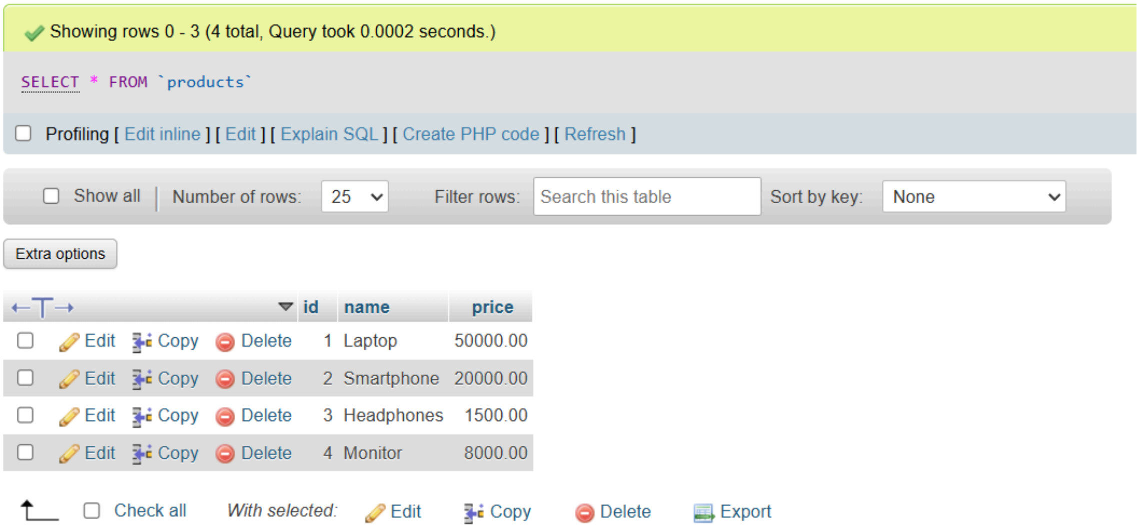
Name: Gaurang Vaghela
Rollno: TEAD-22561
Mini Project Lab
Mini Project
Problem Statement:

Create Database of Products:



✓ Showing rows 0 - 3 (4 total, Query took 0.0002 seconds.)

```
SELECT * FROM `products`
```

□ Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]
□ Show all | Number of rows: 25 Filter rows: Search this table Sort by key: None
Extra options

				id	name	price
□	Edit	Copy	Delete	1	Laptop	50000.00
□	Edit	Copy	Delete	2	Smartphone	20000.00
□	Edit	Copy	Delete	3	Headphones	1500.00
□	Edit	Copy	Delete	4	Monitor	8000.00

□ Check all *With selected:* Edit Copy Delete Export

SQL Injection vulnerable web page:

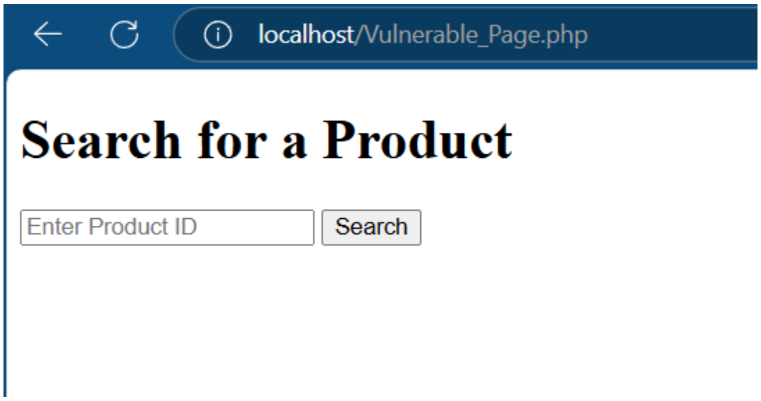
CODE:

```
<?php
$conn = new mysqli("localhost", "root", "", "sql_injection_demo");

if (isset($_GET["id"])) {
    $product_id = $_GET["id"];
    $query = "SELECT * FROM products WHERE id = '$product_id'";
    $result = $conn->query($query);

    while ($row = $result->fetch_assoc()) {
        echo "<p>Product Name: " . $row["name"] . "</p>";
        echo "<p>Price: $" . $row["price"] . "</p>";
    }
}
?>
<!DOCTYPE html>
<html>
```

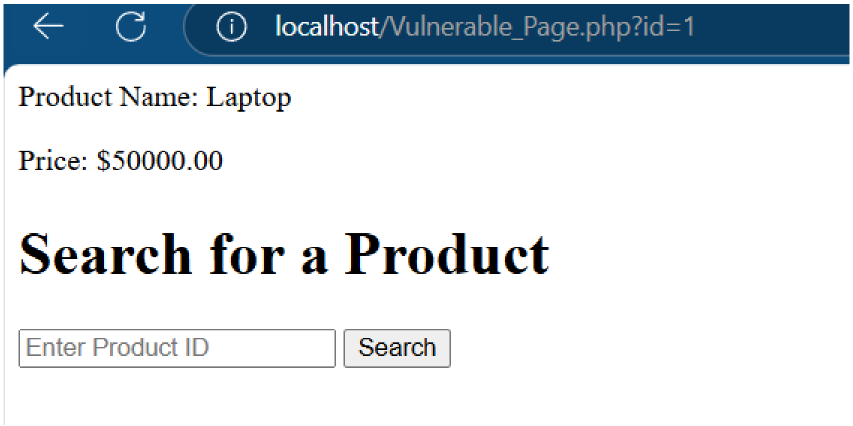
```
<head>
  <title>Product Search</title>
</head>
<body>
  <h1>Search for a Product</h1>
  <form method="GET">
    <input type="text" name="id" placeholder="Enter Product ID">
    <button type="submit">Search</button>
  </form>
</body>
</html>
```

