr><tr><td>COLOR: </td><td>". $row["color"]."</td></tr>";

}

echo"</tbody></table>";

}

else

{

echo "0 results";

}

}

if(isset($\_POST['submit1']))

{

session\_start();

$c\_name=$\_POST['c\_name'];

**$sql="Select c\_id,cname from company where cname='$c\_name'";**

$result = $conn->query($sql);

if ($result->num\_rows > 0)

{

if ($result->num\_rows > 0)

{

while($row = $result->fetch\_assoc())

{

echo "<br> COMPANY ID: ". $row["c\_id"]. " <br>NAME: ". $row["cname"]."<br>";

}

}

}

else

{

echo "0 results";

}

}

if(isset($\_POST['submit2']))

{

session\_start();

$sql="Select \* from pharmacy where ph\_id=601";

$result = $conn->query($sql);

if ($result->num\_rows > 0)

{

if ($result->num\_rows > 0)

{

while($row = $result->fetch\_assoc())

{

echo "<br> ID: ". $row["ph\_id"]. " <br>NAME: ". $row["ph\_name"]." <br>ADDRESS: ". $row["ph\_address"]."<br>";

}

}

}

else

{

echo "0 results";

}

}

$conn->close();

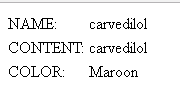
?>

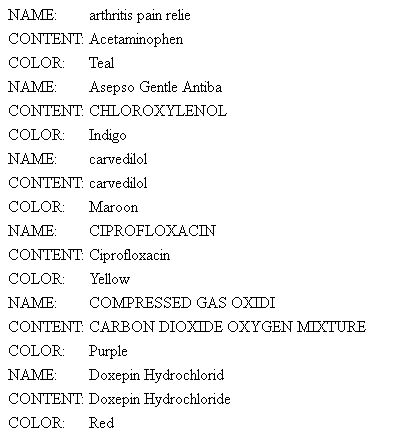
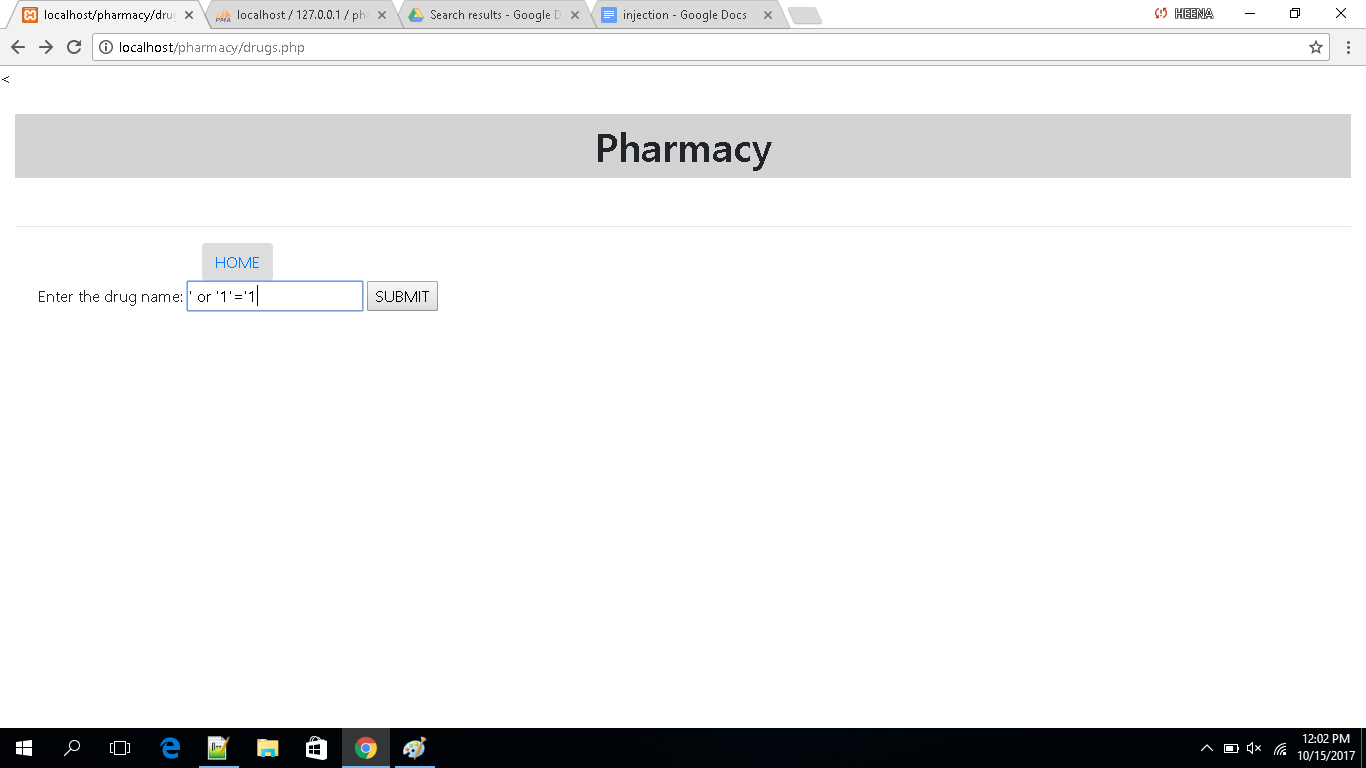
**OUTPUT:**

**1.TAUTOLOGY : using 1=1**

**$sql="Select \* from drug where trade\_name='$trade\_name'";**

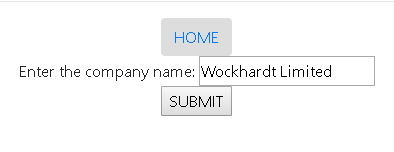
****

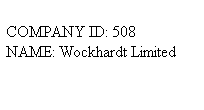
****

**INJECTION:**

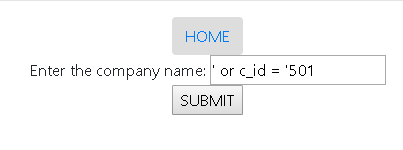
**2.Explicitly searching through id instead of name**

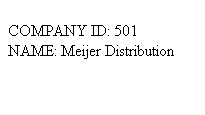
**$sql="Select c\_id,cname from company where cname='$c\_name'";**

****

****

**INJECTION:**

****

****