OUTPUT:

If input is ‘1’:



Search for a Product

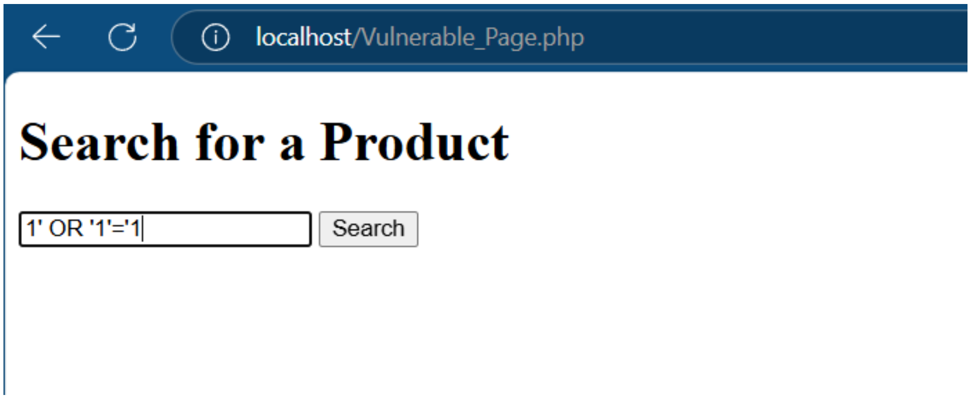


Product Name: Laptop

Price: $50000.00

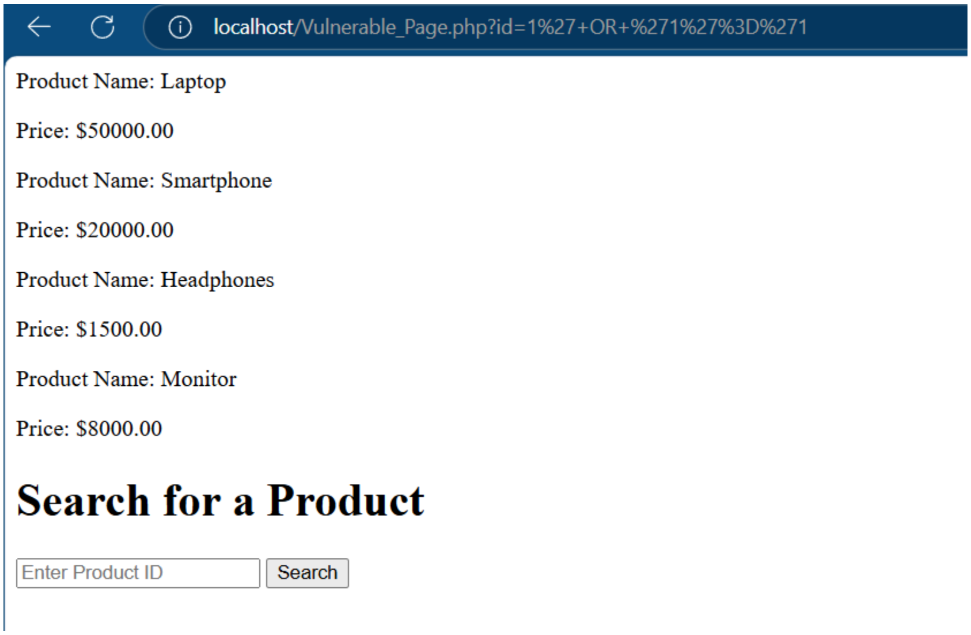
Search for a Product

If input is ‘1 OR 1=1’:



Search for a Product

1' OR '1'='1



```
Product Name: Laptop

Price: $50000.00

Product Name: Smartphone

Price: $20000.00

Product Name: Headphones

Price: $1500.00

Product Name: Monitor

Price: $8000.00
```

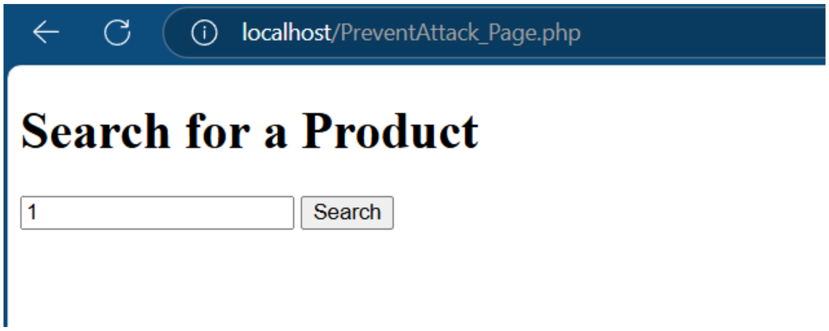
Search for a Product

SQL Injection Prevented web page:
CODE:

```
<?php
$conn = new mysqli("localhost", "root", "", "sql_injection_demo");

if (isset($_GET["id"])) {
    $stmt = $conn->prepare("SELECT * FROM products WHERE id = ?");
    $stmt->bind_param("i", $_GET["id"]);
    $stmt->execute();
    $result = $stmt->get_result();

    while ($row = $result->fetch_assoc()) {
        echo "<p>Product Name: " . htmlspecialchars($row["name"]) . "</p>";
        echo "<p>Price: $" . htmlspecialchars($row["price"]) . "</p>";
    }
}
?>

<!DOCTYPE html>
<html>
<head>
    <title>Product Search</title>
</head>
<body>
    <h1>Search for a Product</h1>
    <form method="GET">
        <input type="text" name="id" placeholder="Enter Product ID">
        <button type="submit">Search</button>
    </form>
</body>
</html>
```

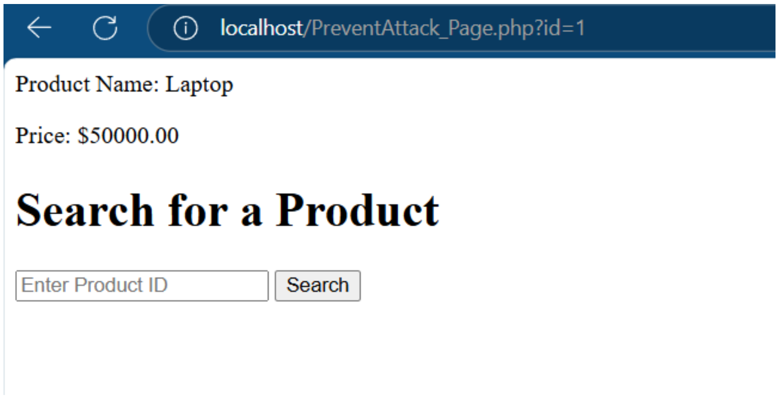
OUTPUT:

If input is ‘1’:



localhost/PreventAttack_Page.php

Search for a Product

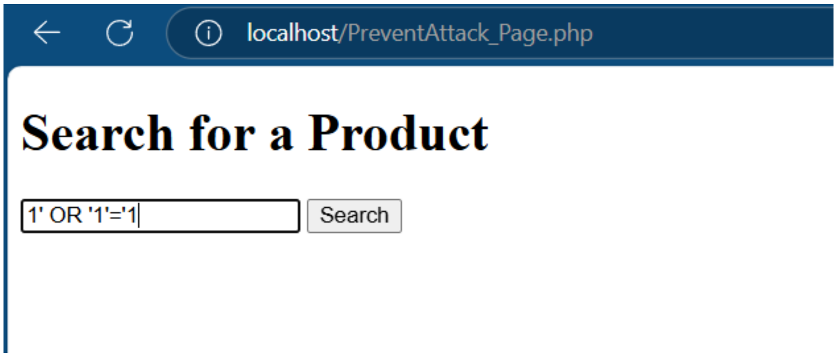


localhost/PreventAttack_Page.php?id=1

```
Product Name: Laptop

Price: $50000.00
```

Search for a Product

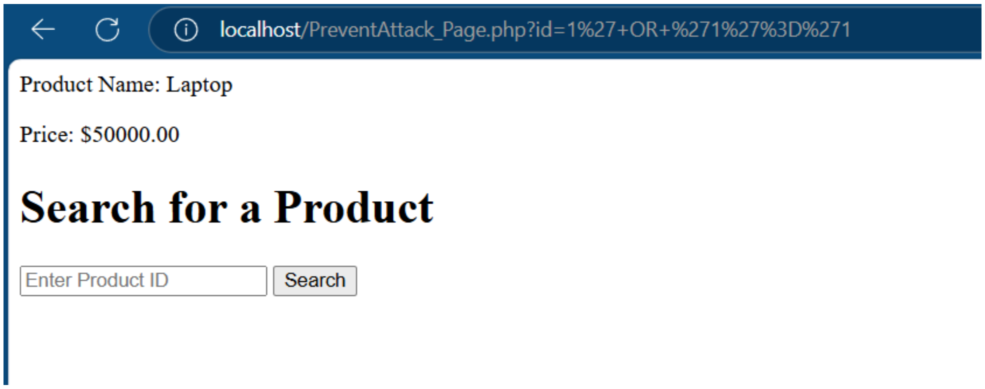
If input is ‘1 OR 1=1’:



localhost/PreventAttack_Page.php

Search for a Product

1' OR '1'='1



localhost/PreventAttack_Page.php?id=1%27+OR+%271%27%3D%271

Product Name: Laptop

Price: $50000.00

Search for a Product